Ричард Кларк, Роберт Нейк

Третья мировая война: какой она будет?

Перевела с английского Е. Карманова

Заведующий редакцией Руководитель проекта Ведущий редактор Корректоры Верстка

А. Кривцов А. Юрченко Ю. Сергиенко О. Андросик, Н. Викторова Л. Родионова

ББК 32.973.2 УДК 004.3 Кларк Р., Нейк Р.

К47 Третья мировая война: какой она будет? — СПб.: Питер, 2011. — 336 с.: ил.

ISBN978-5-459-00308-6

На протяжении первого десятилетия XXI века США, Россия, Китай и другие мировые державы развивают новый тип оружия, основанный на новейших технологиях и использовании информационных технологий и Интернета. Специальные подразделения готовят кибернетическое поле битвы с помощью так называемых логических бомб и лазеек, в мирное время размещая виртуальные взрывчатые вещества на территории других стран. Эта новая война — не игра и не плод нашего воображения, не альтернатива обычной войне. В действительности она способна увеличить вероятность более традиционных военных столкновений с применением огнестрельного оружия и ракет. Эта книга поможет понять, что представляет собой кибервойна, как и почему она развивается; проанализировать риски; подготовиться к ней и подумать о том, как ее контролировать. Для создания средств защиты от кибератак потребуется значительное время, но пока этого не произошло, мир подвергается новым серьезным угрозам ослабления международной стабильности и начала новой мировой войны — кибервойны.

Как велись кибервойны и информационные атаки в Сирии, Эстонии, Грузии и Ираке? Как за пятнадцать минут и без единого террориста или солдата одержать победу над целым государством? Новое поле битвы — киберпространство.

ISBN978-0061962233 англ. © HarperCollins, 2010

ISBN978-5-459-00308-6 © Перевод на русский язык ООО Издательство «Питер», 2011

© Издание на русском языке, оформление ООО Издательство «Питер», 2011

Права на издание получены по соглашению с HarperCollinsPublisherInc. Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав.

Информация, содержащаяся в данной книге, получена из источников, рассматриваемых издательством как надежные. Тем не менее, имея в виду возможные человеческие или технические ошибки, издательство не может гарантировать абсолютную точность и полноту приводимых сведений и не несет ответственности за возможные ошибки, связанные с использованием книги.

ООО «Мир книг», 198206, Санкт-Петербург, Петергофское шоссе, 73, лит. А29.
Налоговая льгота — общероссийский классификатор продукции ОК 005-93,
том 2; 95 3005 — литература учебная.

Подписано в печать 08.04.11. Формат 60x88/16. Уел. п. л. 21,000. Тираж 3000. Заказ 4595. Отпечатано по технологии CtPв ИПК ООО «Ленинградское издательство».

194044. Санкт-Петеобуог. ул. Менделеевская, д. 9.

□ГПАВЛЕНИЕ

Введение 7

Глава 1. Экспериментальные работы 15

Глава 2. Кибервоины 5 1

Глава 3. Поле битвы 9 1

Глава 4. Брешь в обороне 1 2В

Глава 5. Оборонительная стратегия 1 84

Глава 6. Как наступать? 217

Глава 7. Кибермир 26 1

Глава В. Повестка дня 3D3

Глоссарий 338

5

Ныне покойному Уильяму Виду Кауфману, который научил
меня и многих других разбираться в проблемах национальной

безопасности.

Ричард. Э. Кларк

Моей жене Элизабет, чья поддержка не знает границ. И нашей
дочери Шарлотте — желаю тебе расти в более мирное время.

Роберт Нейк

Введение

С

тояла серая промозглая вашингтонская зима. На небольшой улице, в особняке, наполненном коллекциями электрогитар и самых разнообразных предметов искусства, собралась наша компания, чтобы вспомнить того, кто учил нас разбираться в проблемах войны и обороны. Февральским вечером 2009 года бывшие студенты, большинству из которых уже шел шестой десяток, поднимали бокалы в честь девяностолетнего профессора Уильяма Вида Кауфмана, скончавшегося несколькими неделями ранее. Билл на протяжении долгих лет рассказывал студентам о вопросах обороны и ядерной стратегии [[1]](#footnote-2)

Третья мировая война: какой она будет?

в Массачусетском технологическом институте (MIT), а затем в Гарварде и Брукингском институте1. Целые поколения гражданских и военных экспертов выросли на его лекциях. Билл был также советником шести министров обороны и работал в администрации Е-кольца Пентагона[[2]](#footnote-3)[[3]](#footnote-4). На протяжении нескольких десятков лет он каждую неделю был вынужден курсировать между Бостоном и Вашингтоном.

За спиной некоторые из нас называли профессора Кауфмана Йодой, отчасти по причине едва уловимого физического сходства, но в основном потому, что мы считали его нашим мастером-джедаем, человеком, который понимал действие Силы и старался научить этому пониманию нас. Как аналитик и советник, Билл был одним из немногих гражданских специалистов, которые разработали основу стратегической ядерной военной доктрины в конце 1950-х — начале 1960-х годов. Именно эти люди предотвратили принятие ядерной стратегии, согласно которой Соединенные Штаты должны были нанести первый удар в ядерной войне, использовать весь ядер- ный потенциал в одной массированной атаке и уничто-

Введение

жить сотни городов в Европе и Азии. Билл и его коллеги, вероятно, спасли мир от атомной войны и сделали возможным контроль над стратегическими вооружениями. Наш разговор постепенно коснулся дальнейших перспектив. Что можем сделать мы в память Уильяма В. Кауфмана и других стратегов второй половины двадцатого столетия? Мы можем, предложил кто-то, продолжить их начинания, использовать то, чему научил нас Билл, ставить сложные и важные вопросы о стратегии сегодняшнего дня. Другие присутствовавшие за столом отметили, что наше время отличается от 1950-х, — тогда ядерное оружие развивалось, не имея продуманной стратегии, но ведь и сейчас стратегии не разработаны.

Но так ли изменилось наше время? На протяжении первого десятилетия XXI века Соединенные Штаты развивают новый тип вооружения, основанного на новейших технологиях, а продуманной стратегии у нас нет. Мы создали новое командование для ведения новой высокотехнологичной войны, пренебрегая публичными дебатами, обсуждениями в СМИ, серьезным парламентским надзором, академическим анализом или международным диалогом. Мы живем во время, в чем-то поразительно схожее с 1950-ми годами. Наверное, мы должны принять участие в просвещенной дискуссии и провести строгий анализ этого нового вида оружия, нового вида войны.

Речь идет о киберпространстве и войне, которая ведется в нем. 1 октября 2009 года начало работу новое подразделение Министерства обороны — Кибернетическое командование США, миссия которого заключается в использовании информационных технологий и Интернета в качестве оружия. Подобные подразделения существуют в России, Китае и ряде других стран. Эти военные и разведывательные организации готовят кибернетическое поле битвы с помощью так называемых логических бомб [[4]](#footnote-5)

Третья мировая война: какой она будет?

1

и лазеек, в мирное время размещают виртуальные взрывчатые вещества на территории других стран. В силу особенностей характера кибервойны у многих может возникнуть желание нанести первый удар. И в первую очередь это затронет не военных, а мирных граждан. Скорость, с которой можно поразить тысячи целей практически на всей планете, грозит стремительно развивающимися кризисами. Сила, которая предотвратила ядерную войну, — устрашение — не поможет при кибервойне. Сам феномен кибервойны покрыт такой завесой секретности, что по сравнению с ней даже холодная война кажется эпохой гласности и открытости. Но самый большой секрет кибервойны, пожалуй, заключается в том, что США, готовясь к наступательной войне, в то же самое время продолжают вести политику, при которой эффективная защита нации от кибератаки невозможна.

Страна, которая изобрела новую технологию и тактику ее применения, может и не стать победителем, если ее вооруженные силы зациклились на методах прошлого и слишком надеются на оружие, которое привыкли считать непревзойденным. Создатели нового наступательного оружия могут проиграть, если не выяснят, как защищаться от оружия, которое они уже продемонстрировали всему миру. Несмотря на то что американский полковник Билли Митчелл1 первым обосновал возможность небольших самолетов топить могучие линейные корабли, на практике эту догадку использовал японский военно-морской флот и едва не победил американцев в Тихом океане во время Второй мировой войны. Танк придумали англичане, а тактику стремительной массированной танковой

Введение

атаки при поддержке авиации и артиллерии — французский полковник Шарль де Голль. Однако в 1930-х годах недавно побежденная Германия усовершенствовала танк и первой стала применять тактику де Голля, названную блицкригом. (В 1990-е годы, а затем в 2003 году вооруженные силы США использовали в войне модернизированную версию блицкрига семидесятилетней давности — быстрое продвижение тяжелых танковых частей при поддержке авиации.)

Согретый братством бывших однокашников и мартини, я покинул особняк и побрел в холодную ночь, размышляя над иронией истории и обещая себе и Биллу приложить все силы, и начать открытое публичное обсуждение и исследование стратегии кибервойны прежде, чем нас втянут в нее. Эта книга — первый «взнос» по моему обязательству. Я знал: чтобы написать эту книгу, мне нужен молодой партнер, который присоединится к моим попыткам разобраться в военных и технологических последствиях кибервойны. Разные поколения по-разному воспринимают киберпространство. Для меня, шестидесятилетнего человека, киберпространство — это технология, рождение и развитие которой я видел своими глазами. Когда оно появилось, я уже занимался проблемами ядерного оружия в биполярном мире. В 2001 году я стал первым советником президента по кибербезопасности, но мои взгляды на кибервойну сформировались не без влияния опыта работы в области ядерной стратегии и разведки.

Когда мы писали эту книгу, Роду Нейку было тридцать. Для его поколения Интернет и киберпространство столь же естественны, как воздух и вода. Карьера Роба связана с проблемами национальной безопасности и международными проблемами XXI века. Мы работали вместе в школе государственного управления им. Джона Ф. Кеннеди (вхо-

 11

Третья мировая война: какой она будет?

дит в состав Гарвардского университета), в консалтинговой компании GoodHarborConsultingи принимали участие в президентской кампании Обамы. В 2009 году Роб получил престижный грант Совета по международным отношениям и приступил к изучению кибервойн. Книгу мы решили писать от первого лица, поскольку в тексте я много раз обращаюсь к собственному опыту сотрудничества с правительством, разработчиками информационных технологий, вашингтонскими кланами, но исследование, текст и концепция — это результат нашего совместного труда. Мы обошли Вашингтон, объездили всю страну в поисках ответов на множество вопросов, связанных с кибервойной. Многие люди помогли нам в этих поисках, некоторые из них предпочли остаться неназванными в этой книге. Мы провели много часов обсуждая, дискутируя, споря, пока не нашли некий синтез наших воззрений. Роб и я единогласны в том, что кибервойна — это не война без потерпевших, не новый чистый вид борьбы, который мы должны приветствовать. Но это и не секретное оружие, которое нужно скрывать от света дня и общественности. Что касается публики, именно гражданское население Соединенных Штатов и частные компании, на которых держится благополучие всей страны, пострадают от этой войны в первую очередь.

Может показаться, что у Америки есть преимущество, но кибервойна опаснее для США, чем для других стран. Эта новая война — не игра и не плод нашего воображения, не альтернатива обычной войне. В действительности она способна увеличить вероятность более традиционных военных столкновений с применением взрывчатых веществ, огнестрельного оружия, ракет. Если бы в наших силах было запихнуть джинна обратно в бутылку, мы бы так и поступили, но это невозможно. Поэтому нам нужно решить целый комплекс задач: понять, что собой представ-

Введение

ляет кибервойна, узнать, как и почему она развивается, проанализировать риски, подготовиться к ней и подумать о том, как ее контролировать.

Эта книга — попытка начать работу в указанном направлении. Она не техническое исследование и не руководство для инженеров по вопросам информационного оружия. Не станет она и энциклопедией для вашингтонских «ботаников», полной аббревиатур и жаргонизмов. И наконец, она определенно не является военным документом, написанным для незамедлительного перевода на пентагонский канцелярит. По этой причине некоторые эксперты, возможно, сочтут эту книгу примитивной в тех местах, где обсуждаются проблемы, над которыми они работают, и туманной, когда затрагиваются вопросы, выходящие за пределы их компетенции. В целом же мы старались найти баланс и изложить информацию в неофициальном стиле — простом и иногда забавном. Однако мы не обошлись и без необходимого в такой книге обсуждения технологий, вашингтонских реалий и даже некоторых военных и разведывательных вопросов. Более того, не удалось полностью избежать сокращений и профессионального жаргона, в связи с чем мы добавили небольшой словарик.

Руководители службы национальной безопасности за десятилетия приучили меня не поднимать проблемы, не предлагая путей их решения. В книге, разумеется, рассматривается множество проблем, но при этом приведены и возможные способы их решения. Для воплощения в жизнь этих или других средств защиты потребуется время, ведь сейчас США и другие страны сталкиваются с новыми серьезными угрозами миру, международной стабильности, внутреннему порядку, а также национальному и индивидуальному экономическому благосостоянию.

 1 з

Третья мировая война: какой она будет?

\* \* \*

Мы выражаем благодарность всем тем, кто помог написать эту книгу, особенно правительственным и неправительственным экспертам, которые предпочли остаться неназванными. Питер Затко, Джон Мэллери, Крис Джордан, Эд Аморосо, Сэмми Сейдяри и Барнэби Пейдж помогли нам разобраться в технических аспектах кибербезопасности. Пол Куртц стал резонатором наших идей и постоянно помогал кристаллизовать важнейшие мысли. Кен Мини- хэн, Майк Макконнелл и Рич Вилхелм поделились своими соображениями по рассматриваемым здесь непростым вопросам. Мы признательны Жанет Наполитано за то, что она, несмотря на плотный график, нашла время для встречи с нами. Мы также благодарны Рэнд Бирс за его мудрость. Уилл Ховертон помог нам закончить работу над книгой, у него прекрасное редакторское чутье и дар к исследовательской работе. Уилл Барденверпер также посодействовал нам как редактор. А без Бев Раундтри мы бы просто не справились.

Глава 1

Экспериментальные работы

М

есяц отражался в медленных водах Евфрата, на берегах которого вот уже пять тысячелетий сражаются народы. Стояла ночь 6 сентября 2007 года, и у Евфрата вот-вот должна была произойти атака нового типа — та, что началась в киберпространстве. На восточном берегу реки, в ста двадцати километрах на юг от турецкой границы, косые тени разрезали песчаные стены высохшего русла реки. Большое строящееся здание тускло светилось.

Третья мировая война: какой она будет?

Шестью часами ранее из него вышли многочисленные рабочие из Северной Кореи, дисциплинированно выстроившись в очереди, чтобы сесть в автобусы и отправиться в общежитие. Для стройплощадки это место выглядело слишком темным и незащищенным, как будто подрядчик опасался привлечь внимание. Вдруг маленькие звездочки, горевшие над стройплощадкой, вспыхнули и залили пространство бело-голубым светом, стало ярче, чем днем. Это длилось не больше минуты, хотя нескольким сирийцам и корейцам, оставшимся на стройке, показалось, что прошла вечность. Сверкнула слепящая вспышка, затем прокатилась оглушающая звуковая волна, и все превратилось в развалины. Если бы люди не лишились на время слуха из-за взрыва, они, припавшие к земле, услышали бы отдаленный звук реактивных двигателей военных самолетов. Если бы они могли видеть сквозь пламя, уничтожавшее стройку, то заметили бы высоко в небе, над сигнальными ракетами, которые все еще спускались на маленьких парашютах, они заметили бы, как несколько истребителей F-15 Eaglesи F-16 Falconsповернули на север и полетели по направлению к Турции. А кто-то мог бы даже разглядеть сине-белые звезды Давида на крыльях самолетов военно-воздушных сил Израиля, полностью уничтоживших плод многолетней секретной работы.

Почти столь же необычным, как и этот налет, стало дальнейшее политическое безмолвие. Управление по связям с общественностью израильского правительства молчало. Что еще более странно, Сирия, которая подверглась бомбардировке, не сделала никаких заявлений. Постепенно история начала просачиваться в американские и британские СМИ. Израиль нанес удар по комплексу в Восточной Сирии, который строила Северная Корея. Здание было связано с производством оружия массового поражения, утверждали СМИ, ссылаясь на неназванные

Экспериментальные работы

источники. Израильские цензоры позволили своим газетам процитировать сообщения американских средств массовой информации, но запретили писать собственные комментарии. Это, утверждали они, вопрос национальной безопасности. Позднее правительство Сирии, под напором сообщений СМИ, признало факт нападения и даже заявило протест. Сирийский президент Ассад стал утверждать, что разрушено было пустое здание. Любопытно, что только Северная Корея присоединилась к Дамаску, выражая возмущение этим внезапным нападением. Пресса несколько расходилась во мнениях, что и почему произошло, но по большей части журналисты цитировали заявление израильских правительственных источников о том, что здание являлось северокорейским заводом по производству ядерного оружия.

Если так и было, значит, Северная Корея нарушила соглашение с Соединенными Штатами и другими крупными державами о прекращении продажи секретов производства ядерного оружия. Что еще хуже, это означает, что Сирия, ведущая переговоры с Израилем через посредника (Турцию), пытается тайно завладеть ядерным оружием — совершить то, от чего отказался даже Саддам Хусейн еще до вторжения США в Ирак.

Вскоре, однако, самопровозглашенные эксперты поставили под сомнение историю «Сирия создавала ядер- ную бомбу».

В западной прессе появились фотографии, сделанные с разведывательного спутника. Эксперты отметили, что стройплощадка накануне бомбардировки довольно плохо охранялась. Некоторые утверждали, что здание было недостаточно высоким, чтобы в нем поместился северокорейский ядерный реактор. Другие указывали на отсутствие какой бы то ни было ядерной инфраструктуры в Сирии. Стали возникать альтернативные теории. Воз-

 17

"ГрЕТЬЯ МИРОВАЯ война: какой она будет?

можно, здание имело отношение к сирийской ракетной программе. Возможно, Израиль ошибся и сооружение было безобидным производственным объектом вроде «фабрики по производству детского питания» (как утверждал Саддам Хусейн в 1990 году) или предполагаемого завода по производству аспирина в Судане, тоже разрушенного американцами в 1998 году. Или, может быть, говорили некоторые комментаторы, Сирия вообще не была целью нападения. Возможно, Израиль посылал Ирану сигнал о том, что еврейское государство способно успешно наносить внезапные удары с воздуха, что подобное может случиться и с иранскими ядерными установками, если Тегеран не свернет ядерную программу.

В прессе цитировались неназванные источники, заявлявшие о разной степени причастности американцев к нападению: американцы обнаружили место на фотографии со спутника; американцы не заметили место, но его нашли израильтяне на снимке, который им вручила американская разведка; американцы помогли составить план бомбардировки, возможно, убедив турецких военных смотреть в Другую сторону, пока израильские самолеты летели над Турцией, чтобы неожиданно атаковать Сирию с севера. Американцы — или это были израильтяне? — проникли на стройплощадку до бомбардировки, чтобы убедиться в присутствии северных корейцев или подтвердить ядерное назначение объекта. Президент Джордж Буш, нехарактерно молчаливый, категорически отказался отвечать на вопрос репортера об израильской атаке.

Единственное, в чем сходились почти все обозреватели, так это факт, что произошло нечто странное. В апреле 2008 года ЦРУ предприняло необычный шаг — представило и опубликовало видеозапись того, что происходило в здании накануне бомбардировки. Фильм практически не оставлял сомнений в том, что это была северокорей-

Экспериментальные работы

ская ядерная установка. Обсуждение этой истории закончилось. Мало внимания привлек и опубликованный семь месяцев спустя доклад Международного агентства по атомной энергетики (МАГАТЭ). Они послали на место происшествия инспекторов. Те обнаружили вовсе не разбомбленные руины и не новое строительство в полном разгаре. Вместо этого международные эксперты увидели аккуратно вспаханную и разрыхленную землю без каких-либо признаков развалин и строительных материалов. Место превратилось в пустырь на окраине города Финикса и казалось совершенно безобидным. Разочарованные инспекторы сделали несколько фотографий, наполнили пластиковые мешочки образцами почвы, а затем покинули берега Евфрата и отправились на берега Дуная в штаб-квартиру на острове близ Вены. Там в лабораториях и были проведены исследования.

МАГАТЭ, не сумев привлечь особого внимания, объявило, что образцы почвы содержат необычные «рукотворные» радиоактивные материалы. Для немногочисленных заинтересованных лиц, которые отслеживали загадочную сирийскую историю, это стало окончательным выводом, подтверждающим добросовестную работу израильской разведки.

Как ни трудно в это поверить, но Сирия обвела всех вокруг пальца и начала производство ядерного оружия, а северокорейский режим помогал ей. Теперь пора было подвергнуть переоценке замыслы и Дамаска, и Пхеньяна. Но за всей этой тайной, однако же, стояла другая интрига. Сирия потратила миллиарды долларов на систему противовоздушной обороны. В ту сентябрьскую ночь сирийские военные внимательно следили за радарами. Чуть ранее Израиль внезапно разместил на Голанских высотах свои войска, приведя их в полную боевую готовность. С этой позиции на оккупированной сирийской территории изра-

Третья мировая война: какой она будет?

ильские солдаты могли увидеть центр Дамаска в бинокли. Сирийские вооруженные силы ожидали сигнала тревоги. Однако ничего необычного на экранах радаров не наблюдалось. Полночь приближалась, а небо над Сирией казалось мирным и почти пустым. Но на самом деле со стороны Турции в сирийское воздушное пространство вторгся строй истребителей Ф-15 и Ф-16. Эти самолеты, спроектированные еще в 1970-х, сложно не заметить. Их корпуса из стали и титана, острые ребра и углы, бомбы и ракеты, свисающие с крыльев, должны были расцветить сирийские радары, как рождественскую елку на Рокфеллер- плаза в декабре. Но этого не произошло.

На следующее утро сирийцы медленно, с неохотой, мучительно пришли к выводу, что накануне ночью Израиль «завладел» дорогущей сетью сирийской противовоздушной обороны. Экраны радаров показывали то, что им приказывали военно-воздушные силы Израиля, — пустоту. Картинка, которую видели сирийцы, не имела никакого отношения к действительности, а в это время израильские самолеты с востока проникли в воздушное пространство Сирии. Сирийские ракеты противовоздушной обороны не запускались потому, что не видели целей. Сирийские истребители ПВО не могли взлететь, поскольку системы российского производства управляются с земли, а сирийские наземные управляющие устройства цели не видели.

Ближе к вечеру зазвонили телефоны в российском Министерстве обороны. Почему это российская система ПВО ослепла? Сирия хотела бы знать ответ. Москва пообещала тотчас же выслать экспертов и техников. Возможно, проблема в эксплуатации или ошибке пользователя, все будет незамедлительно исправлено. Российскому военно-промышленному комплексу не нужна такая дурная слава. Тем более Иран уже почти купил у Москвы но- 20

Экспериментальные работы

вую систему радаров и противовоздушных ракет. Это был шок для командиров противовоздушной обороны и в Тегеране, и в Дамаске.

Кибервоины всего мира, однако, не удивились. Так в информационную эпоху и должна вестись война — кибервойна. Когда в этой книге мы используем термин «кибервойна», он означает действия по проникновению одного государства в компьютеры или сеть другого государства с целью нанесения повреждений или разрушения. Когда Израиль атаковал Сирию, его войска использовали свет и электрические импульсы не для того, чтобы резать, как лазером, или глушить, как «Тазером», но чтобы передавать нули и единицы и контролировать все, что видят сирийские радары ПВО. Вместо того чтобы взрывать радары противовоздушной обороны и лишаться элемента неожиданности, израильтяне сделали так, чтобы враг даже не привел в действие систему защиты.

Израильтяне спланировали и провели кибератаку безупречно. Как они сделали это, можно лишь догадываться.

Существует по меньшей мере три возможных объяснения того, как они взломали сеть сирийцев.

Во-первых, как утверждали некоторые СМИ, израильской атаке мог предшествовать вылет беспилотного летательного аппарата (БПЛА), намеренно запущенного в луч сирийского радара ПВО. По сути своей, принцип работы радаров остался тем же, что и семьдесят лет назад, во времена битвы за Англию. Радиолокационная станция посылает направленный радиолуч. Если луч во что-либо упирается, он отражается и возвращается обратно к радиоприемному устройству. Затем процессор рассчитывает, где находился объект, когда в него попал радиолуч, на какой высоте он летел, с какой скоростью двигался и даже какого он был размера. Главное здесь в том, что радар позволяет электронному лучу вернуться обратно в ком-

 2 1

Третья мировая война: какой она будет?

пьютерную систему наземного базирования. Радар — это дверь в компьютер, открытая, чтобы получать обратно сигналы, отправленные для обнаружения объектов в небе. Сирийская система ПВО могла не заметить израильский беспилотный летательный аппарат, поскольку он покрыт материалом, поглощающим или отклоняющим радиолокационные лучи. Однако БПЛА, в свою очередь, мог обнаружить луч радара, идущий к нему от земли, и использовать ту же самую радиочастоту, чтобы передать пакеты информации в компьютер радара, а оттуда в сеть сирийской системы противовоздушной обороны. Эти пакеты нарушили нормальную работу системы, но также дали ей команду не замечать, что не все в порядке. Возможно, они просто повторяли данные, полученные системой до атаки. Таким образом, хотя радиолокационный луч мог обнаружить вторгшиеся самолеты, отраженный сигнал не был зарегистрирован компьютерами сирийской системы ПВО. Небо казалось пустым, хотя на самом деле его заполонили израильские истребители. Американские СМИ писали, что у США имеется подобная система под кодовым названием SeniorSuter.

Второй вариант — возможно, российская программа, управляющая сирийской ПВО, была «подправлена» израильскими агентами. На каком-то этапе — в российском компьютерном центре или на сирийском военном объекте — кто-то, работающий на Израиль или его союзников, мог специально подготовить «черный ход» в машинном коде, состоящем из миллионов строк, которые управляют действием программы противовоздушной обороны. Ловушка (или «троянский конь») — это всего лишь несколько строк машинного кода, ничем на вид не отличающихся от прочей абракадабры, которую представляют собой инструкции для работы системы или приложения. (Тесты, проведенные Агентством национальной безопас-

22

Экспериментальные работы

ности, показали, что даже самые опытные эксперты, просматривая миллионы символьных строк, могут не заметить ошибку, добавленную в программу.) Ловушка могла содержать инструкцию о том, как реагировать на события в определенных обстоятельствах. К примеру, если радар принимает определенный сигнал, он не должен показывать цели в небе на протяжении указанного периода времени, скажем, трех последующих часов. Таким образом, от израильского беспилотного летательного аппарата требовалось всего лишь послать маленький сигнал. Ловушка могла оказаться скрытой точкой электронного доступа, которая позволяет подсоединиться к сети ПВО, пройти систему контроля, брандмауэр, дешифровщик и завладеть управлением сети, получив все права и привилегии администратора.

Суть третьего варианта в том, что израильский агент мог найти оптоволоконный кабель сирийской системы ПВО и подсоединиться к линии (это сложнее сделать, чем сказать, но все же выполнимо). Израильский агент мог передать по кабелю команду, которая открыла бы для него «черный ход». Конечно, сложно представить израильского агента, передвигающегося ползком по территории Сирии, чтобы найти и разрезать оптоволоконный кабель, но ничего невероятного в этом нет. Уже не первое десятилетие высказываются предположения о том, что Израиль занимается подготовкой шпионов. Оптоволоконные кабели системы сирийской ПВО тянутся через всю страну. Преимущество такого метода внедрения в сеть противника очевидно — не нужно ставить успех операции в зависимость от сигнала захвата, передаваемого в сеть от беспилотного летательного аппарата. Более того, агент, работающий на месте, мог, например, установить прямое соединение со штабом израильских военно-воздушных сил. Используя методы связи с малой вероятностью перехвата, израиль-

23

Третья мировая война: какой она будет?

ский агент мог прямо из центра Дамаска по скрытому каналу передавать сообщения через спутник, не опасаясь, что кто-нибудь в Сирии его обнаружит.

Любой из методов обмана сирийской ПВО мог быть позаимствован у Соединенных Штатов. Израильские друзья всего лишь использовали несколько методов из программ, над которыми мы работаем более двух десятилетий. В 1990 году, когда Соединенные Штаты первый раз готовились к войне с Ираком, американские кибервоины и коммандос из спецподразделений собрались, чтобы обсудить, как уничтожить иракскую систему противоракетной обороны до того, как самолеты США и союзников полетят к Багдаду. Как объяснил мне герой «Бури в пустыне» генерал Норм Шварцкопф, «у этих кобр была безумная идея» проникнуть в Ирак до того, как прогремит первый выстрел, и запустить программу, которая приведет к необратимой поломке всех компьютеров, объединенных в сеть по всей стране.

Шварцкопф счел такой план слишком рискованным и ненадежным. Он был невысокого мнения об американских коммандос и боялся, что они попадут в плен еще до начала войны. Более того, Шварцкопф опасался, что иракцы смогут восстановить компьютеры и начнут сбивать самолеты, которые он планировал в первый день воздушной войны направить в атаку. «Если вы хотите доказать мне, что их радары и ракеты не работают, взорвите их. Тогда они точно выйдут из строя. Затем начинайте атаку и бомбите цели». Таким образом, большая часть бомбовых ударов американцев и союзников была нанесена не по штаб- квартире в Багдаде и дивизиям иракских вооруженных сил, а по радарам и ракетам системы противовоздушной обороны. Некоторые американские самолеты оказались сбиты, некоторые пилоты погибли, а некоторые попали в плен.

24

Экспериментальные работы

Когда 13 лет спустя США во второй раз начали войну с Ираком, еще накануне вторжения первых американских истребителей иракские военные знали, что их закрытая секретная надежная военная сеть рассекречена. Американцы предоставили им эту информацию.

Как раз перед началом войны тысячи иракских офицеров получили электронные письма, разосланные почтовой системой Министерства обороны Ирака. Хотя их текст никогда не публиковался, несколько надежных источников в достаточной степени раскрывают суть их содержания, чтобы предположить, что мог прочесть, скажем, бригадный генерал иракской армии, под командованием которого находится бронетанковая часть неподалеку от Басры:

Командование центральной военной группировки США доводит до вашего сведения, что мы можем отдать приказ о вторжении в Ирак в любой момент. Если мы это сделаем, войска, противостоящие нам, будут уничтожены, как это произошло несколько лет назад. Мы не хотим вредить ни вам, ни вашим солдатам. Наша цель — низвергнуть режим Саддама и его сыновей. Если вы хотите остаться невредимыми, выстройте танки и бронемашины рядами и покиньте их. Уходите, вам и вашим войскам лучше разойтись по домам. Вы и другие иракские офицеры будете восстановлены в должностях после свержение режима Саддама.

Неудивительно, что многие иракские офицеры последовали рекомендациям, которые были разосланы по внутренней иракской сети. Как обнаружили американцы, многие подразделения аккуратно выстроили танки за пределами баз, тем самым позволив американским само-

25

Третья мировая война: какой она будет?

летам аккуратно их взорвать. Некоторые иракские военачальники распустили свои подразделения за несколько часов до начала войны. Люди переоделись в гражданскую одежду и ушли домой или, по крайней мере, попытались так поступить.

Хотя администрация Буша и выразила готовность внедриться в иракскую сеть, чтобы провести психологическую подготовку до начала традиционных военных действий, она, по всей видимости, не пошла на взлом банковской сети Ирака и других стран, чтобы лишить Саддама Хусейна доступа к деньгам. Такие возможности действительно существуют, но юристы опасаются, что другие страны воспримут покушение на банковские счета как нарушение международного закона и сочтут опасным прецедентом. Юрисконсульты также боятся непредусмотренных последствий, в частности того, что американские хакеры ограбят не те счета или разрушат всю систему финансовых институтов.

Вторая война между США и Ираком, как и нападение Израиля на Сирию, продемонстрировала два преимущества кибервойны. Во-первых, кибервойна облегчает традиционные наступательные военные действия, выводя из строя систему обороны врага. Во-вторых, кибервойна позволяет деморализовать врага с помощью пропаганды, рассылки информации по электронной почте и через другие интернет-ресурсы вместо устаревшей практики сбрасывания листовок. (Вспомните тысячи листовок с текстом на арабском языке и рисунками, которые сбрасывались с самолетов над иракскими войсками в 1991 году, — это были подробные инструкции о том, как капитулировать. Эти листовки несли с собой тысячи иракских солдат, когда сдавались.)

26

Экспериментальные работы
\* \* \*

Налет на сирийскую ядерную установку и киберактивность США накануне вторжения в Ирак — вот примеры использования хакеров как вспомогательного инструмента традиционной наступательной войны. Однако использование киберпространства в политических, дипломатических и военных целях не обязательно должно сопровождаться бомбардировками и танковыми сражениями. Представить, как будет выглядеть автономная кибервойна, помог, как ни странно, небольшой ганзейский город с населением в 400 тысяч человек, расположенный на берегах Балтийского моря, — Таллинн. Советский Союз распался, и многие его республики отмежевались от Москвы и СССР. Эстония была вынуждена войти в состав Советского Союза, после того как Красная Армия освободила Балтийские республики от нацистов во время Великой Отечественной войны, как называют Вторую мировую в России.

Красная Армия или, по крайней мере, коммунистическая партия Советского Союза не желали, чтобы эстонцы, так же как и остальные народы Восточной Европы, забыли жертвы, принесенные во имя их освобождения. Поэтому в Таллине, как и в большинстве столиц восточноевропейских стран, воздвигались огромные памятники солдатам Красной Армии. Чаще всего эти бронзовые солдаты устанавливались на могилах красноармейцев. Я на такой монумент впервые наткнулся, почти в буквальном смысле слова, в Вене в 1974 году. Когда я спросил охранявших его полицейских, почему нейтральная Австрия поместила изваяние гигантского солдата едва ли не в самом центре столицы, они ответили, что после войны этого потребовал Советский Союз, заручившись также обещанием Австрии никогда его не убирать. На самом деле этот памятник защищен конвенцией, которую вместе с Советским Союзом подписали США и Австрия, когда советские войска вы-

27

Третья мировая воина: какой она будет?

водились из Австрии в 1950 году. В 1970-х жители Вены называли эту бронзовую громадину «единственным русским солдатом, который не насиловал наших женщин». Очевидно, эти статуи так же важны для русских, как для многих американских ветеранов, их семей и потомков священны заокеанские могилы соотечественников, погибших во время Второй мировой войны. Гигантские бронзовые монументы имеют важный смысл и для освобожденных, правда, смысл этот совершенно иной. Памятники и захороненные под ними тела красноармейцев служили символическими громоотводами. А в Таллинне такое сооружение привлекло кибермолнию.

Напряжение между этническими русскими, проживающими в Эстонии, и коренным населением страны стало расти с тех пор, как на исходе холодной войны страна объявила о своей независимости. Большинство эстонцев стремились избавиться от любых напоминаний о тех 50 годах, когда Эстония вынужденно входила в состав СССР. В феврале 2007 года законодатели выдвинули инициативу «Об устранении запрещенных строений», согласно которой необходимо было разрушить все, что связано с оккупацией, включая бронзового солдата. Эстонцев возмущал тот факт, что с приходом Красной Армии были осквернены могилы их собственных ветеранов.

Москва с недовольством заметила, что демонтаж бронзового солдата бесчестит героически погибших советских воинов, включая тех, кто похоронен под ним. Стремясь избежать инцидента, эстонский президент наложил вето на закон. Но давление общества, требовавшего демонтировать памятник, росло, а решимость русской этнической группы защищать, а эстонской — уничтожить монумент принимала все более воинственный характер. Вслед за промозглой балтийской зимой пришла весна, и политические страсти выплеснулись на улицы. В ночь на 27 апреля

ZB

Экспериментальные работы

2007 года, теперь называемую «бронзовой», у памятника произошло столкновение радикально настроенных представителей обеих этнических групп с полицией. Власти быстро вмешались и перенесли статую на новое охраняемое место на военном кладбище. Однако разногласия на этом не утихли, перенос памятника вызвал возмущеннопатриотический отклик московских СМИ и Думы — российской законодательной власти.

Именно тогда конфликт переместился в киберпространство. Эстония, как ни странно, является одной из самых «интернетизированных» стран мира и вместе с Южной Кореей существенно обгоняет Соединенные Штаты по широте использования Интернета в повседневной жизни. Такие достижения создают отличную мишень для кибератаки. После «бронзовой» ночи на серверы, поддерживающие самые популярные в Эстонии веб-страницы, обрушилась масса запросов, и в результате перегрузки некоторые из них вышли из строя. Другие были так заняты входящими пингами, что, по сути, оказались недоступными. Жители Эстонии не могли посещать веб-сайты газет, пользоваться услугами государственных электронных служб и банков.

Эстония столкнулась с DDoS-атакой. Как правило, DDoS-атака является незначительной помехой, а вовсе не главным кибероружием. По сути, это предварительно запрограммированный поток интернет-трафика, выводящий из строя или блокирующий сеть. Атака является распределенной в том смысле, что тысячи, даже сотни тысяч компьютеров включаются в процесс рассылки электронных запросов на несколько интернет-адресов. Атакованные компьютеры образуют ботнет (от (RO)BOT+ NET(WORK), роботизированная сеть) зомби-компьютеров под дистанционным управлением. Атакованный зомби-компьютер выполняет инструкции, загруженные

29

Третья мировая война: какой она будет?

в него без ведома владельца. На самом деле хозяева компьютеров могут даже не знать, что их компьютеры превратились в зомби и участвуют в DDoS-атаке. Пользователь в лучшем случае замечает, что его ноутбук работает чуть медленнее, а страницы открываются чуть дольше, чем обычно, и это единственный признак. Все злонамеренные действия происходят внутри, никак не отражаясь на экране монитора. Ваш компьютер прямо сейчас может быть частью ботнета.

Обычно все происходит так: за недели или месяцы до того, как ботнет переходит в наступление, пользователь заходит на некую совершенно безобидную на вид страницу, и с этой страницы загружается программа, превращающая компьютер в зомби. Или открывает электронное письмо своего знакомого, которое внедряет в компьютер программу зомбирования. Антивирусы или брандмауэр могут поймать и заблокировать заразу, но хакеры постоянно находят новые способы обойти защиту.

Иногда зомби-компьютер спокойно ждет команды. Иной раз он начинает искать другие компьютеры для атаки. Когда один компьютер заражает другие, а те делают то же самое, — работает так называемый вирус «червь», и заражение переходит с одного компьютера на тысячи и миллионы. Всего лишь за час инфекция может распространиться по всему миру.

Эстонская DDoS-атака стала самой крупной в истории. Заработало несколько разных ботнетов, и каждый охватывал десятки тысяч зараженных компьютеров. Сначала эстонцы подумали, что вывод из строя нескольких вебстраниц — дело рук раздраженных и возмущенных русских. Но затем ботнеты начали атаковать интернет-адреса, не известные большинству людей. Это были не общедоступные веб-страницы, а адреса серверов, управляющих телефонной сетью, системой верификации кредитных

за

Экспериментальные работы

карт, каталогами интернет-ресурсов. Потоки запросов на эстонские сайты стали поступать с более чем миллиона компьютеров. Hansapank, крупнейший банк в стране, не устоял. На всей территории нарушились торговля и связь, но атака не прекращалась.

Раньше один сайт мог подвергаться DDoS-атаке в течение нескольких дней. На этот раз все было иначе. Сотни важнейших сайтов страны подвергались атакам неделя за неделей и не могли вернуться в исходное состояние, предшествовавшее сбою. В то время как эксперты по компьютерной безопасности со всей Европы и Северной Америки устремились в Таллинн, Эстония обратилась в НАТО. Команда реагирования на инциденты попыталась принять контрмеры, которые в прошлом позволяли эффективно справляться с меньшими DDoS-атаками. Зомби легко адаптировались, возможно, перепрограммированные главными компьютерами. Атака продолжалась... С помощью специальной аппаратуры эксперты по кибербезопасности проследили за атакующими пингами и смогли поймать момент, когда зараженные машины «звонят домой» на главные компьютеры. Маршрут этих сообщений удалось проследить вплоть до управляющих компьютеров, а иногда и дальше, до управляющих устройств более высокого уровня. Эстония утверждала, что управляющие машины располагаются в России и что в программном коде использовалась кириллица.

Российское руководство с негодованием отвергло свою причастность к кибератаке на Эстонию. Кроме того, оно ответило отказом на официальный дипломатический запрос о содействии в отслеживании взломщиков, хотя по существующему двустороннему соглашению Москва должна была оказывать помощь. Проинформированные о том, что следы ведут в Россию, правительственные чиновники предположили, что, вероятно, российские патриоты, раз-

 з 1

Третья мировая война: какой она будет?

гневанные поступком Эстонии, взяли дело в собственные руки. Возможно, так и было.

Но даже если верить в теорию российских патриотов, без ответа остается вопрос, почему российское правительство не попыталось пресечь незаконную деятельность таких «комитетов бдительности». Никто ни на минуту не сомневался в том, что у преемников КГБ была возможность найти и заблокировать компьютеры виновных. Те, кто ближе знаком с современной Россией, предполагали, что дело не только в пассивности российских правоохранительных служб, закрывающих глаза на хулиганство националистически настроенной молодежи. Большинство опытных российских хакеров, за исключением тех, кто фактически работает на государство, в той или иной степени сотрудничают с организованной преступностью. Организованной преступности позволено процветать благодаря непризнаваемой связи со службами безопасности. В действительности различие между криминальной сетью и службами безопасности, которые контролируют большинство российских министерств и органов местного самоуправления, весьма размыто. Многие эксперты по России полагают, что некоторые высшие государственные должностные лица не препятствуют организованной преступности, получая свой «кусок пирога», или, как в случае с Эстонией, компенсацию за помощь в грязных делах. Помните слова дона Карлеоне из «Крестного отца»: «Когда-нибудь... а возможно, этот день и не наступит... я попрошу тебя оказать мне услугу».

После «бронзовой» ночи российские службы безопасности дали команду отечественным СМИ разжечь патриотические чувства против Эстонии. Несложно представить, что они попросили преступные группировки привлечь хакеров, возможно, даже снабдив их некоторой ценной информацией. Имеет ли российская госбезопас- 32

Экспериментальные работы

33

ность отношение к кибератаке в Эстонии? Возможно, стоит переформулировать вопрос. Они предложили провести атаку, способствовали ей, отказались расследовать дело и наказать виновных? Но, в конце концов, так ли это различие важно, если вы гражданин Эстонии, который не может снять свои деньги с карты банка Hansapank?

После этой кибератаки НАТО приняло решение создать центр киберзащиты. Он открылся в 2008 году в нескольких километрах от того места, где когда-то стоял бронзовый солдат, — теперь там растут молодые деревья. Увы, натовский центр в Таллинне мало помог, когда другая бывшая советская республика-сателлит, Грузия, и матушка-Россия схлестнулись в борьбе за небольшие спорные территории.

Грузия простирается вдоль побережья Черного моря, к югу от России. Более века эти страны пребывали в определенно непростых отношениях. Территория Грузии чуть меньше Южной Калифорнии, в стране проживает около четырех миллионов человек. В силу ее расположения и размера в Москве было принято считать, что страна входит в «сферу влияния» Кремля. Когда Российская империя после Октябрьской революции начала распадаться на части, грузины попытались отделиться и в 1918 году провозгласили независимость, пока русские воевали друг с другом. Но как только гражданская война в России прекратилась, победоносная Красная Армия вторглась в Грузию, установила марионеточное правительство и сделала ее частью Союза Советских Социалистических Республик. Советский режим сохранялся в стране вплоть до 1991 года, когда, воспользовавшись тем, что российское правительство опять погрязло в хаосе, Грузия объявила независимость.

Два года спустя Грузия утратила контроль над двумя территориями — Южной Осетией и Абхазией. Поддержи- [[5]](#footnote-6)

Третья мировая война: какой она будет?

ваемое Москвой местное русское население сумело одержать победу над разрозненной грузинской армией и изгнало большую часть грузинского населения. Затем были выбраны «независимые» правительства. Несмотря на то что эти регионы всем остальным миром считались частью Грузии, они рассчитывали на финансирование и защиту со стороны России. В июле 2008 года южноосетинские повстанцы (или российские агенты, в зависимости от того, какой версии событий вы придерживаетесь) спровоцировали конфликт с Грузией, начав ракетную атаку на несколько грузинских сел.

Грузинская армия, как и следовало ожидать, ответила на ракетный удар по своей территории бомбардировкой столицы Южной Осетии. Впоследствии 7 августа Грузия оккупировала регион. Не удивленные таким поворотом событий, российские войска на следующий день ввели свои подразделения, быстро изгнав из Южной Осетии грузинскую армию. В тот же момент, когда российские войска выдвинулись на позиции, подключились и кибервоины. Их целью было не дать жителям Грузии узнать, что происходит, поэтому они атаковали сайты грузинских СМИ и правительства. Доступ Грузии к сайтам CNNи ВВС был также заблокирован.

В реальном мире Россия также бомбардировала Грузию и захватила небольшую часть грузинской территории, до этого не считавшуюся спорной, якобы для создания буферной зоны. Пока грузинская армия отступала из Осетии, повстанческие группировки в Абхазии решили воспользоваться ситуацией и с незначительной помощью российских покровителей выставили всех грузин. Российские войска в качестве дополнительного буфера прихватили еще один участок грузинской территории. Спустя пять дней бои практически прекратились. Президент Франции Николя Саркози выступил посредником

34

Экспериментальные работы

в подписании мирного договора, в соответствии с которым Россия обязалась немедленно вывести войска и покинуть спорные территории, как только международные миротворческие силы прибудут для обеспечения безопасности. Эти силы так и не прибыли, и за несколько недель Россия признала Южную Осетию и Абхазию независимыми государствами. Независимые государства сразу пригласили своих российских покровителей остаться.

Для американского большинства, за исключением кандидата в президенты Джона Маккейна, который старался представить происшедшее кризисом национальной безопасности Америки, события в Грузии казались далекими и маловажными. Как только американцы убедили себя в том, что новостные репортажи о вторжении в Грузию не означают, что российские войска или генерал Шерман снова наступают на Атланту[[6]](#footnote-7), они просто перестали обращать на них внимание. Но истинное значение этого события, помимо того что оно продемонстрировало отношение российских лидеров к своей бывшей территории, заключается в демонстрации их отношении к использованию кибератак. Прежде чем война вспыхнула в реальности, грузинские правительственные сайты подверглись нападению. На начальных этапах была организована стандартная DDoS-атака на официальные сайты грузинского руководства и веб-сервер президентского сайта. Чтобы вывести его из строя, на него добавили картинки, сравнивавшие грузинского лидера Михаила Саакашвили с Адольфом Гитлером. Поначалу это казалось банальной,

Третья мировая война: какой она будет?

даже детской выходкой. Затем, по мере того, как разворачивались военные действия на земле, кибератаки стали более интенсивными и изощренными.

Доступ Грузии в Интернет осуществляется через Россию и Турцию. Большая часть маршрутизаторов в России и Турции, через которые проходит грузинский трафик, подверглась таким массированным атакам, что исходящий поток блокировался. В результате жители Грузии не могли пользоваться внешними новостными или информационными ресурсами и отправлять электронную почту за пределы страны.

Грузины попытались защитить свое киберпространство и воспрепятствовать DDoS-атакам обходными маневрами. Русские отвечали на каждый их ход. Грузия пыталась заблокировать трафик, идущий из России, — русские изменили маршрут, и атаки приняли вид пакетов из Китая. Кроме располагавшегося в Москве головного компьютера, управляющего всеми ботнетами, использовались серверы Канады, Турции и Эстонии.

Грузия перенесла веб-страницу президента на калифорнийский сервер. Русские создали несколько клонов президентского сайта и перенаправили трафик туда.

Грузинские банки выключили свои серверы и решили переждать атаку, рассудив, что лучше временная приостановка банковского обслуживания в оперативном режиме, чем риск хищения важнейших данных или повреждения внутренних систем. Русские, не способные добраться до грузинских банков, стали рассылать со своих ботнетов огромные потоки информации в международную банковскую систему, симулируя кибератаки из Грузии. Атаки вызвали автоматическую ответную реакцию большинства иностранных банков, и связь с грузинским банковским сектором прекратилась. Без доступа к европейским банковским системам грузинские банки оказались

36

Экспериментальные работы

парализоваными. Вышла из строя система кредитных карт, а вслед за ней и система мобильной связи.

Кульминационной стала DDoS-атака шести ботнетов, которые использовали компьютеры ничего не подозревавших интернет-пользователей и волонтеров, загрузивших программу для взлома с нескольких антигрузинских веб-сайтов. После установки такой программы доброволец вступал в кибервойну, просто нажав кнопку StartFlood.

Как и в случае с Эстонией, российское правительство заявило, что кибератаки были реакцией населения, неподконтрольного Кремлю. Однако группа западных IT- специалистов пришла к выводу, что веб-сайты, использованные для запуска атак, были связаны с российскими разведывательными службами. Уровень скоординированности, продемонстрированный в атаках, и финансовая поддержка позволяют предположить, что здесь замешаны не обычные пользователи, движимые патриотическим порывом. Даже если верить российскому правительству (например, заявлению о том, что кибершторм, обрушившийся на Грузию, как и в прошлый раз на Эстонию, не был делом государственных служб), очевидно, что правительство не предприняло никаких попыток прекратить эту акцию. В конце концов, огромная советская разведывательная служба — КГБ — до сих пор живет и здравствует, хотя называется по-другому и имеет несколько иную структуру. На самом деле могущество КГБ лишь возросло за время правления Владимира Путина. Любая сколько-нибудь масштабная киберактивность в России, будь ее источником правительство, криминальные круги или обычные граждане, возможна лишь с одобрения службы госбезопасности и ее боссов в Кремле.

Если все было так, как мы предполагаем, то российское правительство, по сути, попросило добровольцев наказать Эстонию с помощью кибератак, а затем воспользовалось

37

Третья мировая война: какой она будет?

тем же методом в дополнение к классическим военным действиям в Грузии. Но эти действия не характеризуют реальные возможности российских вооруженных сил и разведслужбы в случае реальной атаки в киберпространстве. Русские, в сущности, продемонстрировали некоторую сдержанность в использовании кибероружия против Эстонии и Грузии. Возможно, они приберегают лучшие средства на случай экстренной необходимости, для конфликтов с участием НАТО и США.

Долгие годы руководители разведслужбы США полагали, что использовать кибероружие, даже в таких скоромных масштабах, как в случаях с Эстонией и Грузией, способны Россия, Китай, Израиль и, разумеется, Соединенные Штаты. Но летом 2009 года в числе этих стран совершенно неожиданно оказалась еще одна. Все произошло в последний понедельник мая 2009 года. Вечером, в начале восьмого, на подъездной дороге к аэропорту Даллеса (штат Вирджиния) постепенно рассасывалась пробка. В располагавшемся неподалеку офисе Геологической службы США зафиксировали землетрясение амплитудой 4,7 балла, которое произошло в Азии. Специалисты начали рассчитывать положение его эпицентра. Оказалось, что он находится в северной части Корейского полуострова, в 70 километрах от города Кимчхэк. Подобное событие было зафиксировано в октябре 2006 года в том же месте. Как позже выяснилось, оба случая были вызваны ядерны- ми испытаниями.

После многолетних переговоров с США, Китаем и Россией правительство Северной Кореи, странное и закрытое, решило манкировать международным давлением и провести ядерные испытания во второй раз. Первую попытку, предпринятую тремя годами ранее, некоторые западные наблюдатели охарактеризовали как «частичное фиаско». На протяжении нескольких часов после второго взрыва

3S

Экспериментальные работы

Сьюзен И. Райс, представитель США в ООН, не отходила от телефона в номере нью-йоркской гостиницы «WaldorfTowers». Она совещалась с Белым домом и Госдепартаментом, а затем стала обзванивать представителей других стран, в первую очередь Японии и Южной Кореи. Южная Корея, в лице генерального секретаря Пан Ги Муна, возглавляющего ООН, согласилась на экстренное совещание Совета безопасности. Итогом этого спонтанного собрания стало международное осуждение и очередные санкции. Полтора десятилетия попыток предотвратить развитие ядерного потенциала Северной Кореи дипломатическими средствами не дали результата. Почему?

Некоторые эксперты объясняли, что у нищего Севера нет других рычагов для получения льготных займов, бесплатной еды и дешевого топлива. Пхеньяну приходилось снова и снова продавать обещание не развивать далее ядерный потенциал страны. Другие указывали на слухи о нездоровье загадочного «Великого руководителя» Ким Чен Ира, лидера Корейской Народно-Демократической Республики. Умевшие гадать по чайным листьям верили: «Великий руководитель» знал о том, что дни его сочтены, и выбрал своим преемником третьего сына, двадцатипятилетнего Ким Чжон Ына. Чтобы не дать Соединенным Штатам или Южной Корее воспользоваться этим переходным периодом, заявляли аналитики, Северная Корея решила побряцать оружием, хотя бы атомным, чтобы напугать, привлечь внимание, дать понять, какие ужасы могут случиться, а затем пойти на переговоры и, в конечном счете, пополнить казну.

Если расчет был на то, что США и другие страны после взрыва поспешат «завалить» Северную Корею пшеницей и нефтью, он не оправдался. Руководство США, выразив неодобрение и объявив о размещении ракет на Гавайях, уже в июне вновь сосредоточилось на реформе

39

Третья мировая война: какой она будет?

здравоохранения, Афганистане и бичевании собственной разведки. Кто-то из американских чиновников открыто заявил, что США собирается провести «Кибершторм» — учения с целью проверки уровня защиты компьютерных сетей. В учениях 2009 года планировали принять участие Япония, Южная Корея и другие страны. Северокорейские СМИ быстро отреагировали, назвав планируемые учения прикрытием для вторжения в их страну. Такого рода параноидальные умозаключения очень характерны для северокорейского режима. Никто в Вашингтоне не обратил на них особого внимания.

После 4 июля чиновники разъехались из Вашингтона в отпуска на пляжи Восточного побережья. Туристы устремились в NationalMall[[7]](#footnote-8), где многотысячные толпы наблюдали красные всполохи фейерверка, традиционно устраиваемого на День независимости. На противоположной стороне земного шара ракеты также запускались не впустую. Американский спутник обнаружил пуск ракет из Северной Кореи, а в вычислительном центре в Колорадо быстро определили, что ракеты были малой дальности и их цель находилась в море. Затем произошел второй запуск. Затем еще и еще. Семь северокорейских ракет ознаменовали День независимости США. Было это требованием помощи или демонстрацией силы, но все происходившее казалось вызовом. И этим все не закончилось. Действия переместились в киберпространство.

Накануне праздника 4 июля северокорейские спецслужбы разослали кодированное сообщение на 40 тысяч компьютеров, объединенных в ботнет. В сообщении содер-

Экспериментальные работы

жался простой набор команд, в соответствии с которыми компьютеры начинали посылать запросы на ряд американских и южнокорейских правительственных и коммерческих веб-сайтов. Каждый инфицированный компьютер при включении присоединялся к атаке. Пользователь ком- пьютера-зомби мог разве что обратить внимание, что процессор работает медленнее, а интернет-запросы выполняются несколько дольше обычного, и больше ничего. Да, это была еще одна DDoS-атака зомби, объединенных в ботнет. В какой-то момент во время праздника в американском правительстве заметили, что сойты dhs.govи state.govстали временно недоступны. Если бы кто-нибудь захотел проверить уровень террористической угрозы перед тем, как отправиться полюбоваться фейерверком, сделать это на сайте Министерства внутренней безопасности было невозможно.

Каждый зомби-компьютер направил множество запросов на эти сайты и атаковал систему, нарушая нормальное обслуживание пользователей.

На американские веб-сайты обрушивался миллион запросов в секунду. Сайты Министерства финансов, Секретной службы (SecretService), Федеральной комиссии по торговле и Министерства транспорта в период с 4 по 9 июля на какое-то время выходили из строя. NASDAQ, Нью-Йоркская товарная и Нью-Йоркская фондовая биржи подверглись атаке, как и «Вашингтон пост». Однако DDoS-атака на Белый дом провалилась. Первой DDoS- атаки на Белый дом удалось избежать, поскольку мы с компанией Akamaiорганизовали трафик так, что запросы пользователей направлялись на один из 20 тысяч серверов, разбросанных по всему миру. Атака 2009 года коснулась лишь компьютеров, расположенных рядом с источником. Поэтому проблемы возникли лишь на сайтах Белого дома, размещенных в Азии. Ник Шапиро, пред-

Третья мировая война: какой она будет?

ставитель Белого дома, без особого энтузиазма извинился перед азиатскими пользователями, которые не могли попасть на сайт Белого дома. Затем пришли вторая и третья волны атаки.

1. июля 30~60 тысяч компьютеров, зараженных различными разновидностями вируса, атаковали сайты правительства Южной Кореи, корейские банки и службы компьютерной безопасности. Очевидно, взломщики были убеждены, что атаки на американские сайты бессмысленны, после того как правительство и крупнейшие корпорации начали сотрудничество с интернет-провайдерами, чтобы отфильтровывать запросы взломщиков.
2. июля в шесть часов вечера по корейскому времени началось последнее нападение. На сайты южнокорейских банков и правительственных учреждений обрушились запросы со 166 тысяч компьютеров из 74 стран мира. Но в конечном счете атака была остановлена. Взломщики не пытались взять под контроль какие-либо государственные системы или нарушить деятельность важнейших служб.

Это было, скорее всего, только предупреждение. Нам известно, что у этой атаки имелся и план, и движущая сила. Это был не просто «червь», распространяющийся по всему Интернету. Кто-то направлял атаку, изменял список целей, чтобы сосредоточиться на более уязвимых южнокорейских сайтах.

Американское правительство не стало приписывать атаку Северной Корее, хоть Южная Корея не постеснялась это сделать. Выбор времени позволяет считать северокорейский режим главным подозреваемым, но точно установить виновника сложно. Зараженные компьютеры пытались связаться с одним из восьми главных серверов каждые три минуты. Серверы, в свою очередь, рассылали команды на компьютеры-зомби, указывая, какие сай-

42

Экспериментальные работы

ты атаковать. Восемь главных серверов располагались в Южной Корее, Соединенных Штатах, Германии, Австрии и, что интересно, в Грузии. Южнокорейская комиссия подтвердила выводы вьетнамской компании BachKhoaInternetworkSecurity(BKIS)о том, что все эти серверы управлялись с компьютера, который находился в английском Брайтоне. Далее следы теряются, хотя трудно представить, что вдохновитель атаки сидел за ноутбуком где-нибудь на пляже. Разведслужба Южной Кореи (NIS) полагает, что северокорейский Институт военных исследований участвовал в попытке вывести из строя коммуникационную инфраструктуру страны. Сразу после инцидента представители NISзаявили, что у них имеются улики, указывающие на Северную Корею. Они утверждали, что северокорейское объединение хакеров, так называемый отдел 110, или группа технологической разведки, 7 июня получило заказ на подготовку кибератаки. Согласно этому плану, группа должна была «за минуту разрушить марионеточную коммуникационную сеть Южной Кореи». Заказ последовал за решением Южной Кореи принять участие в учениях «Кибершторм», которые Северная Корея назвала «недопустимой провокацией, разоблачающей стремления завоевать КНДР».

Теперь Южная Корея готовится к полномасштабной кибервойне. Как раз накануне атак Южная Корея объявила о планах к 2012 году учредить новое подразделение, занимающееся киберборьбой. Позднее сроки были перенесены на январь 2010 года. Но что будет делать командование этого нового штаба в случае новых атак в киберпространстве со стороны Северной Кореи, непонятно.

Если Северная Корея снова перейдет в кибернаступление, выбор ответных действий невелик. Ужесточать санкции больше просто некуда. Продовольственная помощь уже приостановлена. О любых военных ответных

43

Третья мировая война: какой она будет?

действиях не может быть и речи. 23 миллиона сеульцев живут в пределах досягаемости северокорейской артиллерии, не говоря уже о демилитаризированной зоне, которую военные именуют не иначе как «коробка смерти».

Ответить такими же действиями практически невозможно, поскольку в Северной Корее практически нет ресурсов, которые могли бы атаковать кибервоины из США или Южной Кореи. В 2002 году Дональд Рамсфелд и другие должностные лица из администрации Буша поддержали идею вторжения в Ирак, поскольку Афганистан не являлся «богатой на мишени» средой — там было мало боевой техники, военных баз и основных коммуникаций, по которым могли бы нанести удар американцы. Северная Корея в компьютерном отношении является эквивалентом Афганистана.

На сайте Nightearth.comможно посмотреть подборку фотографий поверхности Земли, снятых со спутника ночью. Из них составлена карта нашей ярко освещенной планеты, и Южная Корея кажется светлым островом, отделенным от Китая и Японии морем. Темная часть Корейского полуострова к северу от Сеула похожа на море. Северная Корея вряд ли сильно зависит от электросети. Мобильные телефоны есть всего лишь у 20 тысяч человек из 23-миллионного населения. Радио и телевидение транслируют исключительно официальные государственные каналы. Что до Интернета, то, как написала в 2006 году NewYorkTimes, Северная Корея по-прежнему остается «черной дырой». TheEconomistсчитает, что эта страна «почти так же отрезана от виртуального мира, как от реального». В Северной Корее существует около 30 веб-сайтов для связи с внешним миром, которые большей частью занимаются пропагандой, нацеленной на ее южного соседа. В нескольких «западных» отелях разрешено использование спутниковой связи, а несколько удачливых граждан стра-

44

Экспериментальные работы

ны имеют ограниченный доступ к внутренней сети и могут попасть на сайт «Великого руководителя», но почти никуда больше.

Северная Корея немного вложила в развитие своей интернет-инфраструктуры, но немало инвестировала в разрушение инфраструктуры других стран. Отдел 110 — подразделение, которое подозревают в организации июльской атаки, — является составной частью одной из четырех военных структур Северной Кореи. Более шестисот хакеров числятся в 121-м отделе Объединенного комитета по компьютерной войне Корейской народной армии. В секретном отделе, занимающемся кибер- и психологической войной, работают сто хакеров и специалистов по информационным войнам. 35-й департамент Центрального партийного отдела расследований — самое малое по численности, но самое квалифицированное подразделение, которое занимается вопросами как внутренней безопасности, так и внешних кибернаступлений. 121-й отдел — самое многочисленное и, по словам одного служившего там хакера, перешедшего в лагерь противника в 2004 году, самое подготовленное подразделение. Его сотрудники специализируются на выводе из строя военных, управленческих и коммуникационных сетей Южной Кореи. Филиалы этого подразделения расположены в Китае, поскольку подключения к Интернету с территории Северной Кореи весьма малочисленны и их легко идентифицировать.

Неясно, известно ли официальному Пекину о деятельности спецслужб КНДР на территории страны, но кое-что точно ускользает от глаз китайской тайной полиции, особенно в Интернете. Как сообщают, одно из подразделений северокорейской службы кибербезопасности располагается в отеле «Шанхай» в китайском городе Даньдун, у северокорейской границы. Четыре этажа здания занимают специалисты 110-го отделения. Еще одно подразделение

лъ

Третья мировая война: какой она будет?

размещается в городе Саньян, где, по имеющимся данным, северокорейским агентам сдается несколько этажей гостиницы «Myohyang» («Загадочная душистая гора», в честь которой был назван отель, находится на территории Северной Кореи). Агентов обнаружили, когда они протягивали оптоволоконные кабели и устанавливали новейшее оборудование. В общей сложности в КНР может работать от шестисот до тысячи агентов отдела по кибербезопасности во главе с командующим в ранге подполковника. В северокорейских начальных школах отбираются лучшие ученики, из которых выращивают хакеров. В школе их учат разбираться в программировании и компьютерном аппаратном обеспечении, после чего они зачисляются в Университет автоматизации управления в Пхеньяне, где их обучают тому, как взламывать вражеские компьютерные системы. Сейчас здесь обучается около семисот студентов, для которых регулярно проводятся учения. Часть студентов для овладения новейшими технологиями тайно отправляют в Японию.

Июльская атака 2009 года не стала разрушительной, но продемонстрировала невероятную изощренность. Тот факт, что нападение было управляемым, косвенно подтверждает квалификацию взломщиков. Атака продлилась несколько дней, и это является доказательством того, что вирус распространялся из нескольких источников. Данная особенность позволяет предположить, что нападение не было делом рук бездельничающих подростков. Конечно, Северная Корея позаботилась о том, чтобы заронить сомнения в своей виновности. В ходе расследования выяснилось, что программа использовала корейский браузер, а следовательно, ее создание можно приписать и южнокорейским хакерам, где Интернет распространен гораздо шире. Однако экспертов несколько озадачил тот факт, что авторы кода не пытались скрыть свое корейское

46

Экспериментальные работы

происхождение. Человек, способный написать такой код, вполне способен и замести следы. А значит, заказчики кода намеренно стремились оставить улику. Правительство Южной Кореи и многие аналитики из Соединенных Штатов сделали вывод, что атаку заказал «Великий руководитель», чтобы продемонстрировать мощь своей страны в киберпространстве так же, как использовал ракеты в небе.

Послание гласило: «Я все еще у руля и могу создавать проблемы, мое оружие лишит вас превосходства». Отправив такое сообщение, северокорейские дипломаты через несколько недель предложили альтернативу. Они готовы были пойти на переговоры и даже освободить двух американских заключенных. Вскоре Билл Клинтон, прямо как в сцене из кинофильма «Отряд Америка: всемирная полиция», сел за стол переговоров с «Великим руководителем». Но в отличие от куклы, изображавшей Ханса Бликса — инспектора ООН по ядерному оружию, Клинтон не провалился в бассейн с акулами, хотя Северная Корея подготовила такие «люки» в компьютерных сетях по меньшей мере двух континентов. Спустя месяц после июльского происшествия аналитики Пентагона пришли к выводу, что возможной целью северокорейских DDoS-атак было определить, достаточен ли уровень активности ботнетов в Южной Корее, чтобы блокировать маршрутизаторы и оптоволоконные кабели, идущие из страны. Если бы северокорейские агенты смогли «зафлудить» соединение, они легко сумели бы отрезать страну от киберпространства всего остального мира. Это может пригодиться в кризисной ситуации, поскольку США координируют перемещение любых американских военных подразделений через Интернет.

Подготовка Северной Кореи к битве на киберполе продолжается. В октябре, спустя три месяца после DDoS- 47

Третья мировая война: какой она будет?

атаки, южнокорейские СМИ сообщили, что хакеры просочились в CARIS(ChemicalsAccidentResponseInformationSystem — информационная система ответного реагирования на химическую опасность) и извлекли секретную информацию о 1350 опасных химических препаратах. Хакеры, предположительно из Северной Кореи, получили доступ к системе, введя код через компьютер южнокорейского армейского офицера. Потребовалось семь месяцев, чтобы обнаружить факт нападения. Теперь Северная Корея знает, где и как Южная Корея хранит опасные газы, в том числе хлор, используемый для очистки воды. Если хлор попадет в атмосферу, он приведет к смерти от удушья, как было происходило на полях сражения Первой мировой войны.

Кибервоины и большинство средств массовой информации считают эти события первыми официальными столкновениями государств в киберпространстве. Есть и другие примеры, включая операции, проведенные Китаем, Тайванем, Израилем и другими странами. Эстонский инцидент некоторые аналитики назвали Первой сетевой войной.

Их оппоненты не спешат рассматривать эти и другие недавние происшествия как новую форму ведения войны. Израильскую атаку они считают чем-то вроде глушения радиоэфира, тем, что так или иначе осуществляется уже на протяжении полувека. Американские действия в Ираке этим скептикам кажутся раздутыми пропагандой. В российских и северокорейских акциях они усматривают лишь попытку досадить и навредить.

Конечно, жители Сирии, Ирака, Эстонии, Грузии и Южной Кореи не считают эти события неприятностями, и я склонен согласиться с ними. Я привожу эти недавние и хорошо известные примеры киберстолкновений, чтобы продемонстрировать, что конфликты между государства- 4S

Экспериментальные работы

ми переместились в киберпространство. Кроме того, данные события позволяют сделать еще пять выводов.

Кибервойна реальна. События, рассмотренные нами, не отражают истинного масштаба того, что может произойти. В большей части широко известных перестрелок в киберпространстве использовалось только примитивное кибероружие (за исключением израильской операции). Логично предположить, что взломщики не хотят раскрывать более изощренные возможности. То, что США и другие страны способны сделать в киберпространстве, может уничтожить современное государство.

Кибервойна развивается со скоростью света. Поскольку фотоны атакующего пакета передаются по оптоволоконному кабелю невероятно быстро, промежуток времени между началом атаки и ее последствиями едва ли поддается оценке, что создает дополнительные риски для лиц, принимающих решения в критический момент.

Кибервойна глобальна. При любом конфликте кибератаки способны захватить весь мир, поскольку участвующие в них компьютеры и серверы могут находиться в любой части планеты. Значит, в войну мгновенно вовлекаются разные государства.

Кибервойна охватывает все сферы. Системы, которыми мы располагаем, от банков до радаров противовоздушной обороны, доступны из киберпространства, их легко можно захватить или вывести из строя, и для этого не нужно опротиводействовать традиционным системам обороны страны.

Кибервойна уже началась. Ожидая нападения, государства готовятся к битве. Они проникают в сети и инфра- 49

Третья мировая война: какой она будет?

структуры, припасают «черные ходы» и логические бомбы, и делают это уже сейчас, в мирное время. Грань между миром и войной оказывается размытой — вот новый опасный источник нестабильности.

Как мы увидим в последующих главах, есть все основания полагать, что будущие наступательные войны станут дополняться кибернетическими, в то время как кибервойны будут вестись и сами по себе, без взрывов, пехоты, авиации и флота. Но полномасштабных кибервойн, в которых сильнейшие в этом виде войны государства использовали бы свое лучшее оружие, пока не было. Поэтому мы еще не знаем ни потенциального победителя, ни возможных результатов, ни последствий.

В этой книге мы разберемся, почему непрогнозируе- мость, связанная с полномасштабной кибервойной, означает высокую вероятность того, что военное равновесие в мире изменится, а политические и экономические отношения коренным образом преобразятся. Кроме того, мы найдем способы уменьшить эту непрогнозируемость.

Глава 2

**Кибервоины**

В

 США можно было увидеть рекламный ролик: коротко стриженный молодой человек в комбинезоне парашютиста идет по тускло освещенному центру управлении, переговариваясь с подчиненными, на лицах которых мерцают зеленоватые блики от светящихся мониторов. За кадром слышится голос: «...контроль систем управления... систем водоснабжения... это новое поле битвы... здесь будет территория войны... здесь будут вестись главные сражения». Затем мужчина смотрит в камеру и произносит: «Я капитан Скотт

Третья мировая война: какой она будет?

Хинк, кибервоин военно-воздушных сил». Экран темнеет, и на нем появляются три слова: «Воздух. Пространство. Киберпространство». Затем, когда реклама заканчивается, мы видим крылатую эмблему и самого рекламодателя: «Военно-воздушные силы Соединенных Штатов».

Итак, теперь мы знаем, как выглядят кибервоины. Скотт — красивый, стройный, честный офицер, каких большинство в самых могущественных вооруженных силах планеты. Конечно, его образ не вполне совпадает с нашими представлениями о хакерах — прыщавых растрепанных парнях в толстых очках. Чтобы привлечь людей, обладающих необходимыми навыками для ведения кибервойн, военно-воздушные силы, кажется, решили, что им позволено изменить правила. «Пусть они не могут пробежать три мили с рюкзаком за спиной, зато способны вывести из строя систему SCADА[[8]](#footnote-9), — размышляет генерал-майор военно-воздушных сил Уильям Лорд. — Нам нужно создать культурную среду, в которую они смогут встроиться». Такое прогрессивное отношение отражает сильное желание ВВС США играть главную роль в кибервойне. Именно они впервые создали организацию для ведения боевых действий в новом пространстве — Киберуправление ВВС США.

Сражение за кибервойну

В октябре 2009 года за ВВС последовал и флот, организовав собственный отдел кибербезопасности. Создается

Кибервоины

впечатление, что американские вооруженные силы только теперь начали интересоваться кибервойной, вступив в игру довольно поздно. Но это не так. Министерство обороны США «изобрело» Интернет, и возможности использования его в военных целях не оставались без внимания даже в те далекие дни. Как уже отмечалось в первой главе, первые кибервоины планировали использовать во время войны в Персидском заливе кибероружие, чтобы разрушить систему противовоздушной обороны Ирака. Вскоре после «Бури в пустыне» ВВС США создали специальный Центр военной информации. В 1995 году Университет национальной обороны подготовил первый выпуск офицеров, обученных вести кибервоенные кампании. В 1990-х не все военные понимали, что значит кибервойна, и считали ее частью информационной, психологической войны, связывая с операциями по психологическому воздействию на противника. Другие представители разведслужб считали расширяющуюся сеть Интернет золотым дном для электронного шпионажа. Становилось все очевиднее: если вы способны проникнуть в сеть, чтобы собрать информацию, несколько нажатий клавиш могут вывести эту сеть из строя... По мере того как сотрудники электронной разведки все больше осознавали этот факт, перед ними возникала сложная проблема. Парни из разведки знали, что если они скажут «операторам» (боевым подразделениям), что в Интернете можно вести войну нового типа, они утратят контроль над киберпространством, который перейдет к воинам. С другой стороны, воинам, действуя в киберпространстве, по-прежнему приходилось полагаться на «ботаников» из разведки. Более того, возможности киберпространства позволяли легко нанести существенный урон врагу, и такой шанс нельзя было упускать. Постепенно воины осознали, что и «ботаники» кое на что сгодятся.

53

Третья мировая война: какой она будет?

Ко второму президентскому сроку Джорджа Буша важность кибервойны стала очевидной Пентагону, и военно-воздушные силы, флот и разведывательные органы затеяли отчаянную борьбу в стремлении играть лидирующую роль в новом пространстве военных действий. Некоторые ратовали за создание объединенного командования всех трех служб в рамках одной интегрированной структуры, ставя в пример объединенные командования по транспорту, стратегическому ядерному вооружению и по каждому региону военных действий. Когда в 1980-х годах казалось, что важную роль будут играть космические войска, Пентагон создал соответствующее объединенное командование, считая, что это пространство должны контролировать Соединенные Штаты. Объединенное космическое командование вооруженных сил США существовало с 1985-го по 2002 год, до тех пор, пока не стало очевидно, что ни у правительства США, ни у других стран нет средств на ведение масштабных военных действий в космосе. Космическое командование влилось в стратегическое командование (STRATCOM), управляющее стратегическими ядерными силами. В 2002 году кибервойна перешла в ведение STRATCOM, штаб-квартира которого находится на авиабазе в Небраске. Военно-воздушным силам предписано было руководить действующими боевыми частями. Создание Киберкомандования ВВС США и важность киберпространства, продемонстрированная в рекламной кампании по привлечению добровольцев в ряды военно-воздушных сил, вызвали раздражение других служб и многих сотрудников Пентагона.

Некоторых беспокоило то, что ВВС слишком открыто говорят о том, что, по их мнению, должно храниться в тайне — о самом существовании кибервойны. Глава ВВС США публично заявил: «Пусть страна знает — пришла эпоха кибервойн». Да еще злосчастная реклама, пугаю-

54

Кибервоины

щая блэкаутом (крахом энергосистемы страны). В другом ролике показывался Пентагон и утверждалось, что он подвергается атаке в киберпространстве по миллиону раз в день, но защищается такими доблестными воинами, как геройский сержант ВВС, сидящий за компьютером. Добавьте бесконечные интервью с руководителями ВВС, которые не скрывали своих решительных намерений. «Наша цель — контролировать киберпространство, занимаясь как обороной, так и нападением», — признавался генерал- лейтенант Роберт Элдер. Руководитель оперативной группы по операциям в киберпространстве высказался столь же откровенно: «Нельзя только обороняться в киберпространстве. Если вы не доминируете в киберпространстве, вы не можете доминировать в других областях».

К 2008 году все в Пентагоне убедились в важности кибервойны, а также в том, что ею не должны заниматься только ВВС. В принципе, все были согласны на создание объединенной структуры, но боялись снова совершить ошибку «Космического командования». Вдруг войны в киберсфере окажутся чем-то столь же преходящим, как космические. Альтернативой было создание объединенного командования, подчиненного STRATCOM(Стратегическое командование США) хотя бы на бумаге. ВВС тогда прекратили бы считать себя главными, им пришлось бы довольствоваться более скромным положением.

У разведки имелись свои соображения. После реорганизации 11 сентября 2001 года все 18 подразделений управляются одним человеком. В 2008 году главой разведки стал Майк Макконел. Слегка сутулый, в очках с толстыми стеклами и мягким голосом, он выглядел как преуспевающий бизнесмен с Уолл-стрит. Макконел пришел в разведку из консалтингового консорциума BoozAllenHamilton.Он отказался от традиционной карьеры в Booz. Большую часть жизни Макконел служил в военно-мор-

55

Третья мировая война: какой она будет?

ской разведке и ушел в отставку трехзвездным генералом Агентства национальной безопасности (NationalSecurityAgency, NSA).

Если послушать, как Макконел или его преемник генерал ВВС Кен Минихэн говорят о АНБ, вы начнете понимать, почему они считают, что передать часть их полномочий другим глупо и практически нереально. Они подчеркивают, что АНБ имеет огромный опыт, поскольку десятилетиями «делало невозможное» в сфере электронного шпионажа. Роль АНБ в киберпространстве следует из его традиционной задачи — прослушивать радиосигналы и телефонные разговоры. Интернет является всего лишь еще одним средством массовой информации. Распространенность Интернета растет, так же как и заинтересованность в нем АНБ. АНБ, в котором трудятся доктора наук и инженеры-электронщики, постепенно становится ведущим мировым центром исследования киберпространства.

Хотя АНБ не обладает полномочиями вести какую-либо подрывную деятельность, оно основательно внедрено в интернет-инфраструктуру за пределами США с целью шпионажа.

Когда в 1996 году Макконел ушел из АНБ в BoozAllenHamilton,он продолжил заниматься проблемами Интернета, помогая ведущим американским компаниям решать задачи кибербезопасности. По возвращении в разведывательный бизнес в 2007 году он, будучи вторым человеком в национальной разведке, попытался получить власть над всеми разведывательными службами США, включая ЦРУ. От этого пострадала его давняя дружба с Майком Хейдэном (директором ЦРУ). Хейдэн когда-то тоже возглавлял АНБ. На протяжении почти всей службы в ЦРУ он оставался четырехзвездным генералом ВВС США.

Поскольку оба Майка (и Макконел и Хейдэн) имели отношение к АНБ, они были единогласны по меньшей

56

КИБЕРВОИНЫ

мере в одном вопросе — любое новое Киберкомандование не должно пытаться взять на себя полномочия, десятилетиями принадлежавшие АНБ. Если что-то и нужно предпринять, полагали они, как и многие другие выходцы из АНБ, так это просто превратить АНБ в Киберкомандование. Их мнение имело вес в Пентагоне, поскольку они, до определенной поры, знали о киберпространстве больше остальных. Чтобы воспрепятствовать АНБ в «захвате Киберкомандования», некоторые военные заявили, что АНБ на самом деле является гражданской организацией, одним из отделов разведовательного управления и поэтому по закону не может вести военные действия. Они ссылались на законы США, в которых прописаны полномочия и ограничения различных правительственных ведомств и агентств. Конечно, законы можно поменять. И тем не менее вопрос, кто будет руководить кибервойнами Америки, стал предметом ожесточенных дискуссий между военными и гражданскими специалистами по правовым аспектам правительственной деятельности.

В любом другом случае исход дела, скорее всего, решился бы в пользу военных и возникла бы совершенно новая организация, принявшая на вооружение хакерский опыт АНБ. Однако в 2006 году министр обороны Дональд Рамсфелд, пытавшийся расширить сферу своего влияния, после провала на выборах, отчасти вызванного неэффективностью ведения войны в Ираке, был вынужден оставить пост. На место Рамсфелда пришел Роберт Гейтс (президент Техасского университета А&М). На тот момент я знал его уже три десятка лет и ожидал, что он станет хорошим министром обороны. Он не был ни выходцем из Пентагона, ни новичком в сфере госбезопасности из академической или промышленной среды, которыми обычно легко манипулируют опытные сотрудники Пентагона. Боб был офицером ЦРУ, который дослужился до поста дирек-

57

Третья мировая война: какой она будет?

тора, побывав до этого в Совете национальной безопасности. Гейтс наблюдал за дебатами о Киберкомандовании с позиции представителя разведывательного сообщества и, что еще важнее, с высокого поста сотрудника Белого дома. Когда вы работаете в команде президента, кто бы им ни был в данный момент, вы понимаете, что интересы страны превыше интересов отдельных служб, даже тех, с которыми вы связаны сами. Гейтс мог смотреть на вещи широко и был прагматичен.

В результате был найден компромисс — директор АНБ станет четырехзвездным генералом (получит еще одну звезду) и главой Киберкомандования США. В Пентагоне говорят: «Кто занимает два поста, тот носит две шляпы». Теперь Киберкомандование должно было стать подразделением STRATCOM. Весь опыт АНБ был бы принят на вооружение Киберкомандованием США, что избавляло от необходимости изобретать множество велосипедов. Военно-воздушные силы, морская пехота и сухопутные войска сохраняли свои киберподразделения, но с условием их подчинения Киберкомандованию США. Именно они должны вести боевые действия в киберпространстве, а не полугражданская разведслужба, которой является АНБ. Хотя у АНБ есть огромный опыт проникновения в Сеть, но, согласно закону США (статья 10), Агентство имеет ограниченное право собирать информацию и не может принимать участие в боевых действиях. Поэтому разрушать системы врага нажатием кнопки должны, согласно статье 50, военные. Чтобы посодействовать Киберкомандованию в защите сетей Министерства обороны, Пентагон должен был разместить своего поставщика интернет-услуг в Форт-Мид, штат Мэриленд, вместе с АНБ. Интернет-провайдер Пентагона не похож на остальных, поскольку он обеспечивает работу самых больших сетей в мире. Называется эта организация DefenseInformation

58

Кибервоины

SystemsAgency(DISA) — управление связи Министерства обороны, и возглавляет его трехзвездный генерал. Итак, спустя девяносто два года после появления на этом месте военной базы Форт-Мид стал центром американских сил киберзащиты и кибернападения. Военные подрядчики строят вокруг офисы в надежде, что и им перепадет что-то из миллиардов долларов, которые потекут в Форт-Мид. Университеты Мэриленда получают огромные гранты на исследования от расположившихся здесь военных, подразделение которых в Вашингтоне называют просто Форт.

В результате решения создать Киберкомандование то, что раньше было Киберкомандованием военно-воздушных сил, стало 24-й воздушной армией со штаб-квартирой на базе ВВС в Лэкленде (штат Техас). Но у этой армии нет самолетов. Ее основная задача — «боеспособные войска, обученные и оснащенные для проведения киберопераций, полностью интегрированных в операции в воздухе и безвоздушном пространстве». 24-я воздушная армия будет контролировать два существующих крыла: 688-е — крыло информационных операций (InformationOperationsWing, IQW),бывший Центр информационных операций военно-воздушных сил (AirForceInformationOperationsCenter),и 67-е крыло сетевой борьбы (NetworkWarfareWing),а также одно новое 689-е крыло связи (CombatCommunicationsWing).Миссия 688-го крыла — поиск самых перспективных направлений, предоставляющих США преимущества в использовании кибероружия. 67-е крыло будет отвечать за защиту сетей ВВС и нападение на вражеские сети. В общей сложности численность 24-й армии составит около 6-8 тысяч военных и гражданских кибервоинов. Если ВВС США получат приказ действовать в соответствии с рекламным роликом («Авария энергосистемы — это просто авария. Но она может быть

59

Третья мировая война: какой она будет?

спровоцирована кибератакой»), эта задача, скорее всего, достанется на 67-му крылу. Девиз этого подразделения появился еще в докибернетические времена воздушной разведки — LuxExTenebris(Свет из тьмы). Несмотря на понижение в ранге их командующего, ВВС не утратили желания вести кибервойну. Летом 2009 года глава ВВС генерал Нортон Шварц написал своим офицерам: «Киберпространство необходимо для ведения современной войны, для военного превосходства Соединенных Штатов, и цель ВВС США — использовать весь спектр возможностей киберпространства. Киберпространство — это сфера, за которую сражаются, и борьба идет уже сегодня».

Чтобы не отстать, военно-морской флот США тоже пошел на реорганизацию. Начальник штаба ВМС адмирал Гэри Ружхэд учредил пост заместителя по вопросам информационного влияния. Это не значит, что Ружхэд и его моряки влияют на всех; просто вооруженные силы США постоянно подчеркивают, что они должны влиять на киберпространство. Примерно так в 1960-х в Пентагоне говорили о ядерном оружии. Историк Лоуренс Фридман, занимающийся вопросами ядерной стратегии США, заметил, что Уильям Кауфман, Генри Киссинджер и другие стратеги прекрасно понимали, что нужно было «приглушить наступательный дух, царивший в кругах ВВС... чья риторика вытекала из представления о войне, которое было устаревшим и опасным». Такого же рода настроения сильны в кругах кибервоинов ВВС сегодня и, вероятно, также в ВМС.

Адмирал Ружхэд учредил не только новый пост, но и новое боевое командование. Пятый флот отвечает за Персидский залив, шестой — за Средиземное море, седьмой — за Южно-Китайское море. Специально для ведения кибервойны ВМФ США восстановил десятый флот. Во время Второй мировой войны это небольшое подразде- ьа

Кибервоины

ление занималось координацией противолодочной борьбы в Атлантическом океане, а вскоре после победы над Германией в 1945 году было расформировано. Тогда, как и сейчас, десятый флот был «фантомным», без кораблей. Он базировался на суше и выполнял необходимые координирующие функции. Скромный по возможностям и масштабу, десятый флот во время Второй мировой справлялся со своим задачами силами пятидесяти офицеров разведки. Теперь у ВМС более амбициозные планы. Существующее командование боевых информационных систем продолжит свою деятельность, перейдя в подчинение десятому флоту. Хоть военно-морской флот и не занимается саморекламой, как военно-воздушные силы, флот уверяет, что в его рядах служит не меньше разбирающихся в технике парней, чем в ВВС.

Кибервоины сухопутных войск располагаются в Командовании развития телекоммуникационных технологий (NetworkEnterpriseTechnologyCommand), 9-м соединении связи (9thSignalCommand),дислоцированном в Форт-Хуачука (штат Аризона). Служащие этого подразделения приписаны к войскам связи, расположенным в разных географических регионах планеты. Подразделения, находящиеся в подчинении у армейской разведки, способны вести боевые операции вместе с традиционными разведчастями. Они совместно с АНБ обеспечивают разведданными части, ведущие боевые действия в Ираке и Афганистане. A-GNOSC(Армейский центр безопасности и поддержки работы глобальных сетей) руководит деятельностью LandWarNet,и это армия считает своим вкладом в работу компьютерных сетей Министерства обороны США. В июле 2008 года в сухопутных войсках появился собственный сетевой батальон. Если сухопутные войска считают наименее подходящими для ведения кибервойны, значит, они это заслужили. После принятия решения

 е 1

Третья мировая война: какой она будет?

о создании Киберкомандования министр обороны поручил пересмотреть кибермиссию сухопутных войск.

Если большинство тех, кто следил за борьбой вокруг кибервойны в Пентагоне, сочли, что АНБ победило, бывший директор АНБ Кен Минихэн был с этим не согласен, что дало мне повод задуматься. Кен — мой хороший друг, я знаю его с тех пор, как он возглавил в 1996 году АНБ. Кен считает, что нужно пересмотреть подход АНБ и вооруженных сил США к кибероперациям. Флот, полагает он, фокусируется только на других флотах, военно-воздушные силы — на противовоздушной обороне. Сухопутные войска безнадежно потеряны, а АНБ остается разведывательной службой. «Ни одна из этих организаций не концентрируется в достаточной степени на иностранной контрразведке в киберпространстве или на захвате важнейших инфраструктур, которые, возможно, Соединенные Штаты захотят вывести из строя без применения бомб в следующем конфликте». Кен убежден, что в военном киберпланировании отсутствует программа национального масштаба, которая позволила бы АНБ и другим организациям работать согласованно. «Сейчас все сосредоточены на том, что хотят делать, а не на том, что от них в случае необходимости может потребовать президент».

Минихэн и Макконел уверены в том, что Киберкомандование не способно защитить Соединенные Штаты. «Все наступательные возможности США в киберпространстве не будут значить ничего, если никто не сможет защитить страну от кибератаки», — говорит Макконел. Миссия Киберкомандования — защищать Министерство обороны и, возможно, некоторые правительственные организации, но у него нет ни плана, ни возможностей защитить гражданскую инфраструктуру. Оба бывших директора АНБ полагают, что такую миссию должно выполнять Министерство внутренней безопасности согласно существующему пла-

62

Кибервоины

ну; но оба они утверждают, что это министерство в данный момент не способно защищать даже внутреннее корпоративное киберпространство. Не способен на это и Пентагон. Как отмечает Минихэн, «хоть эта организация и называется Министерством обороны, если от нее потребуется защитить страну от кибератаки со стороны иностранных держав, ваши полтриллиона долларов в год не помогут».

Секретные попытки создания
стратегии

Восприятие киберпространства как территории, где происходит борьба, территории, на которой Соединенные Штаты обязаны доминировать, пронизывает все разговоры военных на тему кибервойны. Национальная военная стратегия ведения киберопераций (частично рассекреченная в соответствии с Законом о свободе информации) демонстрирует отношение военных к кибервойне, в том числе и потому, что она составлена как документ, который не должны были увидеть мы, простые граждане. Она показывает, что говорят за закрытыми дверями Пентагона. Поражает не только признание реальности кибервойны, но и почти благоговейный тон в обсуждении этого краеугольного камня современной боеспособности. Поскольку редко предоставляется возможность услышать что-либо о кибервойне из уст военных, стоит внимательно прочитать этот секретный документ, в котором сформулирована американская стратегия кибервойны.

В этом документе заявляется, что наша цель — «обеспечить стратегическое превосходство США в киберпространстве». Такое превосходство необходимо для того, чтобы гарантировать «свободу действий» американским

63

Третья мировая война: какой она будет?

военным и «лишить ее наших противников». Чтобы добиться превосходства, Соединенные Штаты должны атаковать: «Необходимо расширить возможности нападения в киберпространстве и удерживать инициативу». При первом прочтении стратегия кажется обычным программным заявлением, но при ближайшем рассмотрении становится очевидным, что стратегия отражает понимание некоторых ключевых проблем, созданных кибервойной. В вопросе территориальных границ киберпространства стратегия признает проблему независимости («в силу отсутствия геополитических границ... операции в киберпространстве происходят практически повсеместно»), а также наличие невоенных целей («киберпространство выходит за геополитические границы... в него жестко интегрирована деятельность важнейших инфраструктур и коммерческих институтов»). Однако здесь не идет речь о том, что вооруженные силы США должны защищать такие гражданские объекты. Ответственность за оборону гражданских объектов стратегия возлагает на Министерство национальной безопасности.

Необходимость нанесения первого удара отчасти продиктована тем фактором, что действия, предпринимаемые в киберпространстве, развиваются с невиданной для прежних войн скоростью («киберпространство позволяет маневрировать... почти со скоростью света... Оно дает командующим возможности достигать цели невероятными прежде темпами»). Более того, в стратегии отмечается, что если не действовать быстро, можно вообще не действовать, поскольку «уязвимую цель могут переместить или обеспечить новой защитой без предупреждения, что снижает эффективность операций в киберпространстве». Одним словом, если ждать, пока первым нападет противник, может оказаться, что он одновременно с атакой убрал ваши логические бомбы или отсоединил вашу цель

64

Кибервоины

65

от сети, которую вы намеревались использовать для своей атаки. В стратегии не рассматриваются проблемы, связанные с возможностью и необходимостью действовать на опережение.

Значение киберпространства и кибервойны подчеркивается заявлением, что «Министерство обороны будет руководить традиционными наступательными операциями, чтобы сохранить свободу действий и стратегическое превосходство в кибепространстве». В переводе с канцелярита это означает, что кибератаки не считаются вспомогательным механизмом ведения войны, напротив, Министерство обороны предвидит необходимость бомбардировки реальных объектов с целью защиты от кибератак.

Стратегическая концепция сдерживания упоминается лишь в том месте, где говорится, что желательно «удерживать противника от создания и применения наступательных возможностей против интересов США в киберпространстве». Поскольку около 20-30 стран уже создали наступательные киберподразделения, очевидно, что предотвратить их появление нам не удалось. Чтобы помешать противнику использовать эти возможности против нас, необходимо «опираться на демонстрацию нашего потенциала». Однако атмосфера секретности, окружающая наступательное кибероружие США, означает, что мы не можем продемонстрировать свои возможности. Следуя логике авторов военной стратегии США, мы не в состоянии сдержать противника. Здесь не предлагается путей решения головоломки, хоть она и признается. Таким образом, в документе поднимается ряд ключевых вопросов, которые должны рассматриваться в стратегии, но ответов на них не дается. Получается, что это не совсем стратегия, а скорее анализ ситуации. Что касается руководства к действию, то декларируется необходимость брать на себя инициативу в киберстолкновениях, опережая про- [[9]](#footnote-10)

Третья мировая война: какой она будет?

тивника, и делать все возможное для того, чтобы доминировать в киберпространстве, поскольку иначе превосходство Америки во всех прочих сферах окажется неполным.

Однако в основе документа лежит реалистичная оценка проблем, с которыми сталкиваются США в кибервойне: «противник может воспользоваться [нашей] зависимостью» от киберпространства; «без дальнейших существенных усилий США утратит свои преимущества в киберпространстве» и «рискует наравне со своими противниками». Иначе говоря, в стратегии отмечен тот факт, что другие страны в кибервойне способны нанести нам такой же урон, как и мы им. И даже больший, ведь мы больше зависим от киберпространства, что может сыграть на руку нападающим. Если США так уязвимы, то перед кем? Кто другие кибервоины?

Проснитесь! Призыв из Кувейта

Вполне вероятно, что именно война в Персидском заливе убедила генералов Народно-освободительной армии Китая в необходимости иметь особое преимущество, асимметричные технические возможности для противостояния Соединенным Штатам.

«Буря в пустыне» стала первой настоящей войной после Вьетнама. За десять лет, предшествовавших событиям 1990-1991 годов в Персидском заливе, присутствие американских военных на карте мира было относительно ограниченным по сравнению с Советским Союзом и его ядерным арсеналом. Вторжение президента Рейгана на Гренаду и Буша-старшего в Панаму были мелкими схватками на наших собственных задворках, и прошли они не слишком удачно. Эти конфликты продемонстрировали

66

КиБЕРваины

недостатоную функциональность и плохую координацию, которыми отличилась и неудачная миссия в Иране в 1979 году, которая «помогла» Джимми Картеру покинуть президентский пост.

Затем была «Буря в пустыне». Джордж Буш и его кабинет собрали самую крупную коалицию со времен Второй мировой войны. Более 30 стран объединились против Саддама Хусейна, собрав 4 тысячи единиц авиатехники, 12 тысяч танков и около двух миллионов военных, жалованье которым оплачивали Япония, Германия, Кувейт и Саудовская Аравия. Война ознаменовала начало новой эпохи в международных отношениях, которую генерал Брент Скоукрофт, помощник Буша-старшего по вопросам национальной безопасности, назвал ни много ни мало новым мировым порядком. В нем сохранялся бы суверенитет всех стран, а миссия ООН, наконец, была бы выполнена, поскольку Советский Союз больше не мог ей препятствовать. «Буря в пустыне» ознаменовала зарождение новых приемов ведения войны — компьютер и другие высокие технологии управляли службой тыла и обеспечивали почти мгновенную передачу информации. В книге TheFirstInformationWar(«Первая информационная война»), вышедшей в 1992 году, американская промышленная группа Communicationsand, ElectronicsAssociationоткрыто засвидетельствовала, что применение компьютерных сетей изменило войну.

Хотя генерал Норман Шварцкопф и другие старшие офицеры, пожалуй, не были готовы использовать кибероружие для разрушения иракской системы противовоздушной обороны, им понравилась возможность наводить прицел на врага с помощью компьютерных сетей. Военным также приглянулось новое поколение «умного» оружия, существование которого обеспечили информационные технологии. В отличие от большого количества тра- 67

Третья мировая война: какой она будет?

диционных бомб, каждая «умная» бомба всегда попадала точно в мишень. Это значительно сократило число боевых вылетов и позволило почти полностью исключить сопутствующий ущерб гражданскому населению и гражданским объектам.

Конечно, «умное» оружие в 1991 году было не таким совершенным и его было не много. В фильме 1996 года «Хвост виляет собакой» (Wagthedog) вымышленный политик по имени Конрад «Кони» Брин, которого играет Роберт де Ниро, утверждает, что знаменитая бомба, попавшая в трубу, была снята в Голливуде. «Что люди помнят о войне в Персидском заливе?» — спрашивает Брин. «Бомбу, которая попала в трубу. Позвольте мне сказать вам кое-что: я был в том здании, где снимали эту сцену, используя модель, сделанную из кубиков ,,Лего“». Хоть утверждение героя де Ниро и является ложью, стоит отметить, что «умные» бомбы в 1991 году чересчур расхваливали. Видеозапись была настоящей, но СМИ, кажется, не отдавали себе отчета в том, что американские военные с Б-52 сбрасывали в большинстве случаев не абсолютно точные бомбы, управляемые лазерами и спутниками, а обычные «тупые». «Умные» бомбы тогда имелись в ограниченном количестве и не отличались большой надежностью, но они продемонстрировали направление развития приемов ведения войны и, кстати, показали китайцам, что те отстали на десятилетия.

Весь ход операции «Буря в пустыне» транслировался по телевидению, и американцы буквально прилипли к экранам, наблюдая, как бомбы «попадают в трубы». Они снова приветствовали мастерство грозных американских вооруженных сил. Армия Саддама Хусейна была четвертой по численности в мире. Его оружие, спроектированное и сделанное в Советском Союзе (или Китае), было уничтожено еще до того, как его успели применить. Боевые дей- 6S

Кибервоины

ствия на земле продолжались сто часов; за ними последовало 38 дней ударов с воздуха. Среди тех, кто следил за ходом войны по телевизору, было и китайское военное руководство. Бывший директор Национальной разведки адмирал Майк Макконел считает, что «китайцы были немало шокированы, наблюдая ход „Бури в пустыне". Позднее они, возможно, прочитали „Первую информационную войну" и другие источники, что позволило им осознать, как сильно они отстали. Вскоре они назвали войну в Персидском заливе zhongdaЫапде — „великая трансформация"».

На протяжении нескольких лет китайцы открыто говорили о том, чему их научила «Буря в пустыне». Они отмечали, что раньше, в случае войны, надеялись одержать победу над Соединенными Штатами благодаря численному превосходству. Теперь они пришли к выводу, что данная стратегия неэффективна. Китайцы начали сокращать войска и инвестировать в новые технологии. Одной из таких технологий стала wangluohua— «сетевизация» — освоение нового, компьютерного поля боя. Их публичные заявления поразительно напоминали речи генералов ВВС США. Один китайский эксперт объяснял в военной газете, что «вражеская страна может получить парализующий удар через Интернет». Другой, полковник, возможно, размышляя о США и Китае, писал, что «превосходящие силы, которые потеряют информационное превосходство, будут повержены, а меньшие, захватив информационное превосходство, смогут одержать победу». Генерал-майор Ванг Пуфенг, возглавляющий кафедру оперативного искусства в одном из военных училищ, открыто заявлял о том, что цель страны — zhixinxiquan— «информационное превосходство». Генерал-майор Дэй Квингмин отметил, что такое превосходство может быть достигнуто только с помощью упреждающей кибератаки. Эти экспер- 69

Третья мировая война: какой она будет?

ты в области стратегии создали «интегральную сеть электронной войны», напоминающую повальное увлечение сетевыми боевыми действиями в Пентагоне. К концу 1990-х китайские стратеги сошлись на мысли, что кибероружие позволит стране компенсировать нехватку качественного вооружения, если сравнивать арсенал Китая с Соединенными Штатами. Адмирал Макконел отметил: «Из опыта „Бури в пустыне" китайцы сделали вывод, что они должны бросить вызов главенству Америки на поле боя, для чего им нужно создать технику, способную вывести из игры наши спутники и обеспечить вторжение в наше киберпространство. Китайцы считают, что ради защиты Китая в этом новом мире им нужно лишить Соединенные Штаты преимущества в случае войны».

В китайских формулировках то и дело встречается выражение «асимметричная война». Большая часть того, что нам известно о китайской доктрине асимметричной войны, сформулировано в небольшом томике, название которого переводится как «Неограниченная война». Эта книга, написанная высокопоставленными чинами китайской армии, вышла в свет в 1999 году. В ней изложен план того, как более слабые страны могут изменить существующую расстановку сил и добиться преимущества, используя оружие и приемы, которые выходят за пределы традиционного военного арсенала. Издатели английского перевода этой книги назвали ее «генеральным планом уничтожения Америки», как гласит добавленный подзаголовок. А на обложке, на случай, если читатель не уловит основную идею, изображен Всемирный торговый центр, объятый пламенем. На обороте обложки приведены слова какого-то фанатика из правого крыла о том, что книга «доказывает причастность Китая к событиям 11 сентября». Несмотря на некоторую «правизну» американского издания книги, она является одним из лучших источни- [[10]](#footnote-11)

КИБЕРВОИНЫ

ков, которые помогают нам понять отношение китайских вооруженных сил к кибервойне.

В книге пропагандируется тактика shashoujian— «жезл ассасина» — использование слабых мест в традиционных (кажущихся) преимуществах противника. Цель стратегии — «вести бой исходя из имеющегося оружия» и «создавать необходимое для боя оружие». Здесь предлагается игнорировать принятые правила ведения войны, включая запрет использовать в качестве цели гражданское население, манипуляцию зарубежными средствами массовой информации, наркотики, контроль рынков и т. д. В книге, написанной десять лет назад, делается большой акцент на кибервойне. Возможность использования кибероружия против превосходящих сил не означает, что Китай намеревается вести в войну с Соединенными Штатами, просто военные понимают, что война возможна и поэтому нужен план. Китайское руководство использует выражение «мирный подъем», говоря о запланированном превращении Китая в одну (но не единственную) из мировых сверхдержав. И все же адмирал Майк Макконел считает, что «китайцы используют наши системы по причине их информационного преимущества, они ищут тактико-технические данные систем вооружения и изучают научные исследования в области физики». Стремительный экономический рост Китая и зависимость от мировых ресурсов, так же как и разногласия с соседями (Тайванем, Вьетнамом), вероятно, наводят военных на мысль, что они должны быть готовы к возможному конфликту. И они готовятся. Глава вооруженных сил США адмирал Майк Маллен (председатель Объединенного комитета начальников штабов) считает, что подготовка нацелена прямо на Соединенные Штаты: «[Китай] развивает мощности, связанные с ведением боя на море и в воздухе, во многом ориентированные на войну с нами», — заявил он в своей

 71

Третья мировая война: какой она будет?

речи на собрании Морской лиги в мае 2009 года. «Кажется, они больше всего сосредоточены на военно-морских силах США и наших базах, расположенных в той части планеты», — продолжил он. В ежегодном отчете министра обороны за 2009 год, озаглавленном «Военная мощь Китайской Народной Республики», эти заявления поддерживаются. Китайцы разработали РЛС дальнего обнаружения, благодаря которым они могут видеть, что происходит на нашей авиабазе в Гуаме. Они спроектировали противолодочные ракеты, которые приближаются так быстро, что их не в состоянии перехватить ни одна из наших систем обороны. Китай купил у России авианосец «Адмирал Кузнецов», который в настоящее время модернизируется на верфи в Даляне. Скоро китайцы начнут строить собственные авианосцы и откроют специальную программу обучения пилотов. Они установили вдоль побережья более двух тысяч ракет, направленных на Тайвань, и каждый год добавляют еще сотню. Совсем скоро они разместят ракеты с радиусом действия 8 тысяч километров, что даст им возможность наносить ядерные удары через океан.

Все это звучит несколько устрашающе, но при ближайшем рассмотрении понятно: одной модернизации недостаточно, чтобы противостоять традиционному перевесу сил США. Военный бюджет Китая уступает американскому в разы, он составляет всего лишь 70 миллиардов долларов, что в восемь раз меньше бюджета Пентагона без учета расходов на войны в Афганистане и Ираке. Ударная группа американских авианосцев является одной из самых мощных неядерных сил в истории человечества. Она состоит из десятков кораблей, включая ракетоносцы, эсминцы, миноносцы, подводные лодки, транспорты снабжения, и способна преодолевать по 700 морских миль в день, что позволяет попасть по воде в любую точку планеты максимум за две недели. В составе военно-морского флота США

72

Кибервоины

имеется 11 боевых групп авианосцев, и сейчас ВМС ожидает три авианосца нового поколения, первый из которых планируется спустить на воду в 2015 году.

По данным Пентагона за 2009 год, Китай не успеет ввести бывший российский авианосец в эксплуатацию раньше 2015-го. Представители разведывательного сообщества США сходятся во мнении, что Китаю нужно еще по крайней мере десять лет, чтобы суметь одержать уверенную победу над таким некрупным противником, как Вьетнам. Отбросить же от своих берегов силы врагов, уступающих США, Китай сумеет не ранее 2015 года. Если только...

Если только Китай не сумеет изменить соотношение сил, ведя кибервойну против американских авианосцев. Китайцы всегда восхищались американскими авианосцами, но их внимание к ним увеличилось в 1996 году, когда президент Билл Клинтон послал две боевые группы авианосцев на защиту Тайваня во время одного обмена особенно жесткими заявлениями между Пекином и Тайбэем. Китайские военные в соответствии с новой стратегией предложили «виртуальный план» уничтожения группы авианосцев в документе «Тактический канал передачи данных в информационной войне». Материалы, которые легли в основу этого несекретного документа, составленного двумя офицерами китайских военно-воздушных сил, были доступны через Интернет, а его целью стало показать, как с помощью относительно низкотехнологичных методов можно заблокировать или разрушить информационные системы, на которые полагаются вооруженные силы США.

Такого рода тактические приемы можно найти в стратегии «Неограниченная война». Основной план: украсть технологию противника, найти в ней изъяны, воспользоваться ими и разработать собственную версию программы. Однако не ускользнула от китайских военных стра-

73

Третья мировая война: какой она будет?

тегов и способность кибероружия совершенно исчезать с поля боя. В случае войны Китай готов нанести удар по тылу врага, но не обычным оружием, а асимметрично, посредством кибератаки. Даже значительная модернизация оборудования не позволит Китаю догнать США еще много десятилетий. Однако если Китай будет использовать асимметричную тактику, включая кибервойну, будьте уверены: новые современные вооруженные силы Китая окажутся достаточно совершенными для того, чтобы бросить вызов американским войскам с помощью кибератаки. Недавно Пентагон напугала статья в Orbisпод названием «Как Соединенные Штаты проиграют морскую войну 2015 года». В ней Джеймс Краска ярко описал, как в недалеком будущем Китай сумеет бросить вызов Соединенным Штатам и победить.

Восточные хакеры

Судя по нашим сведениям о кибермощностях Китая и по шпионским кампаниям, проведенным этой страной, Китай использует двойной подход. С конца 1990-х Китай систематически реализовывал все то, что должна делать страна, способная вести кибернаступление и осознающая, что и сама может оказаться мишенью в кибервойне, а именно:

<§ создал гражданские группы хакеров;

® занялся масштабным кибершпионажем, в том числе и в области программного обеспечения и аппаратных средств;

<Э предпринял шаги для защиты собственного киберпространства;

74

Кибервоины

® разместил в инфраструктуре США множество логических бомб.

Одновременно с разработкой киберстратегии Китай воспользовался услугами хакеров, которым близки государственные интересы. По оценкам Американско-китайской комиссии по обзору состояния экономики и безопасности, в Китае работает около 250 групп хакеров, достаточно продвинутых для того, чтобы поставить под угрозу интересы США в киберпространстве. Мы видели, на что они были способны на заре своего существования, когда Соединенные Штаты проводили кампанию по прекращению массовых убийств в Косово. Американцы имели едва ли не самое совершенное интеллектуальное оружие и использовали его, чтобы уничтожить военный аппарат советской эпохи, не потеряв ни одного американского солдата (один боевой самолет все же разбился из-за механической неисправности). К сожалению, интеллектуальным оружием нельзя компенсировать отсутствие интеллекта. Шесть бомб, сброшенных с американских самолетов, ударили точно по цели, намеченной в штабе ЦРУ. Этой целью должно было стать Федеральное управление поставок и закупок — координационный орган сербских вооруженных сил. Однако же координаты были указаны неверно, и вместо управления бомбы попали в китайское посольство, располагавшееся в трехстах метрах от предполагаемой цели.

Китайцы протестовали у консульств и посольств Соединенных Штатов, делали заявления в ООН и другие организации и требовали компенсации для пострадавших и их семей. После бомбардировки посольства сайты правительства США и НАТО подверглись атакам, которые нарушили нормальный процесс работы. На электронную почту государственных служащих обрушились тонны писем

75

Третья мировая война: какой она будет?

с протестами. Некоторые сайты НАТО вышли из строя, другие работали с перебоями. Атака не нанесла большого вреда американским вооруженным силам или деятельности правительства. Она не слишком превышала масштабы сегодняшнего «хактивизма» — довольно спокойной формы онлайнового протеста. Однако эта атака стала первым опытом Китая в использовании киберпространства для выражения протеста. Китайские «хактивисты» повторили то же самое в 2001 году, когда американский самолет-шпион якобы проник в воздушное пространство Китая и был вынужден приземлиться. Обычные китайские хакеры проводили довольно примитивные кибератаки, но не бездействовала и китайская промышленная разведка.

Китайское правительство взяло в оборот два кита американской компьютерной индустрии, Microsoftи Cisco. Угрожая прекратить закупки продукции Microsoft,Пекин убедил Билла Гейтса предоставить Китаю копию закрытого кода операционной системы. Руководство Microsoftотказалось предоставить этот код своим крупнейшим коммерческим потребителям в Америке. Затем Китай получил информацию о сетевом маршрутизаторе Cisco,обеспечивающем работу практически всех сетей Соединенных Штатов и большинства интернет-серверов. Когда-то у Ciscoбыл завод по производству маршрутизаторов в Китае. Потом китайские компании начали продавать дешевые копии маршрутизаторов. Как утверждают, в число покупателей вошел даже Пентагон и ряд других федеральных правительственных организаций. Такие маршрутизаторы стали появляться на рынке в 2004 году. Через три года ФБР и Министерство юстиции США обвинили братьев, владевших компанией SyrenTechnology,в продаже ворованных маршрутизаторов целому ряду клиентов, включая корпус морской пехоты, военно-воздушные силы и многочисленных военных подрядчиков. В пятидесятистраничном от-

76

КИЕЕРВОИНЫ

чете, составленном ФБР, говорится, что эти маршрутизаторы могут использоваться иностранными разведслужбами для разрушения сетей и «ослабления шифровальных систем». Между тем другая китайская компания, Huawei, продавала точно такие же маршрутизаторы по всей Европе и Азии. Они отличались только тем, что на них вместо торгового знака Ciscoстоял Huawei.

Благодаря знаниям недостатков продукции Microsoftи Ciscoкитайские хакеры способны остановить деятельность большинства сетей. Но разве сами китайцы не столь же уязвимы? Ответ на этот вопрос был бы утвердительным, если бы они использовали те же продукты Microsoftи Cisco,что и мы. Но по соглашению с Microsoftкитайцы модифицировали версию, которая продается в их стране, дополнив ее собственным программным кодом. Они даже разработали собственную операционную систему Kylin, построенную на базе FreeBSD. Именно Kylinиспользует Народно-освободительная армия Китая. Есть сведения, что Китай разработал собственный микропроцессор для использования в серверах и маршрутизаторах Huawei. Китайское правительство пытается установить программное обеспечение GreenDam. YouthEscortна всех компьютерах под предлогом борьбы с распространением детской порнографии и других запрещенных материалов. Если это программное обеспечение заработает и его установят на всех системах, GreenDamсможет отслеживать и вредоносное ПО, размещаемое вражескими государствами.

Помимо GreenDamсуществует еще одна система, которую американские остряки называют великой китайской стеной, — GreatFirewall.Эта управляемая правительством система на самом деле брандмауэром не является, она сканирует трафик в поисках антиправительственных материалов, таких как Всеобщая декларация прав человека. Эта система перехватывает доменное имя и перенаправ-

77

Третья мировая война: какой она будет?

ляет вас на одобренный китайским правительством клон реального сайта, если вы, находясь в Китае, попытаетесь зайти, к примеру, на веб-страницу Христианской евангелической организации. Она также способна отключить китайские сети от всего остального Интернета, что очень удобно, если вы предполагаете, что США собираются начать против вас кибератаку. Джеймс Малвелон, один из ведущих американских экспертов по китайскому киберарсеналу, говорит, что, взятые вместе, GreenDam, GreatFirewallи другие системы доказывают «существенные инвестиции китайских властей в блокировку, фильтрацию и мониторинг» собственного кибепространства.

В 2003 году Китай объявил о создании собственных кибервойск. На военно-морской базе острова Хайнань базируются третий технический отдел Народно-освободительной армии Китая и Лингшуйская база радиоэлектронной разведки. По данным Пентагона, эти части отвечают за нападение и защиту в киберпространстве, кроме того, ими разработано невиданное ранее кибероружие, которое не остановит никакая оборона. В одной из публикаций китайцы перечислили десять вариантов использования такого оружия:

0 размещение информационных мин;

О руководство информационной разведкой;

О изменение сетевых данных;

0 запуск информационных бомб;

0 сброс информационного «мусора»;

0 распространение пропаганды;

0 использование дезинформации;

7 В

Кибервоины

0 создание информационных клонов (именно так!);

0 организация информационной обороны;

0 создание сетевых станций слежения.

Китай действительно создал две сетевые станции слежения неподалеку от США, на Кубе. С разрешения правительства Кастро китайские военные разместили здесь оборудование для мониторинга американского трафика и коммуникаций Министерства обороны. Примерно в то время, когда Китай объявил о создании киберчастей, США пережили один из худших на сегодняшний день эпизодов кибершпионажа. «Титановый дождь», как назвали его американцы, привел к декодированию около 10-20 терабайтов несекретной информации Пентагона. Хакеры сделали своей мишенью военного подрядчика LockheedMartinи другие военные сайты и — по причинам, которые до сих пор сложно объяснить, — Всемирный банк. Слабые места сетей Пентагона и других организаций были заранее изучены, а затем использованы для доступа к информации через серверы Южной Кореи и Гонконга. Спецслужбы сумели проследить цепочку от этих промежуточных серверов до конечного сервера, находящегося в китайской провинции Гуандун. Генерал-майор военно- воздушных сил США открыто приписал эти атаки не китайским «хактивистам», а китайскому правительству.

К 2007 году китайское правительство, очевидно, участвовало в целом ряде проникновений в американские и европейские сети, успешно скачивая огромные объемы данных. Директор британской службы контрразведки MI-5 Джонатан Эванс отправил письма 300 ведущим компаниям Великобритании, извещая о том, что в их сети, возможно, проникли китайские спецслужбы. Германский коллега Эванса Ханс Ремберг также выдвигает обвинение

79

Третья мировая война: какой она будет?

китайскому правительству, на этот раз во взломе компьютера Ангелы Меркель, канцлера Германии. Компьютерный шпионаж коснулся и высокопоставленных американцев, включая и министра обороны Роберта Гейтса. Китайские шпионы скопировали информацию с ноутбука министра торговли США Карлоса Гутьерреса, когда тот посещал Пекин, а затем пытались использовать ее, чтобы получить доступ к компьютерам Министерства торговли. Заместитель министра обороны Роберт Лоулес, комментируя происшедшее, признал, что у китайцев есть «серьезные возможности для атаки и повреждения наших компьютерных систем... для выведения из строя наших важнейших систем. Они считают это основным компонентом асимметричной войны».

В 2009 году канадские исследователи обнаружили одну интересную компьютерную программу, которую назвали GhostNet.Она была установлена на 1300 компьютерах в посольствах разных стран по всему миру. Программа позволяла удаленно без ведома пользователя включать камеру и микрофон компьютера и спокойно передавать изображение и звук на серверы в Китае. Главной мишенью этой программы стали офисы, связанные с неправительственными организациями, занимающимися тибетскими вопросами. Работа программы, прежде чем была раскрыта, продолжалась на протяжении 22 месяцев. В том же году из американской разведки в СМИ просочилась информация о том, что китайские хакеры проникли в электрораспределительную сеть США и поставили логические бомбы, с помощью которых можно было вывести эту сеть из строя.

Масштаб китайского хакерства против американской, европейской и японской промышленности и исследовательских организаций беспрецедентен. Экзабайты данных копируются с компьютеров университетов, промышлен- в □

Кибервоины

ных лабораторий, государственных предприятий. Все, от секретных фармацевтических формул, биоинжинирин- говых моделей, нанотехнологиий до систем вооружения, чертежей повседневных промышленных изделий с помощью Народно-освободительной армии Китая и частных хакерских групп попадает в огромную корпорацию под названием Китай. Недавно Googleзаявил об очередном разоблачении весьма изощренной кампании, нацеленной на их интеллектуальную собственность, а также на электронную переписку лидеров китайского диссидентского движения.

Хакеры использовали целевой фишинг (мошенничество, направленное на получение банковских конфиденциальных данных), чтобы заставить руководство Googleпосетить сайты, с которых автоматически загружалось вредоносное ПО, открывавшее хакерам доступ к корневому каталогу. Если в ходе обычного фишинга сети закидываются повсюду в попытках поймать хоть несколько человек, достаточно доверчивых для того, чтобы клюнуть на электронные письма от нигерийских мошенников, целевой фишинг направлен на конкретного человека. Сначала через Facebookили Linked-inвыясняется круг его общения, затем отправляется письмо от человека, которому он доверяет. Если бы вы были главой исследовательского центра Google, вы могли бы получить письмо от коллеги примерно такого содержания: «Привет, Чак! Думаю, эта история тебя заинтересует...» и ссылку на довольно безобидный сайт. Когда человек из Googleнажимал на ссылку и попадал на сайт, хакеры, используя уязвимость «нулевого дня»[[11]](#footnote-12) в InternetExplorer, тогда еще не обнаруженную

Третья мировая война: какой она будет?

и не исправленную, спокойно загружали вредоносное ПО (мэлвер) так, что ни одна антивирусная программа, никакие другие средства не позволяли этого заметить. Мэлвер создавал «черный ход» в компьютере таким образом, что хакеры получали доступ к нему и прокладывали путь дальше по корпоративной сети до тех пор, пока не попадали на сервер, содержащий исходный код, — бриллиант в короне компании-разработчика ПО.

Когда исследователи из Googleобнаружили в середине декабря происходящее, они проследили хакерский путь, ведущий к серверу на Тайване, где и нашли копии своих собственных данных и данных по меньшей мере 20 других компаний, среди которых были Adobe, DowChemicalи военный подрядчик NorthropGrumman.Отсюда следы вели в континентальный Китай. Googleобратился в ФБР, сделав публичное заявление об имевшем место взломе и планах уйти с китайского рынка к середине января.

Некоторые скажут, что война с Китаем маловероятна. Зависимость Китая от американских рынков сбыта, триллионы, инвестированные в казначейские векселя ОТТТА означают, что Китай рискует многое потерять. Но один из чиновников Пентагона, пожелавший сохранить анонимность, в этом не уверен. Он отмечает, что экономический кризис в США повлиял и на Китай, в связи с чем миллионы китайских рабочих оказались на улице. Китайское правительство не выразило беспокойства, которое бы возникло в таком случае на Западе, и, очевидно, не собирается ослаблять свою власть над китайским народом.

Урок заключается в том, что Китай способен пережить экономические трудности и может пойти на них, если выгоды от войны покажутся достаточно высокими.

Что это могут быть за выгоды? Часто приводится банальный ответ: возможно, Китай окажется в такой ситуации, что ему придется помешать Тайваню подписать

SZ

КИБЕРВПИНЫ

декларацию независимости. Однако когда серьезные аналитики оценивают шансы открытого конфликта с Китаем, они видят, что Китай делает ставки на воды Южно-Китайского моря. Расположенные там острова Спартли не особенно привлекательны для туризма. Да это не совсем и острова. Если собрать вместе все рифы, песчаные отмели и камни Южно-Китайского моря, получится не более пяти квадратных километров суши. Эти пять квадратных километров разбросаны на территории около 400 тысяч квадратных километров. Не из-за островов враждуют Китай, Вьетнам, Тайвань, Малайзия, Филиппины и Бруней, а из- за того, что находится под ними и вокруг них. В здешних водах сохраняются крупнейшие в мире запасы рыбы, ресурс, который нельзя сбрасывать со счетов, учитывая рост населения стран, претендующих на эти территории. Кроме того, острова окружает важнейший торговый путь, связывающий Индийский океан со странами Тихоокеанского региона, здесь проходят трубопроводы, по которым течет значительная часть мировых запасов нефти со Среднего Востока. Кроме того, есть еще нефть и газ самих Спартли. Неосвоенные месторождения, согласно оценкам, обладают большими запасами газа, чем Кувейт, который сейчас занимает четвертое место в мире. Местного газа хватит любой из этих стран на десятилетия вперед. Нефтяные месторождения уже разрабатываются объединенными усилиями нескольких стран с использованием платформ.

Если Китай решит поиграть своими накачанными военными мускулами, вполне вероятно, он попытается вырвать эти острова из рук соседей, — такой сценарий мы рассмотрим чуть позже. При попытке Китая захватить эти острова США будут вынуждены, пусть и неохотно, отреагировать. США подписали договор о безопасности и с Филиппинами, и с Тайванем, aChevronпосодействовал Вьетнаму в разработке морских месторождений нефти.

вз

Третья мировая война: какой она будет?

С другой стороны, США могут воздержаться от выступления против Китая в Тихоокеанском бассейне в том случае, если платой за вмешательство станут значительные повреждения или разрушения в собственной стране. По словам министра обороны Роберта Гейтса, кибератаки «могут заставить США изменить первоначальные намерения использовать силу, чтобы помочь своим союзникам в Тихом океане». Достаточно ли этого для того, чтобы удержать США от конфронтации с Китаем? Если вероятность того, чтоКитай выведет из строя наш наступательный потенциал, недостаточно пугает нас, может быть, нас удержало бы осознание собственной уязвимости перед кибератакой. Установка логических бомб действительно могла иметь место. Один бывший правительственный чиновник сказал, что, по его убеждению, китайцы хотят, чтобы мы знали — если мы вмешаемся в конфликт с Тайванем, электрораспределительная сеть США наверняка выйдет из строя. «Они стремятся заставить Соединенные Штаты отказаться от применения военной силы в сфере их интересов».

Однако проблема в том, что устрашение работает только в том случае, когда другая сторона его слышит. Американские лидеры, возможно, не до конца поняли, что до них пытается донести Пекин. США не сделали практически ничего, чтобы укрепить слабые места в своей электрораспределительной сети и других гражданских сетях.

Расставим оценки

Я сфокусировался на Китае потому, что его кибервоенное развитие оказалось, как ни странно, до некоторой степени прозрачным. Представители американской разведки, од-

КИБЕРВСЭИНЫ

нако не считают Китай самой большой угрозой США в ки- бепространстве. «Русские определенно лучше, они почти как мы», — сказал один из них. Существует, по-видимому, единодушное мнение: Китай привлекает больше внимания потому, что он — намеренно или нет — оставляет следы и «хлебные крошки», ведущие прямо на площадь Тяньаньмэнь. Вольные российские хакеры, включая тех, кто сотрудничает с крупными преступными организациями, — реальная сила в киберпространстве, как было продемонстрировано во время кибератак на Эстонию и Грузию, рассмотренных в первой главе.

Считается, что деятельность «хактивистов» и криминальных организаций в целом санкционирована бывшим 16-м отделом печально известного советского разведывательного органа КГБ. Позднее это подразделение стало называться ФАПСИ. Мало кто из американских офицеров разведки помнит, как расшифровывается аббревиатура ФАПСИ (Федеральное агентство правительственной связи и информации), они просто называют его московским АНБ.

Как и американское Агентство национальной безопасности, ФАПСИ начинало с шифровки и дешифровки, радиоперехвата, подслушивания и перехвата телефонных разговоров. Как только появился Интернет, ФАПСИ оказалось там, подмяв под себя крупнейших интернет- провайдеров и позже выдвинув требование всем провайдерам использовать системы мониторинга, доступ к которым имелся только у ФАПСИ. Конечно, во время активного становления Интернета Советский Союз прекратил свое существование, как и теоретически КГБ и ФАПСИ. Но на самом деле организации просто дали своим центрам другие названия. После нескольких изменений ФАПСИ в 2003 году превратилось в Службу специальной связи и информации. Не все его здания находятся в Москве.

В 5

Третья мировая война: какой она будет?

В Воронеже расположена, возможно, крупнейшая в мире (и, определенно, одна из лучших) хакерская школа. Сейчас ее учащиеся наверняка называют себя кибервоинами.

Квалифицированные киберподразделения имеют Израиль и Франция. Сотрудники американской разведки предполагают, что 20-30 государств вполне способны вести кибервойну, среди них Тайвань, Иран, Австралия, Южная Корея, Индия, Пакистан и несколько стран НАТО. «Подавляющее большинство промышленно развитых стран могут организовать кибератаку», — говорит бывший директор Национальной разведки адмирал Майк Макконел.

Кибервоины атакуют

Теперь вы, возможно, верите в реальность кибервоинов, но что еще они могут сделать, кроме как нарушить работу нескольких веб-сайтов? Конечно, мы еще не видели полномасштабной кибервойны, но легко можем представить себя ее жертвой. Представьте день в недалеком будущем. Вы, помощник президента по вопросам национальной безопасности, собираетесь домой после рабочего дня, и вдруг вам звонят из оперативного штаба Белого дома. АНБ передало сообщение CRITIC— редкий сигнал тревоги, свидетельствующий о том, что произошло нечто действительно важное. Вам сообщают: «Несколько разных вредоносных программ „нулевого дня“ атакуют американский сегмент Интернета, угрожая жизнедеятельности важнейших инфраструктур». Старший дежурный офицер оперативного штаба предлагает вам спуститься к нему и помочь разобраться, что происходит. Когда вы добираетесь до оперативного штаба, на проводе директор управления оборонной связью. Он только что совещался с министром

Вб

Кибервоины

обороны, и тот посоветовал позвонить вам. NIPRNET— несекретная сеть Министерства обороны — выходит из строя. Маршрутизаторы по всей сети непрерывно перезагружаются. Сетевой трафик, по сути, заблокирован. Пока он говорит эти слова, вы слышите, как кто-то на заднем фоне пытается привлечь его внимание. Когда генерал возвращается на линию, он спокойно произносит: «Теперь то же самое происходит в SIPRNETи JWICS».Значит, та же участь постигла секретные сети Министерства обороны. Теперь с вами срочно хочет переговорить заместитель министра национальной безопасности, еще не знающий, что происходит в Пентагоне. Из Федерального агентства по чрезвычайным ситуациям ему доложили, что два региональных офиса агентства, в Филадельфии и Дентоне (штат Техас), сообщают о крупных пожарах на нефтеперегонных заводах в Филадельфии и Хьюстоне, а также о выбросах смертельно опасного хлора на нескольких химических заводах в штатах Нью-Джерси и Делавэр. Он добавляет, что питсбургская компьютерная группа реагирования на чрезвычайные ситуации завалена отчетами о выходе из строя систем, но у него не было времени выяснить все подробно. Прежде чем вы успеваете поинтересоваться у старшего дежурного офицера, где президент, телефон начинает снова звонить. Это заместитель министра транспорта. «На нас напали?» — спрашивает она. В ответ на ваше «почему?» она выпаливает на одном дыхании, что случилось. В центре управления воздушным движением Федерального управления гражданской авиации в Херндоне (штат Вирджиния) полностью вышли из строя все системы. Альтернативный центр в Лисбурке в панике, поскольку другие региональные центры не видят, какие самолеты находятся в воздухе, и пытаются вручную установить местоположение и развести сотни самолетов. Из центра Брикьярд в Индианаполисе сообщают о столкновении

В V

Третья мировая война: какой она будет?

двух «боингов». «Я думала, кризис затронул только авиацию, но затем начались аварии на железной дороге», — продолжает она. Федеральное управление железных дорог сообщает о крушениях товарных поездов в Лонг-Бич, Норфолке, Чикаго и Канзас-Сити.

Взглянув на информацию о местонахождении президента, вы видите лаконичное «в Вашингтоне». Он находится где-то за пределами Белого дома. Словно читая ваши мысли, старший дежурный офицер объясняет, что президент повел первую леди в ресторан. «Тогда соедините меня с начальником его секретной службы», — говорит кто-то. Это министр финансов прибежал из своего офиса в здании близ Белого дома. Только что звонил председатель Федерального резервного банка. Произошла крупная авария центров обработки данных, которая затронула даже резервные копии. Все данные потеряны. DTCCи SIACтоже рушатся». Эти аббревиатуры, поясняет он, означают главные финансовые вычислительные центры Нью-Йорка. «Теперь никто не знает, кому что принадлежит. К утру вся финансовая система рухнет».

Пока он говорит, вы невольно задерживаете взгляд на экране телевизора, где сообщается о сходе с рельсов поезда метро под Потомаком. На другом канале показывают пламя, бушующее в Вирджинии, где взорвался крупный газопровод. Затем начинает мигать освещение в оперативном штабе. Лампы гаснут. Включается аварийное освещение, работающее от аккумулятора, и комнату заполняют полосы света и тени. Плоские экраны телевизоров и мониторы компьютеров ничего не показывают. Свет снова начинает мигать. Издалека доносится громкое жужжание. «Это запасной генератор, сэр», — говорит дежурный офицер. Его помощник снова вручает вам телефон и произносит слова, которые вам так не хочется слышать: «На проводе президент».

вв

Кибервоины

Президент на своем гигантском бронированном автомобиле, напоминающем откормленный стероидами «кадиллак», возвращается из ресторана. Секретная служба эвакуировала его, когда погас весь свет, и теперь они с трудом передвигаются по городу. На улицах Вашингтона то и дело происходят аварии, поскольку не работают светофоры. Президент хочет знать, правда ли то, что ему сообщил агент секретной службы, — все Восточное побережье осталась без электричества? «Хотя... подождите... Что? Команда вице-президента сообщает, что в месте нахождения их шефа электричества нет. Разве он сегодня не в Сан-Франциско? Сколько там сейчас времени?»

Вы смотрите на часы. Всего 20:15. За четверть часа 157 мегаполисов остались без электричества. Облака ядовитого газа несутся на Уилмингтон и Хьюстон. Пылают нефтеперегонные заводы. Аварии в метро Нью-Йорка, Окленда, Вашингтона и Лос-Анджелеса. Товарные поезда сошли с рельсов на крупнейших железнодорожных узлах и сортировочных станциях четырех главных железных дорог страны. Самолеты буквально падают с неба. Газопроводы взорвались, а миллионы людей замерзают. Финансовая система остановилась, потому что в центрах обработки данных уничтожены терабайты информации. Метеорологические, навигационные спутники и спутники связи покинули свои орбиты. Вооруженные силы США превратились в множество изолированных подразделений, безуспешно пытающихся связаться друг с другом.

Несколько тысяч американцев уже погибли, многие ранены и пытаются добраться до больниц. Жертв будет еще больше, но люди, которые должны передавать вам информацию, не смогут выйти на связь. В ближайшие несколько дней города останутся без еды из-за выхода из строя системы железнодорожного сообщения, отключения программного обеспечения на оптовых базах и в транс- 89

Третья мировая война: какой она будет?

портных компаниях. Электричества не будет, потому что ядерные генераторы в целях безопасности заблокированы, а обычные электростанции серьезно повреждены. Высоковольтные линии электропередач повреждены. Некоторые жители страны, не сумев снять наличные деньги, скоро начнут грабить магазины. Полиция и экстренные службы едва ли со всем этим справятся.

В ходе войн, в которых участвовала Америка, ни одна страна не наносила такой урон нашим городам. Сейчас с помощью хорошо спланированной кибератаки это способна совершить любая страна всего лишь за пятнадцать минут и без единого террориста или солдата на нашей территории. Почему же они не сделали этого до сих пор? По тем же причинам, в силу которых девять ядерных государств не применяли ядерное оружие с 1945 года, — им нужны причины. Но в отличие от ядерного оружия, когда нападающего может сдержать ожидание ответных мер или радиоактивная «отдача» по собственной стране, запуск кибератаки сопряжен с меньшими рисками. В кибервойне мы можем никогда не узнать, кто нанес удар. В самом деле, едва ли для дрожащих от холода американцев утешением станет мысль о том, что США отплатят вероятному противнику тем же. «Пока вы были на линии с президентом, сэр, мне звонили из Киберкомандования. Они считают, что нас атаковала Россия, и готовы оставить без света Москву, сэр. Или это был Китай, так что они ударят по Пекину, если вы прикажете. Сэр?»

Глава 3

Попе битвы

К

иберпространство. Можно представить, будто это еще одно измерение, по которому скользят зеленые светящиеся столбики цифр и букв, как в «Матрице». Но на самом деле все еще проще. Киберпространство — это ноутбук, с которым ваш ребенок ходит в школу, ваш настольный компьютер на работе, темное здание без окон в деловом районе города и кабель, протянутый под дорогой. Оно везде, где есть компьютер, процессор или сеть,

Третья мировая война: какой она будет?

связывающая их. И все это теперь — территория войны, где произойдет множество решающих битв XXI столетия. Чтобы понять почему, мы должны ответить на несколько важных вопросов. Что такое киберпространство? Как оно устроено? Как там будут проходить битвы?

Как и почему возможна
КИБЕРВОЙНА

Киберпространство — это все компьютерные сети мира и все, что их объединяет и контролирует. Это не только Интернет. Давайте проясним разницу. Интернет — открытая сеть из множества сетей. Из любой части Интернета вы можете связаться с любым компьютером, связанным с Интернетом, где бы он ни находился. Киберпространство состоит из Интернета и множества других сетей компьютеров, которые не считаются доступными из Интернета. Некоторые из этих сетей похожи на Интернет, но они, по крайней мере теоретически, не связаны с ним. Другие части киберпространства — деловые сети, по которым передаются данные о денежных потоках, торговле на фондовых биржах и операциях по кредитным картам. Некоторые сети являются контролирующими системами, позволяющими одним устройствам общаться с другими, — в той же степени, как панели управления отдают команды насосам, лифтам и генераторам.

Но как эти сети превращаются в поле сражения? В самом широком смысле в них могут проникнуть кибервоины, чтобы взять их под контроль или уничтожить. Если кибервоины захватывают сеть, они могут выкрасть всю информацию или отдать команды, чтобы перевести деньги, раз-

92

Попе битвы

лить нефть, выпустить газ, взорвать генератор, вызвать крушение поезда, разбить самолет, послать взвод в засаду или заставить ракету сдетонировать не там, где нужно. Если кибервоины взламывают сети, крадут данные или превращают компьютер в фильтр, дозирующий информацию, это грозит коллапсом финансовой системы, прерыванием цепочки поставок, сходом спутника с орбиты, остановке полетов. И это вовсе не предположения. Подобное уже происходило в порядке эксперимента, по ошибке или небрежности. Как отметил адмирал Макконел, «информацию, передаваемую по компьютерным сетям, ту, что управляет нашими коммунальными услугами, транспортом, банковскими операциями и коммуникациями, могут использовать или уничтожить за несколько секунд из любой точки планеты, из-за океана. Ни одна флотилия, никакие межконтинентальные ракеты или регулярные армии не сумеют отразить такие атаки, ведь нападающий находится не просто за пределами наших границ, но и за пределами нашего физического пространства, в мире цифр».

Зачем же мы тогда используем столь сложные компьютерные сети, которые допускают несанкционированный доступ и несанкционированное управление? Разве не существует мер безопасности? Архитектура компьютерных сетей, программное и аппаратное обеспечение дают кибервоинам тысячи возможностей обойти любую защиту. Программы пишут люди, а людям свойственно ошибаться и отвлекаться. Сети, которые, как считается, не связанными с Интернетом, на самом деле часто оказываются связаны с ним, что остается тайной даже для их владельцев. Давайте возьмем любое устройство, которым вы ежедневно пользуетесь, чтобы наглядно объяснить, как может случиться кибервойна. Как вы думаете, знают ли в вашем ТСЖ, что лифт, установленный в вашем доме,

93

Третья мировая война: какой она будет?

«звонит домой» (как в фильме «Инопланетянин»)? Ваш лифт через Интернет связывается с людьми, которые сделали его. А знаете ли вы, что ксерокс в вашем офисе, возможно, ведет себя так же? Героиня Джулии Робертс из фильма «Ничего личного» (Duplicity) знала, что многие копировальные аппараты имеют выход в Интернет и могут быть взломаны, но большинство об этом даже не догадывается. Еще меньше людей в курсе последнего трюка — шредеры, машинки для уничтожения бумаг, могут делать копии документов! Прежде чем засекреченные документы отправляются под нож, они проходят перед камерой, которая их фотографирует. Вечером парень- уборщик заберетновую коллекцию «изображений» и отправит ее тому, кто его нанял.

Лифт и ксерокс «звонят домой» — это звучит правдоподобно. А что, если у вашего конкурента есть программист, которые написал несколько строк кода и внедрил его в процессор, который стоит в вашем ксероксе? Предположим, эти несколько строк программного кода заставляют его сохранять изображения всего, что он копирует и помещать в архив. Однажды ксерокс получает доступ в Интернет и — пинг! — отправляет этот файл через всю страну вашему конкуренту. Или, еще хуже, в день, когда ваша компания должна участвовать в конкурсе на заключение крупного контракта, — пинг! — ксерокс самовозгорается, из-за чего включается противопожарная система, весь офис залит водой, и вы не успеваете вовремя отправить заявку. Конкурент выигрывает, а вы остаетесь ни с чем.

Используя подключение к Интернету, о котором вы даже не подозревали, кто-то написал программу и внедрил ее в ваш ксерокс, процессор которого оказался, как ни удивительно, достаточно мощным. Затем кто-то использовал программу, чтобы заставить ксерокс сделать что-то, не свойственное его обычным функциям, например

94

Попе битвы

короткое замыкание. Он знал, что в результате возникнет пожар, возможно, он экспериментировал с другими такими же копировальными аппаратами. В итоге сработала противопожарная система и залила водой ваш офис, а вы подумали, что произошел несчастный случай. Незнакомец дотянулся до вас из киберпространства и организовал хаос в пространстве физическом, это и был хакер. Изначально хакерами называли людей, которые умели писать команды на языке компьютеров, чтобы заставить их делать что-то новое. Когда хакеры проникают в систему, доступ в которую им не разрешен, они становятся киберпреступниками. А если они работают на вооруженные силы США, их называют кибервоинами.

В данном сценарии киберпреступник использовал Интернет как средство — сначала для получения информации, затем для нанесения вреда. Его оружием стали несколько строк кода, которые он дабавил в процессор копировального аппарата. Можно рассудить иначе: с помощью программы он превратил ваш ксерокс в оружие. Ему это удалось, поскольку программу, управляющая ксероксом, можно изменить. Создатели копировального аппарата не думали, что кто-то способен превратить его в оружие, поэтому и не пытались воспрепятствовать этому на этапе написания программы. То же самое относится к проектировщикам сети электропередачи других систем. Они не думали, что кто-то в них проникнет и превратит в оружие. Ваш офис-менеджер не обратил внимания на слова продавца о том, что копировальный аппарат предоставляет возможность дистанционной диагностики, позволяет загружать обновления, устранять проблемы и запрашивать нужные для ремонта запчасти. А хакеры это заметили или просто исследовали соседнее киберпространство и нашли адрес «Хеопега Copier2000, серийный номер 20-003488, Ваша Компания, 1пс.»

95

Третья мировая война: какой она будет?

Если вы сомневаетесь в том, что копировальные аппараты являются частью киберпространтсва, почитайте ImageSourceMagazine:«Раньше для дистанционной диагностики требовался модем. Методика того времени была несколько неудобной для потребителя и дорогой для поставщика, которому рядом с каждым устройством приходилось устанавливать телефонные розетки и распределительные коробки для совместимости с телефонными аппаратами клиента. Но эти барьеры исчезли с появлением Интернета и беспроводных сетей. Теперь, когда все устройства имеют адрес в сети, диагностическое сообщение об ошибке передается в режиме реального времени, и устройство само может связаться со специалистами еще до того, как его владелец узнает о проблеме. Сегодня сервисным центрам просто непростительно игнорировать экономию затрат, которую обеспечивает дистанционная диагностика. Практически каждый производитель принтеров использует либо собственные инструменты дистанционной диагностики (например, Remoteот компании Ricoh,KyoceraAdminи Adminот компании Sharp, DRMот компании Xerox),либо сотрудничает с третьей стороной, такими компаниями, как ImagingPortalsили PrintFleet».

Этот хоть и банальный, гипотетический сценарий полезен потому, что демонстрирует три аспекта киберпространства, которые делают кибервойну возможной:

1. дефекты в архитектуре сети Интернет;
2. дефекты программного и аппаратного обеспечения;
3. работа все большего количества важнейших систем в режиме онлайн.

Давайте рассмотрим каждый аспект в отдельности.

Поле битвы

97

Уязвимости Интернета

Существуют по меньшей мере пять основных уязвимых мест в архитектуре самого Интернета.

Во-первых, это система адресации, которая всегда знает, кто и где находится в Интернете.

Интернет-провайдеров иногда называют операторами, поскольку они оперируют трафиком в Интернете. Разнообразные компании производят маршрутизаторы, серверы, программное обеспечение, но именно интернет-провайдеры объединяют их. Для удобства давайте разделим интернет-провайдеров на две категории.

Существуют национальные интернет-провайдеры, они владеют и управляют тысячами километров оптоволоконных кабелей, которые проложены по всей стране, соединяя крупные города. В США действует шесть таких крупных провайдеров (Verizon, AT&T, Qwest, Sprint, Level 3 и GlobalCrossing).Их называют магистральными интернет-провайдерами. Как только магистраль доходит до вашего города, она соединяется с множеством более мелких провайдеров, которые обслуживают местные предприятия и ваш дом. Интернет-провайдерами могут быть телефонные компании или кабельное телевидение. Их кабели связывают ваш дом со всем остальным миром.

Чтобы представить, как все работает, и найти некоторые уязвимые места Интернета, посмотрим, что происходит, когда я соединяюсь с Интернетом. Я включаю ноутбук и открываю браузер. При этом я сразу выхожу в Интернет и попадаю на свою домашнюю страницу. Допустим, это будет веб-страница консалтинговой фирмы, в которой я работаю. Итак, сидя в своем домашнем офисе в округе Раппаханнок (штат Вирджиния), у подножья Аппалачей, а делаю клик мышкой, и мой браузер переносит меня на [www.mycompany.com](http://www.mycompany.com). Поскольку компью- [[12]](#footnote-13)

Третья мировая война: какой она будет?

тер слов не понимает, адрес нужно перевести на машинный язык единиц и нулей. Для этого браузер использует систему доменных имен. Это что-то вроде телефонной справочной службы — вы называете имя человека, и вам дают его телефонный номер. Офис моей консалтинговой фирмы расположен в 120 километрах от моего дома в Вирджинии, но ее веб-страница находится на удаленном сервере в Миннеаполисе и имеет адрес, например, 123.45.678.90. Столько цифр сложно запомнить. К счастью, этого и не нужно. Браузер обращается к системе доменных имен, чтобы найти адрес. Он посылает сообщение в базу данных сервера, который является составной частью сложной иерархии компьютеров, формирующих систему доменных имен. Для кибервоинов система доменных имен — идеальная мишень. Ее создавали, практически не задумываясь о безопасности, поэтому хакеры легко могут менять информацию и перенаправлять вас на фальшивые веб-страницы.

Когда я открываю браузер, он посылает запрос на сервер, где расположена нужная мне веб-страница. Запрос разделяется на серию пакетов, каждый из которых передается отдельно. Давайте проследим путь одного пакета от моего компьютера до сайта. Первый «прыжок» совершается с компьютера на встроенную с него карту wi-fi, где пакеты превращаются в радиоволны и перелетают по воздуху на мой домашний wi-fi-маршрутизатор. Если этот маршрутизатор недостаточно защищен, хакеры могут проникнуть в компьютер через wi-fiсоединение. Маршрутизатор еще раз преобразовывает сигнал и отправляет его моему местному интернет-провайдеру в быстро растущий городок под названием Кэльпепер. Это прекрасное местечко, но до центра киберпространства от него далековато. Поскольку город расположен далеко от зоны возможного ядерного взрыва, направленного на Вашинг- [[13]](#footnote-14)

Попе битвы

тон, именно здесь хранятся базы данных финансовых и правительственных институтов: например, узел AT&T (Американской телефонно-телеграфной компании) расположен на Аллее любовников, 13 456 (вот как!). Линия моего интернет-провайдера проходит через весь город до места, где электроны моего запроса конвертируются в фотоны, чтобы попасть в оптоволоконную сеть AT&T. Затем пакет попадает в Морристаун (штат Нью-Джерси), где передается на вашингтонский маршрутизатор AT&T, затем возвращается в Нью-Джерси, на этот раз в Мидлтаун. Мидлтаунский маршрутизатор передает пакет в первичному интернет-провайдеру Level3. Попадая в магистраль Level3, пакет проходит через три разных узла в Вашингтоне. К этому времени расстояние, пройденное пакетом по радиоволнам, медным проводам и высокоскоростным участкам оптокабелей, превысило 1300 километров, хотя оказался он на расстоянии всего 120 километров от места отправки. Последний маршрутизатор Level3, находящийся в Вашингтоне, передает его на огромной скорости в Чикаго (наконец-то мы хоть куда-то продвинулись), где он проскакивает еще два маршрутизатора Level3, а затем отправляется в Миннеаполис. Вместо того чтобы сразу попасть к нашему хостинг-провайдеру, пакет проходит еще 1120 километров до следующего маршрутизатора Level3, находящегося в офисе компании в Колорадо, откуда пересылается обратно интернет-провайдеру нашей компании, в Миннеаполисе, и на наш веб-сервер. Чтобы преодолеть расстояние в 1450 километров до Миннеаполиса, наш пакет прошел около 3220 километров, но весь этот процесс длился не более нескольких секунд.

Если бы кибервоинам захотелось отправить этот пакет в неправильном направлении или не дать ему попасть куда-либо, у них было бы минимум две возможности. Во-первых, как уже говорилось, можно было атаковать

99

Третья мировая война: какой она будет?

«справочную службу» Интернета — систему доменных имен и отправить меня на другую страницу, возможно, поддельную и очень похожую на ту, которая мне нужна, где я мог оставить номер своего банковского счета и пароль. Помимо вмешательства в систему доменных имен с целью перехвата запроса кибервоины могут атаковать саму систему. Так произошло в феврале 2007 года, когда шесть из тринадцати крупнейших доменных серверов высшего уровня подверглись DDoS-атаке. Как и в истории с Эстонией и Грузией, на серверы стали поступать тысячи запросов в секунду. Два атакованных сервера вышли из строя, в том числе и тот, который управляет трафиком Министерства обороны. Четыре сервера сумели справиться с атакой, перенаправив запросы на другие сервера, не тронутые хакерами. Атака продолжалась восемь часов, следы ее вели в Тихоокеанский регион. Хакеры остановились, либо испугавшись, что их обнаружат, либо, что более вероятно, потому, что они только тестировали свои возможности. В 2008 году Дэн Камински продемонстрировал, как искушенный противник может взломать систему. Он представил программу, которая открывает доступ к системе доменных имен и спокойно разрушает базу данных. После этого система начинает выдавать неверные номера. Даже неправильная адресация способна вызвать полный хаос в Интернете. Одна из компаний, занимающихся кибербезопасностью, нашла 25 разных способов взломать систему доменных имен, уничтожить или выкрасть данные.

Второе уязвимое место в Интернете — пограничный шлюзовый протокол. За несколько секунд и три тысячи километров пути моего пакета хакер имеет возможность перехватить его в момент перехода в сеть AT&T. Компания AT&T предоставляет самые безопасные и надежные интернет-услуги в мире, но и она уязвима. Когда пакеты [[14]](#footnote-15)

Попе битвы

попадают в магистраль, оказывается, что AT&T никак не связана с моей компанией. А кто связан? Пакеты проверяют базы данных всех крупных интернет-провайдеров. Там они находят информацию от Level3: «Если вы хотите попасть на mycompany.com, идите сюда». Так система маршрутизации регулирует трафик в пунктах объединения интернет-провайдеров, там, где один заканчивает работу, а другой начинает, на границе.

BGP— пограничный шлюзовый протокол — основная система, используемая для маршрутизации пакетов. На пакетах есть ярлыки с адресами «куда» и «откуда», а протокол BGP, как работник почты, решает, на какую сортировочную станцию отправить пакет. Протокол BGP, кроме того, устанавливает «равноправные» отношения между двумя разными маршрутизаторами двух разных сетей. Чтобы пакет перешел из AT&T в Level3, нужно, чтобы маршрутизаторы этих провайдеров имели BGP- соединение. Как говорится в отчете InternetSociety, некоммерческой организации, занимающейся развитием интернет-стандартов, «в протоколах BGPнет внутренних механизмов защиты от атак, которые изменяют, удаляют или фальсифицируют данные, что может привести к нарушению всего процесса маршрутизации в сети». То есть когда Level3 говорит: «Если вы хотите попасть на mycompany.com, идите сюда», никто не проверяет, правда ли это. BGP-система работает на доверии, а не по любимому принципу Рональда Рейгана «доверяй, но проверяй». Если какой-нибудь злоумышленник, сотрудник крупного интернет-провайдера, пожелает воспользоваться Интернетом в своих целях, он легко сможет это сделать, взломав таблицы пограничного шлюзового протокола. Это можно сделать и снаружи — достаточно изменить команды пограничного шлюзового протокола, и интернет-трафик не достигнет своего пункта назначения. [[15]](#footnote-16)

Третья мировая война: какой она будет?

Любой, кто занимается сетевым управлением в крупных интернет-провайдерах, знает об уязвимых местах системы доменных имен и протокола BGP.

Люди вроде Стива Кента из BBNLabsв Кембридже (штат Массачусетс) придумали несколько способов сокращения этих уязвимостей, но Федеральная комиссия по связи не требует от интернет-провайдеров применять эти разработки. Правительственные органы США используют безопасную систему доменных имен, но в коммерческой инфраструктуре такой практики не существует. Решения по системе доменных имен принимаются в неправительственной международной организации ICANN(Ассоциация по присвоению имен и номеров (портов) Интернета), где никак не могут прийти к соглашению о системе безопасности. В результате мишенью кибервоинов может являться сам Интернет, но большинство специалистов по кибербезопасности считают, что это маловероятно, поскольку Интернет необходим для осуществления атаки.

ICANNдемонстрирует еще одно уязвимое место Интернета — систему управления. На самом деле Интернетом никто не руководит. Во времена юности Интернета ARPA(Агентство по перспективным исследовательским проектам МО США) исполняло функции сетевого администратора, но сейчас этим никто не занимается. ICANNболее других организаций близка к тому, чтобы взять на себя ответственность за управление хотя бы частью Интернета. ICANNгарантирует, что веб-адреса будут уникальны. Компьютеры — логические устройства, и они не любят неопределенности. Если бы в сети Интернет существовало два разных компьютера с одним и тем же адресом, маршрутизаторы не знали бы, что делать. ICANNрешает эту проблему, ведя работу по присвоению адресов, но, решая одну из проблем управления Интерне- [[16]](#footnote-17)

Попе битвы

том, не занимается другими. Более десятка межгосударственных и неправительственных организаций играют различные роли в управлении Интернетом, но никакие полномочные органы не обеспечивают общего руководства или контроля.

Третье уязвимое место Интернета: все, что обеспечивает его работу, является открытым, незашифрованным. Когда вы перемещаетесь, большая часть информации пересылается открыто, в незашифрованном виде. Это как FM-радиостанция, которая транслирует песни PinkFloyd, и любой может настроиться на ее волну. Приемник, купленный в RadioShack, позволяет прослушивать переговоры дальнобойщиков и в большинстве городов — полицейских. В некоторых городах полиция даже зашифровывает сигналы, чтобы гангстерские банды не могли прослушивать их разговоры.

Интернет, в общем-то, работает по такому же принципу. Большая часть данных передается открыто, и только лишь небольшая доля трафика зашифрована. Единственная разница в том, что настроиться на чей-то интернет-трафик несколько сложнее. Интернет-провайдеры имеют к нему доступ (и могут предоставлять его правительству), поставщики услуг электронной почты вроде gmailпоступают так же (даже если отрицают это). В обоих случаях вы, пользуясь их услугами, соглашаетесь на то, что они могут видеть ваш веб-трафик или электронные письма. Третья сторона, чтобы получить доступ к трафику, должна его отслеживать, используя для перехвата снифферы.

Сниффер — это устройство, перехватывающее интернет-трафик, которое может быть установлено в любой операционной системе и применяется для перехвата трафика пользователей локальной сети. Когда сниффер попадает в локальную сеть, любой абонент системы может [[17]](#footnote-18)

Третья мировая война: какой она будет?

перехватить весь трафик. Стандартный протокол Ethernetдает вашему компьютеру команду игнорировать все, что не адресовано ему, но это не значит, что он должен так поступать. Продвинутый сниффер способен просматривать весь трафик сети Ethernet. Ваши соседи могут узнать все, что происходит на вашей интернет-улице. Еще более совершенные снифферы могут обмануть сеть посредством так называемого «незаконного посредника». Маршрутизатор считает, что сниффер является компьютером пользователя. Вся информация посылается на сниффер, копируется и только потом уже попадает к реальному адресату.

На многих сайтах (но не везде) используются безопасные каналы связи, когда вы входите в систему, чтобы ваш пароль не был открыт любому, кто пытается его перехватить. Когда передача пароля завершена, вас из соображений стоимости или скорости зачастую переводят в небезопасный режим. Но даже если передачу невозможно перехватить или данные посылаются в нечитаемом виде, это не значит, что вы в безопасности. Регистратор работы клавиатуры, небольшая зловредная программа, без вашего ведома установленная на ваш компьютер, отслеживает все, что вы печатаете, а затем тайно передает эту информацию. Конечно, чтобы такой регистратор проник в ваш компьютер, вы должны совершить какую-то глупость: к примеру, посетить зараженный сайт или загрузить файл из электронного письма от того, кому вы не доверяете. В октябре 2008 года на ВВС сообщали о том, что «ученые из SecurityandCryptographyLaboratoryиз SwissEcolePolytechniqueFederaleпродемонстрировали, что злоумышленники могут с помощью радиоантенны „полностью или частично распознавать нажатие кнопок клавиатуры", улавливая электромагнитное излучение, возникающее при нажатии». [[18]](#footnote-19)

Поле битвы

Четвертым уязвимым местом Интернета является его способность распространять вредоносные программы — вирусы, «черви» и весь так называемый мэлвер. Они используют как дефекты программ, так и ошибки пользователя, к примеру переход на зараженный сайт или открытие сомнительных прикрепленных файлов. Вирусы — это программы, передающиеся от пользователя к пользователю (через Интернет или через портативные носители, например флэш-накопители), которые нарушают нормальную работу компьютера, обеспечивают тайную точку доступа к системе либо крадут конфиденциальные сведения. «Червям» не требуется помощь человека для перехода к другому пользователю, они копируют сами себя, используя известные уязвимые места и прокладывая путь по Интернету. С помощью фишинга злоумышленники стараются заставить пользователя выдать важную информацию — номер банковских счетов, код доступа. Для этого создают электронные сообщения и поддельные веб-сайты, якобы связанные с законным бизнесом, чаще всего банковским.

Весь трафик перемещается по Интернету практически или совсем бесконтрольно. Почти всегда пользователь сам ответствен за собственную безопасность. Большинство интернет-провайдеров не предпринимают даже самых простых шагов для того, чтобы воспрепятствовать вредоносному трафику, отчасти потому, что это дорого и замедляет работу, а также из соображений прайвеси.

Пятое уязвимое место Интернета в том, что это одна большая децентрализованная сеть. Создатели Интернета не хотели, чтобы его контролировали правительства, ни в одиночку, ни коллективно, поэтому они спроектировали систему, в которой приоритет отдается децентрализации, а не безопасности. Основные идеи Интернета начали формироваться в начале 1960-х, и современный Интернет глубоко пропитан настроениями той эпохи. Многие счи-

 1 Р 5

Третья мировая война: какой она будет?

тают Интернет изобретением военных, на самом деле он детище хиппи из кампусов Массачусетского технологического института, Стэнфорда и Беркли. Их финансировало управление перспективного планирования оборонных научно-исследовательских работ, но сеть управления перспективных исследовательских программ была создана не только для обеспечения коммуникаций Министерства обороны. Изначально она связывала четыре университетских компьютера: Калифорнийского университета в Лос- Анджелесе, Стэнфордского университет, Калифорнийского университета в Санта-Барбаре и, как ни странно, Университета Юты.

После создания сети ARPANETпионеры Интернета быстро переключились на то, как связать ARPANETс другими развивавшимися тогда сетями. Для этого они разработали протокол, используемый и по сей день. Роберт Канн, один из тех десяти человек, которых обычно считают создателями Интернета, сформулировал четыре его принципа. Их стоит привести здесь:

1. Каждая сеть должна сохранять индивидуальность. Для подключения к Интернету сети не должны подвергаться переделкам.
2. Коммуникации должны идти по принципу «максимум возможного». Если пакет не прибыл в пункт назначения, источник должен передать его повторно.
3. Для связывания сетей должны использоваться черные ящики (позднее их назовут шлюзами и маршрутизаторами). Шлюзы не должны хранить информацию о протекающих через них потоках данных. Они должны оставаться максимально простыми, без использования сложных средств восстановления после разного рода сбоев. [[19]](#footnote-20)

Попе битвы

1. Не должно существовать глобальной системы управления.

Протоколы, разработанные на основе этих принципов, с одной стороны, содействовали широкому развитию сетевых технологий и созданию Интернета, каким мы знаем его сегодня, но с другой — именно они посеяли семена проблем безопасности.

Авторы этих фундаментальных принципов и представить не могли, что кто-нибудь помимо исполненных благих намерений ученых из университетов и правительственных организаций будет использовать Интернет. Он предназначался для исследовательских целей, обмена идеями и управления важнейшими системами. Таким образом, он должен был стать сетью сетей, а не сетями правительства, финансовых организаций и т. д. Он был разработан для тысяч исследователей, а не для миллиардов пользователей, которые не знакомы между собой и не доверяют друг другу.

На протяжении 1990-х годов Интернет считался силой добра. Не многие сторонники Интернета готовы были признать, что он нейтрален. Он облегчает обмен информацией между учеными и ведение законной электронной коммерции, но также позволяет террористам обучать новобранцев или транслировать в прямом эфире казнь в провинции Анбар. Интернет, во многом как территории племен в Пакистане или южноамериканский кокаиновый треугольник, не подконтролен никому, и поэтому сюда стягивается преступность.

Лари Робертс, написавший первую версию протокола управления передачей, сознавал, что создает небезопасную систему, но не хотел замедлять развитие новой сети и тратить время на настройку программного обеспечения. У него есть простое объяснение — это была маленькая [[20]](#footnote-21)

Третья мировая война: какой она будет?

сеть. Вместо того чтобы пытаться написать безопасную программу, контролирующую распространение информации, Робертс пришел к выводу, что значительно проще защитить линии передачи, зашифровав соединения между всеми и каждым компьютером сети. В конце концов, первые маршрутизаторы стояли в безопасных помещениях в правительственных организациях и академических лабораториях. Самое главное было — защитить информацию во время передачи между двумя точками сети. В том решении не учитывалось будущее распространение новой технологии за пределы шестидесяти с небольшим компьютеров, которые тогда составляли всю сеть. Этими компьютерами управляли проверенные люди. Присоединиться к сети могли только проверенные организации, преданные идее продвижения научных достижений. Благодаря такой немногочисленности, если в сети происходило что-нибудь плохое, не составляло особого труда узнать, кто виноват.

Затем Винт Серф покинул Агентство по перспективным исследовательским проектам и присоединился к МСГ. Винт мой друг, с которым я не согласен по вопросам безопасности Интернета. Но Винт — один из той группы людей, которые по праву зовутся отцами Интернета, поэтому его мнение по связанным с Интернетом вопросам значительно важнее моего. Кроме того, Винт, которого вы никогда не увидите без галстука-бабочки, — обаятельный парень и теперь работает в Google, что опять же говорит в его пользу. MCI(которая теперь является частью AT&T) была первой телекоммуникационной компанией, проложившей часть магистральных каналов и предложившей [[21]](#footnote-22)

Попе битвы

новые технологии корпорациям и даже через интернет- провайдеров домашним пользователям. Винт создал протокол управления передачей вместе с проблемами безопасности, которые теперь стоят перед значительно более широкой аудиторией и которые нельзя решить посредством кодирования соединений. Ведь никому не было точно известно, кто присоединялся к сети MCI.

В любой крупной системе есть слабые места. Сегодня сеть Интернет разрослась настолько, что уже IP-адреса подходят к концу. Когда Интернет развивался, изобретатели придумали систему для идентификации каждого устройства, которое будет подключаться к сети. Они решили, что все IP-адреса должны состоять из 32-разрядов, чего достаточно для присвоения 4,29 миллиарда IP- адресов. Они и представить не могли, что когда-нибудь нам потребуется больше. Сейчас на планете проживает порядка 6,8 миллиарда человек. По текущим стандартам, каждый второй обладает более чем одним IP-адресом. Даже сегодня этого недостаточно. Запад становится все более зависимым от Интернета, растет число пользователей в странах второго и третьего мира, поэтому 4,29 миллиарда IP-адресов может не хватить на всех, кто пожелает присоединиться к Всемирной паутине. С проблемой нехватки адресов еще можно справиться, если мы перейдем на протокол IPv6 до того времени, как исчерпаются все IP-адреса IPv4, то есть если через пару лет большинство устройств смогут работать по новому стандарту. Но если на мгновение задуматься, возникнет повод для переживаний.

Пентагон рисует такой сценарий на не слишком далекое будущее. Каждый солдат в зоне конфликта станет узлом (хабом) сети, и около десятка устройств, которые он использует, будут также подключены к сети, для чего им понадобятся уникальные IP-адреса. Если вы прогуля- [[22]](#footnote-23)

Третья мировая война: какой она будет?

етесь по какому-нибудь магазину современной бытовой техники, то заметите, каким количеством стиральных машин, фенов, посудомоечных машин, микроволновых печей и холодильников можно управлять через Интернет. Если вы задержались на работе, но хотите, чтобы к вашему возвращению духовка нагрелась до 220 градусов, вы заходите на сайт, получаете доступ к своей духовке и указываете нужную температуру прямо с рабочего стола компьютера. Все это значит, что к тому времени, как мы перевалим за 4,29 миллиарда веб-адресов, зависимость нашего общества от Интернета невероятно возрастет и коснется всего, начиная от управления термостатами и заканчивая обороной страны, а проблемы безопасности усугубятся. О том, что это значит для конфликтов в реальном мире, большинство политиков из Пентагона до недавних пор предпочитали не думать. Ведь если у вас есть возможность воздействовать на разные устройства через Интернет, вам под силу не только украсть деньги. Вы можете нанести реальные повреждения, в том числе и нашим вооруженным силам.

Программное и аппаратное

ОБЕСПЕЧЕНИЕ

Из трех факторов, которые делают кибервойну возможной, самым важным, пожалуй, являются ошибки в программном и аппаратном обеспечении. Все устройства, которые мы с вами обсуждали (терминалы ЭВМ и ноутбуки, маршрутизаторы и коммутаторы, почтовые и веб-серверы) производятся разными компаниями. Не- [[23]](#footnote-24)

Попе битвы

редко программное обеспечение, управляющее работой устройств, делают сразу несколько компаний. На американском рынке большая часть ноутбуков производится Dell, HPи Apple(их догоняет китайская компания Lenovo, купившая подразделение IBM, занимавшееся производством переносных ЭВМ). Большие маршрутизаторы выпускаются в основном компаниями Ciscoи Juniper, а теперь еще и китайской Huawei. Серверы производят HP, Dell, IBMи немало других производителей, в зависимости от их назначения. Программное обеспечение создают Microsoft, Oracle, IBMи Appleи целый ряд других компаний. Хотя эти корпорации американские, компьютеры (и программный код) производятся в разных местах.

В книге WorldIsFlat(«Плоский мир») Томас Фридман описывает процесс получения ноутбука DellInspiron 600mначиная с телефонного заказа, который связал его с представителем службы по работе с покупателями в Индии, и заканчивая его доставкой к дверям его дома в Мэриленде. Компьютер был создан на фабрике в Пинанге (Малайзия). Он — результат сотрудничества группы инженеров Dell, находящихся в Остине, и конструкторов из Тайваня. Аппаратная часть была выполнена конструкторами из тайваньской команды. Остальные 30 ключевых компонентовDellприобрел у других поставщиков. Процессор Intelмог быть сделан на Филиппинах, в Коста-Рике, Малайзии или Китае. Памятью занималась корейская компания Samsungили другие менее известные компании из Германии или Японии. Видеокарта прибыла с одной из двух фабрик в Китае. Материнская плата хоть и спроектирована на Тайване, вероятно, была сделана на одном заводов в континентальном Китае. Клавиатура поступила с одной из китайских фабрик, две из которых принадлежат тайваньским компаниям. Плата беспроводной связи произ-

Третья мировая война: какой она будет?

ведена либо американской компанией в Китае, либо китайской компанией в Малайзии или на Тайване. Жесткий диск мог быть выпущен американской компанией Seagateв Сингапуре, Hitachiили Fujitsuв Тайланде либоToshibaна Филиппинах.

Все это было собрано на фабрике в Малайзии, а на жесткий диск записан образ операционной системы WindowsХР (и, возможно, WindowsOffice). Программный код этой системы, насчитывающий более 40 миллионов строк, писался как минимум в десяти разных местах мира. После того как на компьютер установили программное обеспечение, его запаковали и поместили ящик со 150 такими же ноутбуками и отправили на «боинге-747» в Нашвилл. Отсюда ноутбук забрала служба доставки посылок и отправила его Фридману. В общей сложности, гордо сообщает Фридман, «в цепочку поставки моего компьютера, включая поставщиков, вошло около 400 компаний в Северной Америке, Европе и главным образом Азии».

Почему Фридман уделяет целых шесть страниц своей книги геополитическим аспектам? Потому что он верит, что цепочка поставок, объединившая разрозненные комплектующие в один компьютер, связывает страны, ставшие частью этого процесса, следовательно, межгосударственные конфликты в форме, характерной для XX столетия, в XXI веке менее вероятны. Так Фридман модернизирует свою «Теорию золотых арок» из предыдущей книги, согласно которой две страны, в которых есть McDonald’s, никогда не станут воевать друг с другом. Цепочка поставок — это микроэкономический пример коммерческой деятельности, которая, как верят многие теоретики международных отношений, так выгодна для стран, что даже война не будет стоить потенциальных экономических потерь. Фридман рассматривает предотвращенный кризис 2004 года, когда тайваньские полити- [[24]](#footnote-25)

Попе битвы

ки, твердившие об автономии, потерпели поражение на выборах. В рекламном стиле Фридман заявил, что «материнская плата подкупила Родину-мать», и пришел к выводу: статус-кво экономических отношений оказался для тайваньских избирателей фактором куда более важным, чем независимость. Или, возможно, тайваньские избиратели просто не хотели погибнуть в результате китайской оккупации, которой, по сути, и грозил Китай в случае объявления Тайванем независимости. Цепочки поставок для производства компьютеров, которые, по мнению Фридмана, снижают вероятность военных конфликтов, могут увеличить вероятность кибервойны или, по крайней мере, вероятность того, что китайцы победят при любом столкновении. На каждом этапе цепочки поставок, благодаря которой на свет появился компьютер Фридмана (или ваш компьютер, или AppleMacBookPro, на котором я пишу эту книгу), возникают уязвимые места, как правило, случайно, но, наверное, отчасти и намеренно. Они и могут послужить как мишенью, так и оружием кибервойны.

Программное обеспечение является посредником между человеком и компьютером и переводит человеческое намерение посмотреть фильм в режиме онлайн или почитать блог на язык, понятный машине. Компьютеры — это просто эволюционировавшие калькуляторы. На заре развития вычислительной техники ученые осознали, что электрические импульсы можно использовать для представления единиц, а отсутствие импульса — нулей, как точки и тире в азбуке Морзе. Десятичную систему счисления, которую используют люди, потому что у нас десять пальцев, легко перевести в двоичный код так, чтобы при нажатии на электронном калькуляторе кнопки «5» посылалась цепочка импульсов — 101 — пятерка в двоичной системе счисления. Простое электронное сообщение

 113

Третья мировая война: какой она будет?

преобразовывается в электрические импульсы, которые передаются по медным проводам и оптоволоконным кабелям, а затем преобразуются в читабельные для нас сообщения. Для того чтобы это происходило, кто-то должен создать инструкции, понятные компьютеру. Эти инструкции пишутся на языках программирования как компьютерный код, а люди, которые пишут код, как правило, делают ошибки.

Очевидные ошибки исправляются, иначе программа не функционирует так, как нужно, но менее явные остаются и могут быть позднее использованы для получения доступа к коду. Поскольку вычислительные системы работают быстрее, компьютерные программы становятся сложнее, чтобы использовать все возможности новых скоростей и мощности. В Windows95 было менее 10 миллионов строк кода, в WindowsХР их уже 40 миллионов, а в WindowsVista— более 50. За десять с небольшим лет количество строк увеличилось в пять раз, и во столько же возросло количество ошибок. Многие из этих ошибок позволяют хакерам заставлять программу делать то, для чего она не предназначалась. Для того чтобы использовать популярное программное обеспечение в собственных целях, например получить статус администратора, хакеры разрабатывают небольшие приложения — апплеты, которые учитывают особенности программного обеспечения, слабые места и ошибки конфигурации системы. Поскольку компьютерная преступность — это большой бизнес, подготовка к отражению кибератак финансируется столь же хорошо, а хакеры и кибервоины постоянно разрабатывают новые способы обмануть системы. Приложения, создаваемые хакерами, называются вредоносным ПО, или мэлвером. В 2009 году новая разновидность мэлвера появлялась в киберпространстве в среднем каждые 2,2 секунды. Посчитайте: три-четыре крупнейшие компании по [[25]](#footnote-26)

Попе битвы

производству антивирусных программ пользуются сложнейшими схемами отслеживания нового мэлвера, но они находят и блокируют только одну из десяти вредоносных программ. Пока «фикс» — компонент программного обеспечения, блокирующий мэлвер, — доходит до клиентов антивирусной компании, проходят дни, а иногда недели. На протяжении этого времени коммерческие компании, правительственные учреждения и рядовые пользователи остаются беззащитными.

Часто вредоносные программы поджидают вас на совершенно безобидных сайтах. Вы заходите на сайт вашингтонского научного центра, чтобы ознакомиться с последними исследованиями по важной политической проблеме. Научным центрам, как известно, денег вечно не хватает, поэтому они не уделяют достаточного внимания созданию безопасных и надежных сайтов. Пока вы читаете о недавних махинациях вокруг проблем здравоохранения и прав человека в Китае, небольшая вредоносная программка загружается на ваш компьютер. Вы об этом не знаете, но вашему новому «другу» из Белоруссии известна каждая клавиша, которую вы нажимаете. Что будет, когда вы зайдете на свою личную страницу в банке или в защищенную сеть своего работодателя? Нетрудно догадаться.

Самая распространенная ошибка — переполнение буфера. Код веб-страницы должен быть написан так, чтобы пользователь имел возможность ввести фиксированный объем данных, например имя пользователя и пароль. Вспомните Twitter, где вы за раз можете ввести не более 140 символов. Но если разработчик кода забывает ограничить количество символов, пользователь может ввести что-нибудь лишнее. И вместо имени пользователя и пароля там окажутся несколько строк кода, дающих вам права администратора. Представьте, как эти команды оказыва- [[26]](#footnote-27)

Третья мировая война: какой она будет?

ются в полях ввода персональных данных пользователя и превращаются в приложение. Ваша страничка начинает думать, что это вошел системный администратор, и — пинг! — нарушитель внутри.

Ошибки программного кода непросто обнаружить. Даже специалистам бывает сложно идентифицировать ошибки или слабые места в нескольких строках кода. А если речь идет о миллионах строк? Конечно, существуют программы, проверяющие корректность написанного кода, но и им не под силу выловить все ошибки. Каждая новая строка кода увеличивает количество багов программы. В некоторых случаях программисты добавляют эти баги намеренно. Самый знаменитый пример такой «добавки» произошел, когда шутник из Microsoftдобавил в Excel97 программу-симулятор полетов. В Microsoftоб этом узнали лишь тогда, когда люди стали благодарить компанию за такой подарок. Возможно, программисты сделали это ради развлечения, выгоды или по просьбе службы внешней разведки; но какими бы ни были мотивы, невозможно гарантировать то, что в массовых программах не найдется пары строк кода, которые дадут кому-нибудь возможность несанкционированного доступа. В троянском коне прятались «коммандос», в современных «троянах» прячутся команды вредоносного кода. При открытии нового документа в Excelможно было нажать F5, ввести в строку «Х97:Ь97», нажать клавишу Enter, а затем Tab. И, о чудо, вы оказывались в ячейке М97. Достаточно было вызвать «Мастер диаграмм», удерживая кнопки CTRL+SHIFT, и — пинг! — на экране появлялась программа-симулятор полетов.

Иногда разработчики кода специально оставляют «черные ходы», чтобы иметь возможность обновить код в дальнейшем. Но иногда они делают это по менее достойным причинам. Порой другие люди — хакеры и кибервои- [[27]](#footnote-28)

Попе битвы

ны — используют их для того, чтобы незаметно проникнуть в сеть. Когда кто-нибудь взламывает программный продукт (в процессе его разработки или позднее), он может не только украсть копию программы, но и добавить в нее что-нибудь лишнее. Умышленно оставленные «черные ходы», так же как и те, что появляются в результате ошибок, позволяют хакеру получить неограниченный доступ. Хакеры продают и покупают друг у друга «права доступа». Если у вас есть права неограниченного доступа к программе или сети, вы получаете все права и полномочия создателя программы или администратора сети. Вы можете изменять программу, добавлять учетные записи пользователей — делать все что угодно. И, что важно, вы можете уничтожить все следы вашего пребывания здесь, как вор, стирающий отпечатки пальцев и сметающий следы ног.

Разработчики кода могут оставлять не только «черный ход», но и логические бомбы. Логическая бомба в своей самой простой форме — это устройство, которое уничтожает программное обеспечение компьютера, превращая его в бесполезную груду металла. Более совершенные логические бомбы могут сначала дать команду аппаратным средствам сделать что-нибудь во вред себе, например вызвать скачок напряжения в электрической сети или заставить самолет уйти в пике. Затем стирается все, включая саму бомбу. АНБ все больше беспокоит проблема логических бомб, поскольку они, скорее всего, уже заложены по всей нашей электрораспределительной сети. В этом есть определенная ирония, ведь именно американские военные изобрели такую форму оружия. Одна из первых логических бомб, которая, возможно, и стала предвестником кибервойны, была создана еще до эпохи массового распространения Интернета. В начале 1980-х советское руководство составило для своей разведыва- [[28]](#footnote-29)

Третья мировая война: какой она будет?

тельной службы КГБ список западных технологий, которые нужно было выкрасть. Один агент КГБ, у которого был доступ к этому списку, решил, что предпочтет провести остаток дней, потягивая вино в парижском кафе, а не замерзая в Сибири, и поэтому передал этот список французской разведке в обмен на французское гражданство. Франция же, будучи участником Западного альянса, передала его США. КГБ, не зная о том, что у западной разведки есть этот список, продолжал работать. Когда Франция передала список ЦРУ, президент Рейган дал добро на «помощь» Советскому Союзу. ЦРУ начало специальную программу, позволившую Советскому Союзу выкрасть необходимые технологии, но предварительно добавила незначительные ошибки в схемы истребителей-невидимок и космического вооружения. Но не чертежи были основной целью КГБ. Прежде всего России были нужны коммерческие и промышленные технологии, в частности для нефтяной и газовой промышленности. Нефть и газ должны пройти по трубопроводам тысячи километров, чтобы попасть к западным или российским покупателям. В России ощущался острый недостаток технологий автоматизированного управления трубопроводами. Советский Союз пытался купить их у американских компаний, но получил отказ, в связи с чем решено было выкрасть их у канадской фирмы. ЦРУ внедрило вредоносный код в программное обеспечение этой компании, и, когда русские украли код и стали использовать его для управления своими трубопроводами, все поначалу шло отлично. Но какое-то время спустя программа начала ошибаться. В одном сегменте трубопровода программа заставила насос работать на полную мощность, а в другом — закрыла клапан. Давление увеличилось, и произошел самый крупный неядерный взрыв за всю историю — более трех килотонн. [[29]](#footnote-30)

Попе битвы

Если холодная война с Россией разгорится снова или если нам придется воевать с Китаем, превосходство окажется на стороне наших противников. Передовой арсенал, которым обладают Соединенные Штаты, может обернуться против нас самих. Наши военно-воздушные, сухопутные и военно-морские силы зависят от сетевых технологий и уязвимы перед кибероружием, которое разработали Китай и другие противники, чтобы уничтожить традиционное американское превосходство. Вооруженные силы США не способны обойтись без Интернета, как не способен обойтись без него крупнейший интернет-магазин Amazon.com. Материально-техническое обеспечение, управление и контроль, вывод флота на позиции, наведение орудий на цели — все базируется на программном обеспечении и прочих связанных с Интернетом технологиях. И все это так же не защищено, как ваш домашний компьютер, поскольку использует те же несовершенные технологии и то же небезопасное программное и аппаратное обеспечение.

С ростом аутсорсинга увеличивается количество иностранных соисполнителей из Индии и Китая, что, как говорит Фридман, лишь повышает вероятность того, что наши столь же сильные соперники уже сумели проникнуть в главные компании по выпуску программного обеспечения и внедрили свои коды в программы, которым мы привыкли доверять. Эксперты в области вычислительной техники давно уже считают, что коды двух самых распространенных операционных систем написаны хуже всего и не отлажены. Это операционные системы MicrosoftWindows, предназначенные для компьютеров и ноутбуков, и Cisco— для маршрутизаторов. Обе системы про- приетарны, что означает, что они не находятся в свободном доступе. Вы можете купить программное обеспечение как конечный продукт, но вы не имеете доступа к исходно- [[30]](#footnote-31)

Третья мировая война: какой она будет?

му коду. Было несколько случаев, когда защита Microsoftне помогла похитить исходный код, что позволило хакерам исследовать программные ошибки и найти способы использовать их.

Как я упоминал во второй главе, Китай в конечном итоге принудил Microsoftк сотрудничеству. Китайское правительство объявило, что вместо использования Microsoftбудет разрабатывать собственную систему RedFlagна основе Linux. Вскоре после этого Microsoftначала переговоры с официальным Пекином на высочайшем уровне, а консультантом выступил Генри Киссинджер. Microsoftснизила цену, предоставил китайцам свой закрытый код, и открыла научно-исследовательскую лабораторию в Пекине (которая напрямую связана со штаб-квартирой Microsoft). Сделка состоялась, президент Китая посетил затем Билла Гейтса в его доме близ Сиэтла. Китайское правительство теперь пользуется программами Microsoft, но только с добавлением специального модуля шифрования, подготовленного китайской стороной. Один бывший офицер американской разведки сказал нам: «Наверное, это значит, что никто не сможет легко взломать Windows, чтобы заняться шпионажем в Китае. Но это определенно не значит, что Китай не сумеет взломать Windows, чтобы пошпионить за остальными».

То, что можно сделать с миллионами строк кода, можно сделать и с миллионами микросхем внутри компьютеров, маршрутизаторов, серверов. Чипы — это кремниевые внутренности компьютера. Их можно модифицировать, так же как компьютерные программы. Большинство специалистов не смогут, посмотрев на микросхему, определить, есть ли в ней лишние элементы или «черные ходы». Компьютерные микросхемы изначально выпускались в США, но сейчас в основном производятся в Азии. У американского правительства когда-то было собственное про- [[31]](#footnote-32)

Попе битвы

изводство чипов, однако этот завод не поспевает за развитием технологий и не может выпускать микросхемы, необходимые для современных систем.

Недавно второй крупнейший в мире производитель микросхем, AMD, объявил о намерении построить самый передовой завод по производству микропроцессоров в северной части штата Нью-Йорк. Отчасти он будет финансироваться правительством, но не американским — в AMDвкладывают средства Объединенные Арабские Эмираты.

Дело не в том, что американское правительство не видит проблем, что программное и аппаратное обеспечение производится по всему миру. На самом деле в последний год своего президентства Джордж Буш-младший подписал PDD-54 — секретный документ, где намечены шаги, которые необходимо предпринять для лучшей защиты от кибернападения. Одной из таких программ должна стать «безопасная цепочка поставок», но американскому правительству будет трудно покупать программное обеспечение и аппаратные средства исключительно в США.

Техника, контролируемая

ИЗ КИБЕРПРОСТРАНСТВА

Ни уязвимость архитектуры Интернета, ни дефекты программного обеспечения и аппаратных средств не объясняют, как кибервоины могут заставить компьютеры начать атаку. Как чья-то разрушительная рука может протянуться из киберпространства в реальный мир и нанести серьезные повреждения? Ответ мы найдем, вернувшись в Интернет и киберпространство американской промышленности 1990-х. В течение десятилетия руко- [[32]](#footnote-33)

Третья мировая война: какой она будет?

водители ряда информационно-технологических компаний рьяно демонстрировали прочим корпорациям, как им удается экономить огромные суммы денег, пользуясь компьютерными системами. Помимо электронной почты или электронной обработки информации практика деловых отношений включала в себя системы автоматизированного управления, мониторинг материально-производственных запасов, доставку «точно в срок», аналитику баз данных, программы искусственного интеллекта. Главный исполнительный директор одной компании с воодушевлением рассказывал мне в конце 1990-х, как он использует эти возможности в собственной фирме: «Если кто-нибудь хочет что-то приобрести, он заходит на наш сайт. Указывает свои требования и нажимает кнопку „купить". Наша система извещает производителей, планирует доставку компонентов на сборочный завод, составляет расписание сборки и доставки. На сборочном заводе промышленные роботы собирают продукт и упаковывают его в коробку с адресом получателя. Нам не принадлежат ни сервер, который принимает заказ, ни заводы по изготовлению комплектующих, ни сборочный завод, ни самолеты, ни грузовики. Все привлекается со стороны, и все это — доставка “точно в срок"».

У него был только исследовательский отдел, проектная группа и несколько руководителей. Доходность подобных компаний, как и всей американской экономики в целом, росла. И этот рост в 1990-х был обеспечен глубоким проникновением информационно-технологических систем в компании. Во многих сферах промышленности управление, которое когда-то осуществлялось вручную, было передано компьютерам. Представьте фабрику или завод XX столетия, где парень в каске получает по телефону задание от бригадира пойти и закрутить клапан или изменить какие-нибудь настройки. Я прекрасно вижу та- [[33]](#footnote-34)

Попе битвы

кую картину — мой отец работал в подобном месте. Сегодня требуется меньше людей, системы цифрового управления следят за работой и посылают команды машинам, клапанам, роботизированным рукам, лампам, камерам, дверям, лифтам, поездам, самолетам. Интеллектуальные системы инвентаризации следят за продажами в режиме реального времени и посылают заказы на изготовление и доставку комплектующих часто без вмешательства человека. Переход к системам цифрового управления был быстрым и абсолютным. На рубеже тысячелетий старые системы в большинстве своем были отправлены на пенсию, не удостоившись даже места на складе. Как Кортес сжег свои корабли, прибыв в Новый Свет, американские компании и правительственные организации построили новый мир, в котором существуют лишь автоматизированные системы. Когда компьютеры выходят из строя, работники ничего не делают или идут домой. Попробуйте сейчас найти пишущую машинку, и вы получите картину этой новой реальности.

Киберпространство в целом изобилует программными и аппаратными проблемами. Компьютерные сети жизненно необходимы для работы компаний и правительственных организаций. Выражение «жизненно необходимы» выбрано неспроста, поскольку оно отражает тот факт, что мы зависим от компьютерных систем. Без них ничего не работает. Если они получат искаженную информацию, системы продолжат работать, но будут функционировать неправильно.

Несмотря на огромные суммы, которые тратятся на разработку систем компьютерной безопасности, внедрить в сети ложные данные не составит труда. А значит, системы отключаются, нанося вред себе или чему-то еще, посылают людей и отправляют вещи в неправильном направлении. В 3:28 пополудни 11 июня 1999 года в Беллин- [[34]](#footnote-35)

Третья мировая война: какой она будет?

геме (штат Вашингтон) взорвался трубопровод. Бензин начал вытекать ручьем и быстро распространился более чем на километр. Затем он загорелся. Погибли два десятилетних мальчика и восемнадцатилетний юноша. Близлежащая муниципальная водоочистная станция серьезно пострадала от огня. Когда специалисты из Национального совета по безопасности транспорта США выясняли, почему взорвался трубопровод, они особенно подчеркивали «эксплуатационные качества и безопасность системы оперативного управления и обработки данных (SCADA)». Иными словами, программа вышла из строя. В отчете нет вывода о том, что взрыв был вызван вмешательством хакера, но из анализа очевидно, что трубопроводами, подобными беллингемскому, можно управлять из киберпространства.

Самый яркий пример уязвимости компьютерного управления также связан с системой, от которой зависит все, — электрораспределительной. В результате отмены государственного регулирования в 1990-х годах электроэнергетические компании были разделены на производящие и транспортировочные. Им разрешено было покупать и продавать электроэнергию. В то же время они, как и другие компании, переходили на компьютерное управление. Автоматизация распространилась на сферы покупок и продаж, производство и транспортировку. SCADA-система диспетчерского управления и сбора данных применялась на всех подстанциях, трансформаторах, генераторах электрических компаний. SCADAполучала и отправляла сигналы на тысячи устройств, образующих энергетическую систему.

Эти управляющие программы посылают сигналы на приборы, чтобы распределять электрическую нагрузку на различных участках. Эти сигналы чаще всего передаются по внутренней компьютерной сети, а иногда по радио. [[35]](#footnote-36)

Попе битвы

Как показало одно исследование, пятая часть устройств, входящих в состав электросетей, имеет беспроводную точку доступа, 40 % связаны с внутренней компьютерной сетью компании и почти половина имеет прямую связь с Интернетом. Подключение к сети Интернет было организовано для того, чтобы предприятия имели возможность проводить удаленную диагностику. Другое исследование выявило, что в одной крупной энергетической компании 80 % оборудования связано с интранетом, а из интранета, разумеется, есть выход в Интернет. Следовательно, если вы сумеете проникнуть из Интернета в интранет, то сможете управлять работой электросети, сидя где-нибудь в уютном интернет-кафе в другой части планеты. Многочисленные проверки электроэнергетических компаний, проведенные уважаемыми экспертами по кибербезопасности, показали, что подобное очень даже осуществимо. Что же можно сделать с системой управления электросети?

В 2003 году Slammer(компьютерный «червь») внедрился в систему управления электрораспределительной сети и замедлил ее работу. Сбой в работе SCADAснизил скорость управления. Поэтому когда упавшее дерево спровоцировало скачок напряжения на линии в Огайо, аппаратура, которая должна была остановить каскадный эффект, не сработала, пока авария не достигла южной части Нью-Джерси. В результате 8 штатов, 2 канадские провинции и 50 миллионов человек остались без электричества и всего того, для чего требуется электричество (к примеру, без водоснабжения в Кливленде). Аварию вызвало дерево, но такого же эффекта мог добиться хакер, отдав системе соответствующую команду. В 2007 году эксперт ЦРУ Том Донахью был уполномочен сообщить специалистам, что известны случаи, когда хакеры поступали именно так. Хотя Том и не сказал, какая авария [[36]](#footnote-37)

Третья мировая война: какой она будет?

стала результатом такого действия, позже стало ясно, что имелся в виду инцидент в Бразилии. Блэкаут в 2003 году продлился несколько часов, а в некоторых местах растянулся на четыре дня. В Окленде (Новая Зеландия) в 1998 году повреждение, вызванное перегрузкой линий электропередач, привело к отключению электричества, и город на пять недель остался без света. Если управляющая система передаст слишком много энергии по линии высокого напряжения, перегрузка может нарушить работу сетевых фильтров в домах и офисах, из-за чего пострадают электронные приборы, начиная от компьютеров и заканчивая телевизорами и холодильниками, как недавно произошло в моем округе во время грозы.

Еще более наглядным примером того, как с помощью компьютерных команд можно вызвать саморазрушение систем и приборов, являются генераторы электроэнергии. Генераторы, вращаясь, вырабатывают электроэнергию. В Соединенных Штатах и Канаде частота вращения генераторов составляет 60 МГц. Когда генератор запускается, он не подключается к сети до тех пор, пока не разгонится до этой частоты. Если он соединится с сетью раньше времени, энергия остальных работающих генераторов может уничтожить медленно работающий генератор.

Чтобы проверить, способны ли кибервоины разрушить генератор, федеральная правительственная лаборатория в Айдахо провела эксперимент под кодовым названием «Аврора». Исследователи использовали стандартную управляющую сеть и подключили ее к генератору. Затем хакеры взломали сеть из Интернета и нашли программу, которая меняет частоту вращения генератора. Одно нажатие кнопки — и генератор мог пострадать. Как и многое другое, огромные генераторы, которые снабжают энергией Соединенные Штаты, заказываются по принципу доставки «точно в срок». Они не лежат на полках магазинов [[37]](#footnote-38)

Попе битвы

в ожидании покупателя. Если большой генератор будет поврежден, его вряд ли заменят быстро, для этого потребуются месяцы.

К счастью, Федеральное управление электроэнергетики в 2008 году наконец-то потребовало от энергетических компаний принять некоторые меры кибербезопасности и предупредило, что в случае несоблюдения этого требования с компаний будет взыскиваться по миллиону долларов в день, но ни одна еще не была оштрафована. Им дали отсрочку до 2010 года. Затем комиссия обещала начать проверку. Увы, инициатива президента Обамы «Умная сеть» приведет к тому, что электросети станут еще больше зависеть от компьютерных технологий. Так же как из киберпространства можно разрушить линию электропередач, с помощью компьютера можно заставить поезд сойти с рельсов, отправить грузовые вагоны в неверном направлении, спровоцировать взрыв газопровода, поломку или отключение военных систем. Кибервоины способны дотянуться из киберпространства до многих систем, таких как электросеть или система вооружения противника, заставить их отключиться или взорваться.

Архитектура Интернета, дефекты программного обеспечения и аппаратных средств и возможность управлять жизненно важными устройствами из киберпространства — все это в совокупности делает кибервойну возможной. Но почему мы до сих пор не решили эти проблемы?

Глава 4

Брешь в обороне

М

ы уже рассмотрели ряд примеров, демонстрирующих возможности кибервойны, — в основном атаки с целью нарушения нормальной работы различных систем. Мы видели, что Соединенные Штаты, Китай, Россия и другие страны инвестируют огромные средства в кибервоенные подразделения. Мы представили, какими были бы первые минуты разрушительной полномасштабной кибератаки на США. И узнали, что такое кибертехнологии

 1 ZВ

Брешь в обороне

1 29

и как с их помощью организовать такие атаки. Но почему же никто ничего не сделал, чтобы укрепить уязвимые места? Почему мы делаем акцент на способности других атаковать нас, а не отдаем приоритет защите? Попытки выстроить кибероборону США были. Очевидно, они не увенчались успехом. В этой главе мы рассмотрим, какие меры предпринимались, чтобы защитить нашу страну от кибервойны (а также киберпреступности и кибершпионажа), и почему они потерпели полный провал. Итак, пристегните ремни. Сначала мы быстро пронесемся сквозь 20 лет попыток США сделать что-нибудь в сфере кибербезопасности. Затем поговорим о том, почему это оказалось бесполезным.

Первоначальные замыслы
Пентагона

На заре 1990-х Пентагон начал беспокоиться об уязвимости, которая появилась в результате зависимости от новых информационных систем в управлении военными действиями. В 1994 году Министерством обороны США была создана Объединенная комиссия по безопасности, которая занялась новой проблемой, вызванной распространением сетевых технологий. В заключительном отчете комиссии было сформулировано три важнейших принципа:

0 «технологии информационных систем... развиваются быстрее, чем технологии систем информационной безопасности»;

0 «безопасность информационных систем и сетей — главная задача в сфере безопасности этого десятилетия и, возможно, следующего века... при этом мы [[38]](#footnote-39)

Третья мировая война: какой она будет?

недостаточно осознаем высокие риски, с которыми сталкиваемся в этой сфере»;

1. в отчете отмечалась возросшая зависимость частного сектора от информационных систем, вследствие чего уязвимым становится не только Пентагон, но и вся страна.

Сегодня эти три момента справедливы и еще более актуальны. Пророческая статья из журнала Time(1995 год) показывает, что проблемы кибервойны и уязвимых мест в обороне нашей страны серьезно занимали Вашингтон еще 15 лет назад. Но мы продолжаем изобретать велосипед. В статье 1995 года полковник Майк Тэнксли поэтично описал, как в будущем конфликте с менее могущественной державой Соединенные Штаты заставят врага сдаться без единого выстрела. Используя хакерские приемы, которые тогда возможны были разве что в боевиках, американские воины смогут вывести из строя систему телефонной связи противника, разрушить железнодорожную систему, отдать ложные команды войскам неприятеля, захватить радио и телевидение. Согласно фантастическому сценарию Тэнксли, в результате использования этой тактики конфликт закончится, не успев начаться. В материале говорилось, что логическая бомба «будет бездействовать в системе врага до заранее определенного момента, когда она сработает и начнет уничтожать данные. Такие бомбы смогут атаковать компьютеры, которые управляют системой ПВО или центральным банком страны-противника». В статье сообщалось, что у ЦРУ есть «секретная программа, способная внедрять подрывные ловушки-микросхемы в системы вооружения, которые иностранные производители оружия будут поставлять потенциально враждебной стране (чипирование)». Источник из ЦРУ рассказал репортерам, как это делается: «Вы внедряетесь в цепочку [[39]](#footnote-40)

Брешь в обороне

поставок иностранного производителя, затем быстро переходите в режим офлайн, вставляете „жучок“, который отправляется в другую страну... Когда эта система вооружения попадает к противнику, кажется, что все работает отлично, но боеголовки не взрываются».

Статья в Time— прекрасный образец журналистики: в ней проанализированы и сложные технические вопросы, и проистекающие стратегические проблемы, которые стали очевидными для большинства чиновников из правительства лишь много лет спустя. Подзаголовок гласил: «США стремятся превратить компьютеры в завтрашнее оружие массового поражения. Но так ли неуязвим наш тыл?». Этот вопрос сегодня столь же уместен, как и тогда, и, что удивительно, ситуация мало изменилась. «Соединенные Штаты рискуют проиграть информационную гонку вооружений потому, что они так уязвимы перед подобными атаками», — заключают авторы. «В самом деле, — продолжают они, — кибермодернизация, на которую так уповают военные в ущерб традиционным вооружениям, может расколоть американскую оборону». Итак, к середине 1990-х журналисты видели, что Пентагон и разведывательные службы приветствуют возможность создания кибероружия, но не понимают, что это палка о двух концах, один из которых может быть направлен против нас самих.

Шагом марш... в бопото

Тимоти Маквей и Терри Николс в 1995 году разбудили многих. Их безжалостное нападение на детский сад в Оклахома-сити, во время которого было убиты дети и сотрудники учреждения, никого не оставило равнодушным. Билл Клинтон произнес на месте трагедии речь. Когда [[40]](#footnote-41)

Третья мировая война: какой она будет?

он вернулся в Белый дом, я встретился с ним, так же как и другие представители аппарата Белого дома. Он мыслил концептуально, это ему было свойственно. Общество менялось. Несколько человек могут обладать значительной деструктивной силой. Взрывы происходят и в США, а не только на Среднем Востоке. Что, если бомба взорвется на фондовой бирже, или в Капитолии, или в каком-нибудь здании, о важности которого мы даже не задумываемся? Мы долго становились все более развитой в технологическом плане страной, но в некоторых отношениях это делало нас слабее. В ответ на призыв генерального прокурора Жанет Рено Клинтон назначил комиссию для выявления наиболее уязвимых из важнейших сооружений страны. Такие здания бюрократы тут же окрестили критической инфраструктурой, и это название продолжает существовать и запутывать нас по сей день. Новый комитет нарекли Президентской комиссией по защите критических инфраструктур (PCCIP). Неудивительно, что многие называют ее «болотной» комиссией — по имени председателя, генерала ВВС в отставке Роберта Марша (Марши — затопляемые низменности морских побережий. — Примеч. ред.). «Болотная» комиссия была серьезным предприятием, с большой экспертной группой и профессиональным штатом. Они проводили встречи по всей стране, беседовали со специалистами из самых разных областей промышленности, университетов, правительственных организаций. То, к чему они пришли 1997 году, не оправдало наших ожиданий. Вместо того чтобы заниматься такими правоцентристами, как Маквей и Николс, или террористами «Аль-Каиды», которые атаковали в 1993 году Всемирный торговый центр, Марш стал бить тревогу по поводу Интернета. Отметив, что Интернет на тот момент был новым трендом, комиссия Марша подчеркивала, что сеть связывает важнейшие системы — железнодорожную, банков- [[41]](#footnote-42)

Брешь в обороне

скую, электроэнергетическую, производственную, но при этом совершенно ненадежна. Проникнув через Интернет, любой хакер может отключить или повредить критическую инфраструктуру. Приветствуя перспективу создания в стране наступательных подразделений, занимающихся информационной войной, Марш призывал направить существенные усилия на защиту страны. Важнейшей проблемой он назвал частный сектор, который владел большей частью критической инфраструктуры. Эти люди с осторожностью относились к государственному регулированию своей деятельности в целях обеспечения кибербезопасности. Марш и не стал это предлагать, а призвал к «партнерству государственного и частного секторов», к обмену информацией и к проведению исследований, направленных на разработку более безопасных схем.

Я был разочарован, хотя со временем осознал правоту генерала Марша. Как высокопоставленный сотрудник Белого дома, ответственный за безопасность и контртеррористическую деятельность, я надеялся, что этот отчет поможет увеличить финансирование и улучшить структуру, что было необходимо для борьбы с «Аль-Каидой» и другими. А Марш вместо этого говорил о компьютерах, что моей работы не касалось. Мой близкий друг Рэнди Бирс, впоследствии ставший специальным помощником президента по вопросам разведки, а тогда наблюдавший от Белого дома за работой комиссии Марша, заглянул в мой кабинет, плюхнулся на стул и заявил: «Ты должен заняться критической инфраструктурой. Я не могу из-за клипер-чипа». Он имел в виду план, разработанный в 1993 году АНБ, согласно которому правительство собиралось требовать с любого, кто в США использует кодирование, устанавливать чип, позволяющий АНБ по распоряжению суда проводить прослушку. Сторонники идеи неприкосновенности частной жизни, гражданских свобод и представители тех- [[42]](#footnote-43)

Третья мировая война: какой она будет?

нологических кругов объединились в горячую оппозицию. По некоторым причинам они не верили, что АНБ будет заниматься прослушиванием только при наличии ордера (и это была правда, как выяснилось во время президентства Джорджа Буша-младшего). Клипер-чип прекратил свое существование к 1996 году, но зародил глубокое недоверие между индустрией информационных технологий и американским разведывательным сообществом. Бирс, будучи человеком из разведки, полагал, что ему не удастся завоевать доверие IT-индустрии. Поэтому он преподнес мне эту идею на блюдечке с голубой каемочкой. Более того, он уже обсудил это решение с помощником президента по вопросам национальной безопасности Сэнди Бергером, который попросил меня написать директиву, которая излагала бы нашу политику по данному вопросу, и назначал меня ответственным.

Результатом стала четкая формулировка проблемы и цели, но в рамках структуры с ограничениями, которые не позволяли нам достичь ее. Проблема заключалась в том, что «в силу масштабности нашего военного потенциала будущие враги... могут постараться нанести нам урон... с помощью нетрадиционных методов — атаковать нашу инфраструктуру и информационные системы... и тем самым существенно подорвать и нашу военную мощь, и экономику». Пока все шло нормально. Цель заключалась в следующем: «Любые вмешательства или манипуляции критическими функциями должны быть краткими, легко управляемыми, географически изолированными и минимально пагубными». Прекрасно. Но как это сделать? К тому времени все ведомства в правительстве смягчили свое решение: «Главным в проблеме защиты инфраструктуры являются стимулы, которые предлагает рынок... К регуляции мы будем прибегать лишь только в случае краха рынка... и даже тогда органы будут предлагать аль-

БРЕШЬ В ОБОРОНЕ

тернативные направления регуляции». Я получил новое звание, но оно едва бы поместилось на визитке: «Координатор национальной программы по безопасности, защите инфраструктуры и контртерроризму». Неудивительно, что в СМИ стали называть меня просто «повелителем безопасности», реального названия моей должности никто не помнит. Однако из постановления становилось ясно, что координатор не имеет полномочий что-то кому-то предписывать. Члены кабинета в этом были непреклонны. Отсутствие регулирующих и директивных полномочий означало, что на существенные результаты надеяться не стоит.

Тем не менее мы намеревались сотрудничать с частным сектором и правительственными органами. Чем больше я работал над этим вопросом, тем больше увлекался. Марш не был паникером, я начал это понимать, они с его комиссией даже недооценили проблему. Наша работа над «ошибкой 2000» (опасения, что большая часть программного обеспечения не сумеет перейти с 1999-го на 2000 год, в связи с чем просто перестанет работать) значительно расширила мое понимание того, как быстро растет зависимость от компьютеризованных систем и сетей, так или иначе связанных с Интернетом. В 2000 году мне удалось выбить дополнительные 2 миллиарда долларов из федерального бюджета на разработки в области кибербезопасности, но это была лишь малая толика нужных нам средств.

К 2000 году мы разработали Национальный план по защите информационных систем, но правительство до сих пор не продемонстрировало готовности попытаться согласовать работу различных отраслей промышленности, в руках которых сосредоточена критическая инфраструктура. Чтобы подчеркнуть идеологическую корректность решения избегать регулирования, в документах я использовал фразу «воздержание от регулирования», имитируя маоистскую риторику. (Мао призывал: «Копайте глубже, [[43]](#footnote-44)

Третья мировая война: какой она будет?

запасайте больше еды, не стремитесь к гегемонии».) Никто не замечал иронии. И никто из кабинета министров не удосужился защитить собственные сети, чего требовала президентская директива. Таким образом, план оказался беззубым. Однако он дал понять промышленникам и общественности, что ставки высоки. Сопроводительное письмо Билла Клинтона не оставляло сомнений, что IT- революция изменила сущность экономики и национальной безопасности. Теперь, включая свет, звоня в службу спасения, сидя за штурвалом самолета, мы полагались на компьютерные системы управления. «Скоординированное наступление» на компьютеры любого важного сектора экономики имело бы «катастрофические последствия». И это не теоретические предположения, наоборот, «мы знаем, что угроза реальна». Противник, который полагается на «бомбы и пули», теперь может использовать «ноутбук... как оружие... способное нанести чудовищный урон».

В собственном сопроводительном письме я добавил: «Больше любых других стран Америка зависит от киберпространства». Кибератака может «разрушить электрические сети... транспортные системы... финансовые институты. Мы знаем, что другие правительства развивают такие возможности». Как и мы, но я вам этого не говорил.

Шесть смешных имен

На протяжении первых лет моей работы над вопросами кибербезопасности произошло семь крупных происшествий, которые убедили меня в серьезности данной проблемы. Во-первых, в 1997 году, когда мы совместно с АНБ проверяли систему кибербезопасности Пентагона в рамках учений приемлемый получатель (EligibleReceiver), наша команда за два дня проникла в секретную сеть командова- [[44]](#footnote-45)

Брешь в обороне

ния и была готова отдавать ложные приказы. Я поспешил свернуть учения. Помощник министра обороны был шокирован уязвимостью Пентагона и приказал всем подразделениям приобрети и установить системы обнаружения несанкционированного вмешательства. Вскоре выяснилось, что каждый день совершались тысячи попыток проникнуть в сети Министерства обороны. И это только выявленные случаи. В 1998 году, во время кризиса в Ираке, кто-то взломал несекретные компьютеры Министерства обороны. В ФБР атаку назвали «Восход солнца» (многим тогда пришлось проснуться). После нескольких дней паники выяснилось, что нападали не иракцы, а израильтяне. Точнее, один подросток из Израиля и два из Калифорнии. Они и показали, как плохо защищена сеть военной логистики.

В 1999 году ВВС заметили что-то странное в работе своей компьютерной сети. Они обратились в ФБР, те позвонили в АНБ. Выяснилось, что из исследовательских файлов авиабазы было похищено огромное количество данных. Гигантские объемы информации извлекались из компьютеров Министерства обороны и баз данных национальных ядерных лабораторий Министерства энергетики. Этот случай в ФБР получил название «Лунный лабиринт», и он тоже оказался показательным. Никто не мог разобраться в происходившем, ясно было только, что данные пересылались через множество стран, прежде чем попасть куда-то. Два особенно тревожных аспекта заключались в том, что специалисты по компьютерной безопасности не смогли воспрепятствовать похищению данных, даже когда узнали о проблеме, и никто не мог с уверенностью сказать, откуда действовали хакеры (хотя позднее некоторые публично возложили ответственность за атаку на русских). Каждый раз, когда устанавливалась новая защита, ее взламывали. Затем в один день атака прекратилась. Или, скорее всего, они стали действовать так, что мы этого уже не могли видеть. [[45]](#footnote-46)

ТрЕТЬЯмировая война: какой она будет?

В начале 2000 года, когда мы все еще сияли от счастья, что удалось избежать «ошибки 2000», ряд новых интернет- магазинов (AOL, Yahoo, Amazon, E-Trade) подверглись мощной DDoS-атаке (для большинства людей этот термин был тогда в новинку). Это был первый «большой взрыв», который затронул множество компаний и едва не разорил их. Мотивы понять было сложно. Никто не выдвигал никаких требований, не делал политических заявлений. Казалось, кто-то проверял идею тайного захвата множества компьютеров и использования их для атаки. (Этим кем-то, как позднее выяснилось, оказался помощник официанта из Монреаля). Я отнесся к этой DDoS-атаке как к возможности заставить правительство напомнить частному сектору о необходимости серьезно относиться к кибератакам. Президент Клинтон согласился принять руководителей компаний, пострадавших от атаки, а также директоров инфраструктурных предприятий и IT-компаний. Это была первая встреча президента в Белом доме с руководителями частных компаний по проблеме кибератак. И по сей день последняя. Впрочем, разговор оказался весьма откровенным, он открыл глаза многим и привел к тому, что все согласились с необходимостью серьезнее работать над проблемой.

В 2001 году новая администрация Буша прочувствовала эту проблему на собственной шкуре, когда «червь» CodeRedзаразил более 300 тысяч компьютеров за несколько часов, а затем превратил их в зомби, запрограммированных на проведение DDoS-атаки на веб-сайт Белого дома. Мне удалось рассредоточить сайт Белого дома на 20 тысячах серверах с помощью компании Akamai, благодаря чему мы избежали тяжких последствий (а также убедили нескольких поставщиков интернет-услуг отвести атакующий трафик). Вылечить зараженные компьютеры оказалось сложнее. Многие компании и индивидуальные поль-

1 зв

Брешь в обороне

зователи не стремились удалять «червя», несмотря на то что он заражал другие компьютеры. Да и мы не имели возможности заблокировать этим машинам доступ в сеть, хотя они и регулярно рассылали вредоносное ПО. В дни, последовавшие за террористической атакой 29 сентября, быстро распространился еще более серьезный «червь» — NIMDA (Adminнаоборот). Он был нацелен на компьютеры самой защищенной сферы — финансовой. Несмотря на изощренную защиту, многие банки и компании с Уоллстрит были выкинуты в офлайн.

КИБЕРБЕЗОПАСНОСТЬ И БУШ

Потребовались некоторые усилия, чтобы убедить администрацию Буша в том, что кибербезопасность является важной проблемой, но к лету 2001 года руководство Белого дома согласилось выделить отдельный отдел для координации ее решения (административный указ 13 231). Руководил этим отделом я, в должности специального советника президента по кибербезопасности, с осени 2001 года по начало 2003-го. Многие в Белом доме (советник по науке, советник по экономике, директор по бюджету) старались ограничить полномочия нового отдела.

Моя команда, ничуть этим не обеспокоенная, взяла общенациональный план Клинтона и доработала его на основе данных, полученных от 12 учрежденных нами промышленных групп и граждан из десяти муниципалитетов страны (которые, к счастью, вели себя куда цивилизованнее, чем те, кто в 2009 году собирался в муниципалитете для обсуждения вопросов здравоохранения). В результате появилась Национальная стратегия по безопасности киберпространства, которую Буш подписал в февра-

Третья мировая война: какой она будет?

ле 2003 года. По существу разницы в подходах Клинтона и Буша почти не было, за исключением того, что администрация республиканцев не только продолжила воздерживаться от регулирования, но и питала нескрываемое отвращение к идее введения любых новых регулятивных норм со стороны федерального правительства. Буш долгое время оставлял вакантные места в нескольких регулятивных комиссиях, а позже назначал уполномоченных, которые не стремились укрепить существовавший порядок регулирования.

То, как Буш понимал проблему кибербезопасности и интересовался ею на заре своего президентства, лучше всего характеризует вопрос, который он задал мне в 2002 году. Я зашел в Овальный кабинет с известиями об обнаружении распространявшегося дефекта в программном обеспечении, который мог позволить хакерам сделать все что угодно, если только мы не убедим большинство крупных сетей и корпораций устранить его. Единственной реакцией Буша стал следующий вопрос: «А что думает Джон?» Джон был директором крупной информационнотехнологической компании и главным спонсором избирательной комиссии Буша. После формирования Министерства национальной безопасности я решил, что появлась прекрасная возможность собрать многие разрозненные организации для работы над проблемой и объединить их в один центр. Некоторые отделы по кибербезопасности из Министерства торговли, ФБР и Министерства обороны были переведены в Министерство национальной безопасности. Но целое оказалось значительно меньше частей, поскольку многие из лучших представителей объединенных кабинетов предпочли воспользоваться случаем и уйти из правительства. Когда я вышел из администрации Буша вскоре после того, как они начали иракскую войну, Белый дом не стал искать мне замену на посту специального советника. Министерство национальной безопасности ока- [[46]](#footnote-47)

Брешь в обороне

залось самым недееспособным подразделением правительства. Несколько очень хороших людей пытались заставить его заработать, но все они разочаровались и ушли. В СМИ начали говорить о «киберцаре на неделю». Внимание представителей частного сектора к проблеме, которого мы так долго добивались, ослабло.

Четыре года спустя Буш принял решение — гораздо быстрее, чем убеждали меня его подчиненные. Это была секретная акция, которую президент должен был одобрить лично. Составитель президентского графика выделил час на совещание по принятию решения, а оно заняло пять минут. Не было ни одной секретной акции, которая бы не понравилась Бушу. Потом оставшиеся пятьдесят пять минут встречи директор национальной разведки произносил вступительное слово. Все нужные люди — старшие члены кабинета, отвечавшие за безопасность страны, — были на месте. Макконел предложил обсудить угрозу финансовому сектору и всей американской экономике. Получив возможность высказаться, он рассказал о кибервойне и о том, как мы перед ней уязвимы. Особенно уязвим был финансовый сектор, который не смог бы восстановиться после потери данных вследствие атаки, которая нанесла бы невообразимый урон экономике. Потрясенный Буш повернулся к министру финансов Хэнку Паулсону, который согласился с такой оценкой. На этом моменте Буш, сидевший за большим столом в Овальном кабинете, едва ли не взлетел. Он быстро переместился во главу стола и заговорил, яростно жестикулируя: «Информационные технологии всегда считались нашим преимуществом, а не слабостью. Я хочу, чтобы так было всегда. Я хочу план, быстро, очень быстро». Результатом стала CNCI(Всесторонняя национальная программа кибербезопасности) и постановление № 54, посвященное вопросам национальной безопасности. Ни один из этих документов не был опубликован, но в каждом из них предлагался достаточно приемлемый

Третья мировая война: какой она будет?

12-этапный план. Однако основное внимание уделялось защите правительственных сетей. Как ни странно, план не был направлен на решение проблемы, с которой началось обсуждение в Овальном кабинете, — проблемы преодоления уязвимости в кибервойне финансового сектора.

Тем не менее Буш потребовал выделить 50 миллиардов долларов на ближайшие пять лет для разработки всесторонней национальной программы кибербезопасности, которая в итоге не стала ни всесторонней, ни национальной. Эта программа, по словам одного хорошо осведомленного человека, — попытка «остановить кровотечение» из систем Министерства обороны и разведывательного сообщества, которая лишь косвенно затрагивает все остальное. Как бы ее ни превозносили, она не направлена на преодоление уязвимостей частного сектора и наших важнейших инфраструктур. Эта более сложная проблема досталась по наследству следующей администрации.

Предполагалось, что в рамках инициативы будет разработана «стратегия удержания от информационной войны и декларативная доктрина». Реализация этой части плана была почти полностью заморожена. В мае 2008 года комитет по делам вооруженных сил сената раскритиковал секретность этой программы в публичном докладе, отметив, что «сложно представить, как Соединенные Штаты смогут провозгласить убедительную доктрину сдерживания, если каждый аспект наших возможностей и оперативных принципов засекречен». Читая это, я не мог не вспомнить доктора Стрейнджлава, который в фильме Стэнли Кубрика ругал советского посла за то, что Москва хранит в секрете существование мощного средства сдерживания — ядерной „машины судного дня“: «Конечно же, весь смысл «машины судного дня» пропадает, если вы держите ее в секрете! Почему вы не рассказали о ней всему миру?» Вероятно, мы храним в тайне свою стратегию киберсдерживания потому, что она не слишком удачна. [[47]](#footnote-48)

Брешь в обороне

Переполненная чаша Обамы

Еще одно уязвимое место финансового сектора возникло вследствие того, что крупнейшие финансисты успешно лоббировали отказ от правительственного регулирования. На нем и пришлось сконцентрироваться Бараку Обаме, когда он стал президентом. Провал субстандартного ипотечного кредитования и сложная ситуация на рынке ценных бумаг спровоцировали жесточайший финансовый кризис со времен 1929 года. Вследствие этого, а также войны в Ираке и Афганистане, угрозы пандемии гриппа, реформы здравоохранения, глобального потепления, которые требовали его внимания, Обама проигнорировал проблему кибербезопасности. Однако он затрагивал эту же тему во время предвыборной кампании 2008 года. Хоть я и согласился принять участие в кампании в качестве эксперта по проблеме терроризма, но использовал эту возможность, чтобы проработать кандидата и его советников на тему кибервойны. Я не удивился, что Обама уловил суть проблемы, поскольку он проводил самую технологически продвинутую, киберзависимую президентскую кампанию в истории. Еще будучи сенатором, Обама летом 2008 года выступил с речью перед экспертами в области кибербезопасности в Университете Пердью. В речи, посвященной проблемам национальной безопасности, он сделал смелое завление, объявив американскую киберинфраструктуру «стратегическими активами», — такая важная фраза в переводе с языка правительства означает — это стоит защищать. Он пообещал назначить в Белом доме старшего советника, который будет отчитываться непосредственно перед ним, и пообещал, что кибербезопасность станет «главным государственным приоритетом». В брошюре, которую мой соавтор Роб Нейк составил вместе с Джоном Мэллери и Роджером Хурвитцем — специалистами по вычислительной технике из Массачусетского технологи- [[48]](#footnote-49)

Третья мировая война: какой она будет?

ческого института, он пошел еще дальше, раскритиковав администрацию Буша за медлительность перед лицом рисков, связанных с киберпространством, и дал обещание «способствовать разработке безопасных компьютеров и сетей следующего поколения для обеспечения национальной безопасности», больше инвестировать в науку и математическое образование и создать план устранения уязвимых мест, предотвращения хищения информации и корпоративного шпионажа.

Несколько недель спустя Обама столкнулся с очень серьезной киберугрозой. ФБР, не привлекая общего внимания, проинформировало, что есть основания считать, будто китайские хакеры проникли в компьютерные системы участников кампании. Я попросил одного из моих деловых партнеров, Пола Куртца (занимавшегося в Белом доме вопросами кибербезопасности и при Буше, и при Клинтоне), привлечь команду экспертов по кибербезопасности из штаб-квартиры в Чикаго, чтобы оценить масштаб урона и посмотреть, что можно сделать, чтобы обезопасить системы. Китайских хакеров интересовали черновики программных документов. Они использовали достаточно сложные методы под прикрытием благовидной деятельности. Когда к кампании неофициально присоединились специалисты из Чикаго, я попросил всех, кто работает над вопросами национальной безопасности, не использовать домашние компьютеры для этой цели. Несмотря на то что их переписка была несекретной, ею очень интересовался Китай и другие (включая, предположительно, Джона Маккейна, хотя я бы не сказал, что его кампания отличалась глубоким пониманием кибертехнологий). С согласия участников кампании мы раздали всем «чистые» ноутбуки Appleи заблокировали их так, чтобы они могли работать только в пределах виртуальной частной сети, созданной с использованием сервера с совершенно безобидным

 1 44

Брешь в обороне

именем. Я знал, что затруднения возникнут. Вскоре мне стали звонить с жалобами на ограничения: «Дик, я в кафе, и этот чертов компьютер не дает мне подключиться к wifi», «Дик, мне нужно отправить кое-какие файлы из своего ящика, но я не могу выйти в Интернет». Я пытался объяснить, что нам, наверное, не стоит планировать захват Белого дома из кафе, но никого это особенно не убеждало.

Незадолго до инаугурации мы с Полом Куртцем представили новой команде Белого дома проект решения, в котором были сформулированы предложения, озвученные Обамой в речи в Университете Пердью. Мы утверждали, что если Обама будет медлить, кто-нибудь обязательно попытается его остановить. Несмотря на то что многие из аппарата Белого дома понимали проблему и хотели быстрого решения, никто, разумеется, не считал ее первостепенной. Вместо этого администрация Обамы приказала подготовить за 60 дней обзор состояния систем 1Т-безопасности и попросила одного из составителей бушевской CNCI(Всесторонней национальной программы кибербезопасности) возглавить этот проект. И это несмотря на то, что комиссия по кибербезопасности 44-го президента во главе с Джимом Льюисом уже год пыталась прийти к консенсусу по вопросу, что должен делать следующий президент, и уже опубликовала отчет в декабре 2008 года. Когда 110 дней спустя президент объявил результаты, догадайтесь, что произошло? Вернули CNCI. Военное Киберкомандование осталось, но не было ни стратегии кибервойны, ни плана или программы действий по защите частного сектора, ничего того, что могло инициировать международный диалог по этим проблемам. И — опять дежавю — новый президент от демократов отказался от попыток регулирования: «Позвольте мне сказать с предельной ясностью: моя администрация не будет диктовать стандарты безопасности частным компаниям».[[49]](#footnote-50)

Третья мировая война: какой она будет?

Но кое о чем в своих высказываниях Обама не упомянул, а именно: кто будет новым главой отдела кибербезопасности в Белом доме. Мало кто из компетентных людей хотел получить эту должность, в основном потому, что она не давала реальных полномочий и подразумевала подчинение и советнику по экономике, и помощнику президента по вопросам национальной безопасности. Советником по экономике тогда был Лари Саммерс — отправленный в отставку президент Гарварда, который ясно дал понять: он считает, что частный сектор и рыночные силы и сами смогут справиться с угрозой кибервойны, без какого бы то ни было регулирования со стороны государства и любого его вмешательства. Проходили месяцы, но отдел кадров Белого дома не мог убедить ни одного кандидата, что эта работа стоит того, чтобы на нее согласиться. Таким образом, в первый год президентства Обамы в Белом доме никто не пытался управлять кибербезопасностью правительства или программой кибервоенного развития. Двумя главными ведомствами, которые защищали Америку от кибервойны, были Киберкомандование США (для защиты вооруженных сил) и Министерство национальной безопасности (для защиты всего остального). Глава Киберкомандования на протяжении 2009 года занимал сдержанную позицию, поскольку сенат никак не соглашался дать ему четвертую звезду. Чтобы получить повышение, генерал Кейт Александер должен был ответить на вопросы перед комитетом сената, но этот комитет не слишком понимал, чем на самом деле должно заниматься Киберкомандование.

Сенатор от Мичигана Карл Левин, прежде чем назначить слушания, попросил Пентагон сообщить, в чем заключается миссия и стратегия Киберкомандования. Пока сенатор Левин пытался выяснить, что должно защищать Киберкомандование, а генерал Александер занимал сдержанную позицию, я терялся в догадках, что же [[50]](#footnote-51)

Брешь в обороне

обязано защищать Министерство национальной безопасности. Поэтому и обратился к первоисточнику и спросил об этом непосредственно Джанет Наполитано. Она любезно согласилась встретиться со мной в штаб-квартире ее министерства. В отличие от других министерств, штаб- квартиры которых находятся в монументальных зданиях или современных офисных центрах близ NationalMall,это ведомство располагается в обнесенном колючей проволокой лагере на северо-западе Вашингтона. За ограждением находятся несколько невысоких зданий из красного кирпича, которые, если смотреть с улицы, напоминают казармы. Неудивительно, что чиновники, вынужденные перебраться сюда, прозвали это место «Сталаг-13» — в честь вымышленного тюремного лагеря из телевизионного комедийного шоу Hogan’sHeroes.

Изначально здесь находился штаб криптографической службы ВМФ США, предшественницы нынешнего 10-го флота. Как и на всех остальных базах американского флота, здесь можно увидеть небольшую белую церковь и аккуратные вывески с названиями улиц. Одна называется Путь разведчика. Чтобы попасть в кабинет министра, мы прошли вдоль бесконечного ряда серых будок. Личный офис Наполитано выглядел не намного лучше. Для бывшего губернатора Аризоны это мрачное помещение три на четыре метра было серьезным понижением. Тем не менее в один угол она умудрилась втиснуть седло, какие используются в родео для езды на диких лошадях. Помещение выглядело как временное пристанище, даже спустя шесть лет после образования министерства. «Мы собираемся переезжать в новую, большую, штаб-квартиру», — объяснила министр, стараясь сделать акцент на позитивном. Новая штаб-квартира расположена на месте закрытой больницы для душевнобольных в Вашингтоне и будет готова на десятый год существования министерства. Возможно. [[51]](#footnote-52)

Третья мировая война: какой она будет?

* Несмотря на то что вчера был выходной, я провела встречу с руководителями финансового сектора и обсудила проблему кибербезопасности, — начала Наполитано.

В министерстве шел месяц кибербезопасности, и она запланировала ряд событий. Я спросил ее, в чем важнейшая угроза.

* Опытный хакер-одиночка, киберпреступный картель... — ответила она.
* Хорошо, а если бы началась кибервойна? — продолжил я.
* Пентагон играл бы главную роль, но мы бы смогли справиться с последствиями любых повреждений, нанесенных Соединенным Штатам.
* А может, лучше предотвратить повреждения, чтобы справляться пришлось с меньшими последствиями?
* Мы наращиваем возможности, чтобы защитить домен .gov.
* Отлично. Если Киберкомандование США защищает .milи вы однажды сумеете защитить .gov, кто защитит все остальное — важнейшую инфраструктуру, которая принадлежит частному сектору?
* Мы работаем с представителями частного сектора, центрами совместного использования и анализа информации в 18 важнейших отраслях промышленности.
* Но это не означает, что американское правительство защищает критическую инфраструктуру от кибератак, не так ли?
* Нет, не так. Это не входит в задачи Министерства национальной безопасности.

Министерство национальной безопасности разрабатывает систему сканирования кибертрафика, проходящего через федеральные ведомства, на предмет обнаружения вредоносного ПО (вирусов, «червей» и т. д.). Эта система с несколько претенциозным названием «Эйнштейн» выросла из простой программы контроля потоков трафика [[52]](#footnote-53)

Брешь в обороне

(«Эйнштейн-1») в систему обнаружения вторжений и вредоносного ПО («Эйнштейн-2») и скоро научится блокировать интернет-пакеты, кажущиеся вредоносными («Эйнштейн-3»). В рамках попыток защитить правительственные сайты Министерство национальной безопасности и администрация общих служб стараются снизать количество интернет-порталов на домене .gov. Позднее Министерство национальной безопасности установит «Эйн- штейн-3» на каждый из этих порталов, чтобы выявлять вредоносные программы. Управлять сетью «Эйнштейн-3» будет недавно организованное отделение — Национальный интеграционный центр кибербезопасности и коммуникаций в Болстоне (штат Вирджиния).

* Если Министерство национальной безопасности сумеет ее запустить, — спросил я, — то зачем ограничиваться защитой только федерального правительства?
* Возможно, в будущем мы рассмотрим возможность более широкого ее применения.

Наполитано, юрист и бывший федеральный обвинитель, добавила, что если правительство вознамерится сканировать публичный Интернет с целью защиты от кибератак, возникнут препятствия юридического и частного характера. Разве она не может привлечь распорядительный орган, чтобы заставить предприятия критической инфраструктуры усовершенствовать свои возможности защиты от кибератак и регламентировать деятельность интернет-провайдеров или электроэнергетических компаний? К ее чести, она не исключает этих и других возможностей, даже несмотря на то что сам президент Обама отказался от них в своей речи по кибербезопасности в мае 2009 года. Но регулирование, заметила она, может начаться только после совместного использования информации и добровольных мер, которые явно провалились, хотя в первый год президентства Обамы было слишком рано выносить такое суждение. Подход, основанный на [[53]](#footnote-54)

Третья мировая война: какой она будет?

совместном использовании информации и добровольных мерах, пытались использовать уже более десяти лет.

В сфере ее ответственности находится безопасность домена .gov, и Наполитано с гордостью сообщила, что в МНБ открыта тысяча вакансий для людей с опытом работы в кибербезопасности. Но с какой стати квалифицированные кибергики захотят работать на Министерство национальной безопасности, если их зовут куда угодно, начиная от Киберкомандования и заканчивая компаниями Lockheedи BankofAmerica.Наполитано ответила, что она прорабатывает кадровые вопросы, так что министерство сможет платить жалованье, сопоставимое с зарплатами в частном секторе, а еще планирует организовать дополнительные офисы вне Вашингтона — в Калифорнии и других местах, где, вероятно, предпочтут жить гики. Я подумал, что в ее голосе слышится тоска по дому, которую нередко тайно испытывают вашингтонские чиновники. Когда мы покинули кабинет министра, глава береговой охраны США адмирал Тад Ален встретил нас снаружи.

* Рад, что вы пережили разговор с Диком, — пошутил адмирал.
* Пережила, — ответила министр, — но теперь переживаю по поводу кибервойны.

Почему Клинтон, Буш и Обама так и не смогли справиться с проблемой уязвимости американского частного сектора перед кибервойной? Люди, работавшие над этим вопросом годами, имеют на сей счет разные мнения и расставляют разные акценты. Давайте рассмотрим шесть самых популярных объяснений.

1. . Самый бопьшой обман

Первое самое популярное объяснение заключается в том, что после кибератак обычно не остается ни следов, ни зи- [[54]](#footnote-55)

Брешь в obopcihe

яющих кратеров, как после взрыва на Манхэттене 11 сентября. Когда крадут интеллектуальную собственность компании, ее руководство и сотрудники, как правило, об этом даже не подозревают. Представьте, что вы работаете в музее, где хранятся ценные экспонаты, скажем, скульптуры и картины. Когда вы уходите из музея в конце рабочего дня, вы включаете систему сигнализации и убеждаетесь, что все камеры работают и ведется видеозапись. Утром вы возвращаетесь. Сигнализация не сработала, но чтобы знать, что все в порядке, вы просматриваете видео за последние 12 часов и убеждаетесь, что никто не вошел и не вышел из музея за время вашего отсутствия. И, наконец, вы проверяете скульптуры и картины, чтобы удостовериться, что все они на месте. Все хорошо. Так зачем же дальше думать о проблеме безопасности?

По существу, такая же ситуация наблюдается и в Пентагоне с конца 1990-х и по сей день. Возможно, какие-то люди пытаются проникнуть в правительственные сети, но ведь программные средства защиты данных (брандмауэры, системы обнаружения и предотвращения несанкционированного вмешательства) эффективно стравляются с большей частью этих угроз? Зачем начальству думать, что их интеллектуальная собственность, их драгоценности — военные планы, технические чертежи или программы — теперь хранятся не только в их компьютерах, но и на жестких дисках в Китае, России и других странах?

Разница между похитителями произведений искусств и хакерами мирового класса заключается в том, что, когда работают настоящие киберграбители, вы и не догадываетесь, что стали жертвой. «Американское правительство каждый месяц совершает энное количество [точное число не называется] проникновений в иностранные сети», — сказал мне один офицер разведки. «Нас ни разу не засекли. Если нас не засекают, чего же тогда не замечаем мы, защищая собственные сети?» Как убедить кого-либо в на- [[55]](#footnote-56)

Третья мировая война: какой она будет?

линии проблемы, если вы не в состоянии предоставить доказательства ее существования? Данные не исчезают, как картина Вермеера, украденная из Музея Изабеллы Стюарт Гарднер в Бостоне в 1990 году. Очевидно, это новая, уникальная проблема, свойственная именно киберпространству. Историкам военной разведки, однако же, о подобном уже известно. Во времена холодной войны в ВМФ Соединенных Штатов были уверены, что смогут одержать победу над советским флотом, если он когда-либо перейдет к активным военным действиям, до тех пор, пока не узнали, что одна американская семья обеспечила Советам уникальное преимущество. Семья Уолкеров — сотрудник Агентства национальной безопасности и его сын, служивший в американском флоте, — предоставила СССР секретные коды и систему шифров для передачи сообщений между кораблями. С тех пор советский флот знал, где находились наши корабли, куда они направлялись, что им приказано делать, какое вооружение и другие системы на борту не работали. Мы такого и предположить не могли, потому что были уверены, что даже если они перехватывают радиосигналы с нашими сообщениями, расшифровать код им не удастся. Наверное, они и не могли, пока не купили ключ к дешифрованию у американцев. Это не единственный пример столь самонадеянной уверенности: во время Второй мировой войны японцы тоже думали, что никто не сумеет прочитать их шифровки, но Соединенные Штаты и Великобритания справились с этой задачей. Некоторые историки считают, что ВМФ США одержал победу над Императорским флотом Японии именно благодаря возможности дешифровать сообщения. Несомненно, решающая победа США в битве при Мидуэе состоялась именно потому, что американцы знали планы японцев. Разумно предположить, что на протяжении десятилетий коды многих стран, которые, как считалось, расшифро- [[56]](#footnote-57)

Брешь в обороне

вать невозможно, на самом деле раскрывались (и раскрываются). Несмотря на то что историки и сотрудники госбезопасности знают о многочисленных прецедентах, они упорно не желают верить в то, что такое может происходить сейчас и с нами. Американское военное руководство не может представить себе, что их секретная (SIPRNET) и сверхсекретная (JWICS) внутренние сети подвергаются опасности, но несколько экспертов, с которыми я беседовал, в этом уверены. Многие руководители компаний также верят в то, что миллионы долларов, потраченные на системы компьютерной безопасности, означают, что их коммерческие тайны надежно защищены. В конце концов, если кто-нибудь проникал в их секретные файлы, системы обнаружения несанкционированного вмешательства обязательно бы просигнализировали об этом. Правильно?

Нет, не обязательно. Даже если сигнализация включится, не факт, что кто-нибудь сумеет на это среагировать. Всегда есть способы проникнуть в сеть под видом системного администратора или другого полномочного пользователя, и тогда никакой аварийный сигнал вообще не сработает. Более того, если даже он срабатывает, в крупных сетях зачастую на него вообще не обращают внимания. Возможно, на следующий день кто-нибудь проверит журнал регистрации и заметит, что из сети была скачана пара терабайтов информации на некий сервер, который станет первой ступенью долгого пути до пункта назначения. А возможно, никто и не заметит случившегося. Бесценное произведение искусства по-прежнему в музее. А раз так, зачем правительству и заинтересованным только в прибылях руководителям что-то делать?

Во второй главе я упоминал о многодневном происшествии 2003 года под кодовым названием «Титановый дождь». Алан Раллер, мой друг и руководитель общественной организации SANSInstitute,занимающейся образова- [[57]](#footnote-58)

Третья мировая война: какой она будет?

нием в сфере кибербезопасности, описывает, что произошло в один из дней «Титанового дождя», 1 ноября 2003 года.

В 10:23 хакеры воспользовались уязвимым местом в сети командования информационных систем сухопутных войск на базе Форт-Хуачука (штат Аризона).

В 13:19 через тот же «черный ход» они проникли в компьютеры управления информационного обеспечения в Арлингтоне (штат Вирджиния).

В 15:25 они взломали сеть Центра исследования морских и океанских систем Министерства обороны США в Сан-Диего (штат Калифорния).

В 16:46 они ударили по оборонительной установке армейского ракетно-космического центра в Хантсвилле (штат Алабама).

Подобных дней было еще много. Помимо взлома сетей Министерства обороны были украдены терабайты секретной информации из лабораторий НАСА, а также из компьютеров таких корпораций, как LockheedMartinи NorthropGrumman,которые платят миллиарды долларов за безопасность своих сетей. Специалисты по кибербезопасности пытались выяснить, какие методы использовались для проникновения в их сети. Один из них сказал: «Все были слишком самодовольны». Покачал головой, состроил рожу и мягко добавил: «...до тех пор, пока не осознали, что противник только что совершенно незаметно ушел, а возможно, и продолжает нас грабить. Но мы его больше не видим». «Лунный лабиринт» и «Титановый дождь» лучше всего считать краткими эпизодами огромной кампании, большая часть которой осталась незамеченной. Трудно представить, что можно практически беспрепятственно украсть из сети компании терабайты информации. В тех случаях, о которых нам известно, компании и правительственные организации долгое время даже не подозревали о краже данных. У всех пострадав- [[58]](#footnote-59)

Брешь в обороне

ших организаций имелись системы обнаружения несанкционированного вмешательства, которые должны поднимать тревогу в случае, если неавторизированный пользователь пытается проникнуть в сеть. Кое-где были установлены более совершенные системы предотвращения несанкционированного вмешательства, которые не только предупреждают, но и автоматически блокируют хакера. Но сигналы тревоги молчали. Если вы подумали, что по компьютерам лабораторий, компаний, исследовательских центров систематически, словно пылесосом, проходятся некие зарубежные организации, вы правы. Именно так и происходит. Львиная доля нашей интеллектуальной собственности копируется и перемещается за океан. Нам остается лишь надеяться на то, что кто бы этим ни занимался, у них не хватит аналитиков исследовать всё и найти все драгоценности, хотя это и слабая надежда, особенно если в стране, которая организует хакерские атаки, проживает миллиард человек.

Во всей этой мрачной картине есть одно светлое пятно, и связано оно с APL, физической лабораторией Университета Джонса Хопкинса под Балтимором. Лаборатория зарабатывает сотни миллионов долларов в год, проводя для американского правительства исследования в самых разных областях, начиная от космических технологий и заканчивая биомедициной и секретными проектами по национальной безопасности. Лаборатория APLобнаружила, что из ее сети в 2009 году выкрали огромные массивы данных, и сумела остановить этот процесс. APL— одно из тех мест, где работают настоящие эксперты по кибербезопасности, у них заключены контракты с АНБ. Поэтому логично предположить, что их системы предотвращения вторжений сумели заблокировать кражу данных. Однако эти эксперты нашли единственный способ остановить утечку — отключиться от Интернета. APLполностью

Третья мировая война: какой она будет?

перекрыла связь и изолировала целую сеть, сделав ее автономным островом в киберпространстве. На протяжении недель специалисты APLисследовали компьютер за компьютером, чтобы найти «черные ходы» и вредоносные программы. Чтобы убедиться в том, что важные данные никто не копирует прямо из вашей сети, вам нужно знать наверняка, что вы не связаны с кем бы то ни было вне вашей внутренней сети. Но это сложнее, чем может показаться. В больших организациях сотрудники устанавливают соединения со своими домашними компьютерами, ноутбуками с wi-fi, устройствами вроде копировального аппарата, который имеет выход в Интернет. Если вы хоть как соединены с Интернетом, считайте, что утечка уже произошла.

Действительно, хакерам, в том числе лучшим, которые работают на правительства Соединенных Штатов и России, редко не удается проникнуть в сеть, даже если ее операторы считают, что она не связана с Интернетом. Более того, хакеры работают так, что всех, кто бьет тревогу по поводу защиты сетей, окружающие считают параноиками. Они не оставляют следов, за исключением тех случаев, когда сами в этом заинтересованы. Вспомните слова героя Кевина Спейси из фильма «Подозрительные лица» (TheUsualSuspects): «Величайший трюк дьявола состоял в том, чтобы убедить мир, будто он не существует».

1. Это Вегас, детка

Другой ответ на вопрос, почему в Америке до сих пор не поддерживают идею защиты уязвимых мест перед угрозой кибервойны, заключается в том, что «идейные лидеры» этой сферы до сих пор не договорились, что делать. Чтобы проверить данную гипотезу, я отправился на по- [[59]](#footnote-60)

Брешь в обороне

иски таких «идейных лидеров» и нашел их... где бы вы думали? В самом неожиданном месте: в казино CaesarsPalaceв Лас-Вегасе, в августе 2009 года, в сорокаградусную жару.

CaesarsPalace— место, совершенно неподходящее для подобных сборищ. Здесь, среди мерцающих игровых автоматов и столов для блэкджека, красуются статуи и символы империи, погибшей пятнадцать столетий назад. Конференц-залы носят гордые названия «Колизей» или «Палатинский холм», и это не развалины и руины, а самые современные помещения для встреч и презентаций с плоскими экранами и мигающими пультами управления. Каждое лето на протяжении последних 12 лет, когда заканчивается сезон конференций и цены на аренду помещений падают, сюда съезжается иная публика. В большинстве своем это мужчины в шортах и футболках, с рюкзаками за спиной и «маками» и BlackBerryв руках. Лишь немногие из них забегают в ультрамодные магазины — HugoBoss, Zegnaили Hermes,но почти все они были на премьере «Звездного пути». Эта публика —\* хакеры, и в 2009 году здесь, на конференции BlackHat(«Черная шляпа»), их собралось более четырех тысяч — вполне достаточно, чтобы развязать кибервойну глобального масштаба. Вопреки названию на конференцию приехали не злодеи из кинофильмов, а вполне добрые, «этичные» хакеры, которым полагалось бы носить белые шляпы, — директора по информационным технологиям, старшие специалисты по информационной безопасности различных банков, фармацевтических компаний, университетов, правительственных организаций, словом, любых крупных (а также средних) компаний. Название BlackHatпошло с тех времен, когда кульминацией этих ежегодных собраний были сообщения хакеров о том, какие новые способы заставить популярные программные приложения делать [[60]](#footnote-61)

Третья мировая война: какой она будет?

то, для чего они не предназначены, появились. Компании по производству программного обеспечения привыкли думать, что на таких конференциях встречаются плохие парни. Выступления, как правило, демонстрируют, что разработчики программных продуктов недостаточно заботились о безопасности, в результате чего практически всегда можно найти способы проникнуть в компьютерную сеть без авторизации и даже взять всю сеть под контроль. Microsoftбыла главной мишенью хакеров на протяжении многих лет, и руководители из Редмонда каждый год ждали BlackHatс таким же нетерпением, с каким многие из нас ожидают налоговой проверки. В 2009 году участники конференции переключились на компанию Appleв силу растущей популярности ее продукции. Самым обсуждаемым выступлением стало сообщение о том, как взломать iPhoneс помощью простого текстового сообщения SMS. Хоть Биллу Гейтсу и Стиву Джобсу не нравится, когда люди находят и разглашают дефекты в их продуктах, это не преступление. Преступление начинается тогда, когда хакер использует метод, им разработанный (средство атаки), чтобы использовать дефект, который он обнаружил в программе (уязвимость) и проникнуть в корпоративную или правительственную сеть (мишень), в которой он не авторизован. Конечно, когда об уязвимости объявляется на конференции или, что еще хуже, средство атаки получает огласку, любой может взломать какую угодно сеть, работающую на дефектной программе.

Я таки дождался неприятностей в 2002 году, когда в программной речи на конференции сказал: «Как здорово, что хакеры находят дефекты в программах!» Тогда я был специальным советником по кибербезопасности президента Буша. Кто-то, предположительно из Редмонда, рассудил, что нехорошо, когда милый консервативный Белый дом поощряет незаконные действия. Конечно же, на самом [[61]](#footnote-62)

Брешь в овороне

деле я имел в виду следующее — когда «этичные» хакеры обнаруживают дефекты в программном обеспечении, они в первую очередь должны сообщить об этом разработчику ПО, а затем, если ответа не последует, поставить в известность правительство. Только если производитель программного обеспечения отказывается исправить проблему, отметил я, хакеры могут предать обнаруженные факты огласке. По моей логике, если хакеры, собирающиеся на конференции в Лас-Вегасе, способны обнаружить дефекты программ, на это же способны их коллеги из Китая, России и других стран. Поскольку шпионы и преступники и так все узнают, уж лучше пусть об этом знают все. Общие знания о багах в программных продуктах могут означать, что: 1) самые чувствительные сети, вероятно, прекратят использовать данную программу до появления релиза с исправлениями; 2) производителям программного обеспечения придется внести исправления, потому что им либо будет элементарно стыдно, либо их заставят главные клиенты, к примеру банки или Пентагон.

Подобные комментарии не добавили мне симпатий со стороны определенных корпоративных кругов. Им не понравилась моя программная речь, с которой я выступил в том же 2002 году на ежегодной конференции компания RSA1.На конференции RSAсобирается около 12 тысяч практикующих специалистов по кибербезопасности. По вечерам устраиваются большие приемы. Я выступал рано утром. Ожидая своей очереди, я стоял за кулисами и думал, как бы мне сейчас хотелось выпить еще хотя бы чашечку кофе. В большом холле громко играла приглашенная рок-группа. Когда они закончили, я должен был

Третья мировая война: какой она будет?

появиться на сцене в клубах театрального дыма. Представляете эту сцену? Не прекращая думать об острой нехватке кофеина в моем организме, я коротко отметил во вступлении, что, согласно недавнему опросу, многие компании больше тратят на бесплатный кофе для своих сотрудников и клиентов, чем на кибербезопасность. После чего добавил: «Если вы — руководитель крупной компании, в которой больше денег выделяется на кофе, чем на кибербезопасность, будьте готовы, что вас взломают». Пауза. И главное: «Более того, с такими приоритетами вы заслуживаете взлома». Последовали десятки звонков от раздраженных руководителей компаний.

В RSAочень силен корпоративный дух. На конференциях BlackHatгораздо веселее. Увлекательней всего сидеть в тускло освещенном танцевальном зале и наблюдать, как кто-нибудь, не привыкший к публичным выступлениям, проецирует на презентационный экран строчки кода. Забавно видеть недоуменные взгляды сотрудников отеля, обслуживающих конференцию, когда весь зал взрывается хохотом или аплодисментами, что бывает часто, хотя для постороннего в происходящем нет ничего ни смешного, ни достойного похвалы, ни даже понятного. Пожалуй, единственное, что с интересом наблюдают обычные американцев, пробираясь сквозь зал к столам с рулеткой, так это «суд хакеров» — пародия на суд, в ходе которого выясняется, какого рода хакерство следует считать «неэтичным». Очевидно, хакерство самих хакеров к этой категории не относится. Большинство участников конференции просто принимают условие не включать wi-fiна своих ноутбуках. По всем конференц-залам развешаны объявления о том, что использовать wi-fiнастоятельно не рекомендуется. Такие предупреждения в данном случае нужны примерно так же, как объявления в океанариуме о том, что в бассейне с акулами не дежурят спасатели. [[62]](#footnote-63)

Брешь в обороне

1 6 1

В 2009 году организатор конференции Джефф Мосс порвал с многолетней традицией, запланировав в рамках BlackHatодну встречу, доступную не для всех участников. Мосс, который, кстати, на протяжении всей конференции одевался только в черное, ограничил количество гостей на этом собрании 30 вместо обычных 500-800 человек, которые посещают каждую из шести одновременных сессий, что проходят не менее пяти раз в день. На закрытом заседании присутствовали только «старики», те, кто знал, где скрыты виртуальные «тела» в киберпространстве, — бывшие правительственные чиновники, действующие бюрократы, начальники служб безопасности крупнейших корпораций, ученые и старшие должностные лица IT-компаний. Мосс задал им вопрос: «Каких действий мы хотим от Обамы, чтобы защитить киберпространство?» В каком-то странном порыве администрация Обамы назначила Мосса членом консультативного совета по вопросам национальной безопасности, поэтому появился шанс, что он сумеет донести до Белого дома выработанное общими усилиями мнение, если, конечно, его удастся сейчас выработать. Ко всеобщему удивлению, группа достигла согласия по нескольким вопросам — и резкого разногласия по остальным. Консенсус был найден по пяти моментам.

Во-первых, все одобрили идею возвращения к временам, когда федеральное правительство спонсировало исследования и разработки в области кибербезопасности. Этим занималось Агентство перспективных исследований, которое финансировало создание Интернета, но при Буше сфера интернет-безопасности была, по существу, заброшена в пользу сетецентричных приемов ведения войны, без всякого внимания к тому факту, что подобные приемы осуществимы только в условиях безопасного киберпространства. [[63]](#footnote-64)

Третья мировая война: какой она будет?

Во-вторых, незначительное большинство высказалось в пользу разумного регулирования некоторых аспектов кибербезопасности, к примеру принятия федеральных нормативов для операторов интернет-магистралей. Удачной была идея, что правительственные регулятивные органы должны только определять цели, а не контролировать каждый шаг, диктуя средства их достижения. Большинство, однако же, считало, что влиятельные заинтересованные группы в Вашингтоне убедят конгресс заблокировать любые шаги, направленные на регулирование в данной сфере.

В-третьих, было отмечено, что беспокоиться о том, кто провел кибератаку, думать о проблеме атрибуции бесполезно: лучше сконцентрироваться на устойчивости к внешним воздействиям — концепции, которая допускает возможность вредоносной и даже разрушительной атаки и поддерживает идею заблаговременного планирования действий, направленных на восстановление после таких разрушений.

В-четвертых, все единодушно сошлись на том, что не должно быть возможности соединения между локальными сетями и Интернетом. Идея отделения критической инфраструктуры от доступного Интернета оказалась вполне очевидной для этих опытных специалистов в сфере кибербезопасности. Идеи администрации Обамы об «умной» электросети резко критиковали и несколько сотен других специалистов по кибербезопасности, именно потому, что вследствие реализации этих планов энергетические сети, без которых не обходится ни одна другая инфраструктура, станут еще уязвимее перед угрозой неавторизирован- ного вторжения анонимных хакеров, бродящих по Интернету.

Последний пункт, по которому сошлись «мудрейшие мужи» (в числе которых было трое женщин), заключался в следующем — ничто не сможет избавить нас от бед ки- [[64]](#footnote-65)

Врешь в обороне

берпространства до тех пор, пока кто-нибудь не возьмет на себя руководство, которого сейчас так не хватает. В этом наблюдении присутствующие руководители лучших специалистов по кибербезопасности в стране не видели никакой иронии. Они ждали руководства со стороны администрации Обамы. На тот момент Белый дом уже предлагал 30 экспертам возглавить работу по кибербезопасности в администрации президента. Поиски продолжались в Вашингтоне, в то время как здесь, в холле внизу, продолжалась демонстрация того, как нужно взламывать системы. Пока мы, «идейные лидеры», выходили из зала «Помпеи» в некотором унынии и в надежде на руководство, из зала «Везувий» то и дело раздавались возгласы одобрения — кто-то из хакеров «ломал» очередной iPhone. Мы не бросились туда, чтобы посмотреть, какое приложение взломали, а вместо этого направились к столам для блэкджека, где было меньше шансов проиграть, чем у американских компаний и правительственных организаций, мечтавших о безопасном киберпространстве.

**3. Прайвеси и снова на букву «П»**

Когда и левые и правые не соглашаются с предложенным вами решением, это означает две вещи: 1) вероятно, вы на правильном пути; 2) у вас практически нет шансов на то, что ваше решение одобрят. Многое из того, что нужно сделать для обеспечения кибербезопасности Америки, предают анафеме и левая и правая стороны политического спектра. Именно поэтому никакие серьезные меры до сих пор не приняты.

Я проанализирую, что можно с этим сделать, в следующей главе, но сейчас могу сказать вам, что некоторые из [[65]](#footnote-66)

Третья мировая война: какой она будет?

идей потребуют регулирования, а для реализации других потребуется нарушить принцип прайвеси — неприкосновенности частной жизни.

Требовать нового регулирования и создавать риски нарушения прайвеси в Вашингтоне — это все равно что ратовать за насильственные аборты. По моему убеждению, регулирование, по сути своей, нельзя считать ни хорошей, ни плохой мерой — все зависит от того, о каком регулировании идет речь.

Федеральные регуляционные нормы в стиле 1960-х, как правило, полезны для вашингтонских юридических контор, где они были написаны и где способы их обойти обойдутся вам в тысячу долларов за час. Разумное регулирование, подобное тому, которое обсуждалось на конференции BlackHat, формулирует конечную цель и позволяет организациям самостоятельно решать, как ее достичь. Регулирование, которое поставило бы американские компании в экономически невыгодное положение по сравнению с иностранными конкурентами, неблагоразумно, но регулирование, требующее от пользователей минимальных затрат, не кажется мне проделками дьявола. Регулирование, без согласия и даже насильственное, бесполезно почти так же, как требование обязательного присутствия федеральных чиновников на всех заседаниях. Проверка, проводимая третьей стороной, и удаленное подтверждение согласия кажутся вполне разумными подходами. Отказ от регулирования, проверок, вмешательства часто заканчивается событиями, подобными кризису 2008 года и рецессии или использованию свинцовых белил при изготовлении детских игрушек. Чрезмерное регулирование создает искусственно завышенные розничные цены и требования, которые практически (или совсем) не помогают решить изначальную проблему и подавляют креативность и инновации. [[66]](#footnote-67)

Брешь в обороне

В том, что касается прав на неприкосновенность личной жизни и гражданских свобод, я гораздо более категоричен. Мы должны следить, чтобы правительство не нарушало наши права. И это не беспочвенное опасение. Положения Закона о патриотизме1, исполненные благих намерений, в последние годы приводили к многочисленным злоупотреблениям. Другие нормы, препятствующие деятельности правительства, включая сформулированные в Билле о правах и законе о надзоре за иностранными разведками, просто игнорировались. Если меры, необходимые для обеспечения кибербезопасности, открывают возможность дальнейших злоупотреблений со стороны правительства, нам понадобится сделать больше, чем просто принять законы, объявляющие такие действия правительства нелегальными. Это не всегда останавливало их в прошлом (да, мистер Чейни, я вспоминаю вас и здесь). Нам нужно будет создать уполномоченные независимые организации, чтобы следить, не допускаются ли нарушения, и возбуждать дела против тех, кто нарушает принцип прайвеси и гражданские свободы. Самый безопасный путь справиться с этой угрозой — не создавать новые программы, с помощью которых правительственные чиновники могут нарушить наши права. Однако в случае кибервойны могут быть такие ситуации, когда нам придется проверять, возможно ли установить эффективную защиту и запустить новые программы, рискуя нарушить прайвеси. [[67]](#footnote-68)

Третья мировая война: какой она будет?

4. Кассандра

И ОТВЛЕКАЮЩИЙ МАНЕВР

Одной из причин нашей неготовности защищать себя является любопытный феномен. Помните мальчика, который кричал: «Волк! Волк!»? Иногда мальчик, который кричит «Волк!», видит приближение хищника раньше всех остальных. Объединенная комиссия по безопасности 1994 года, комиссия Марша 1997 года, комиссия Центра стратегических и международных исследований 2008 года, комиссия Национальной академии наук в 2009 году и многие другие говорили о кибербезопасности и угрозе кибервойны. Их критиковали, ставя в один ряд с Кассандрами, которые пророчат бедствия. На Землю упадет гигантский метеорит! Изменение магнитных полюсов Земли вызовет солнечный ветер, который уничтожит атмосферу! Почти все настоящие специалисты в соответствующих областях верят, что сценарий с гигантским метеоритом и солнечным ветром вполне реален. Вопрос лишь в том, когда это произойдет. Поэтому, возможно, нам не стоит слишком беспокоиться. Разнообразные комиссии и рабочие группы, предупреждающие об опасности кибервойны, с определением сроков не ошибались. Они говорили нам, что пока есть время на принятие предварительных мер. Следует помнить, что, несмотря на плохую репутацию, Кассандра не ошибалась в своих предсказаниях — просто из-за проклятия Аполлона ей никто никогда не верил.

К сожалению, слишком многие верят в угрозу кибертерроризма. А кибертерроризм — это утка, отвлекающий маневр. Слова «кибер» и «терроризм» вообще не следует употреблять вместе, поскольку они вызывают в уме образ Бен Ладена, ведущего кибервойну из пещеры. Наверное, [[68]](#footnote-69)

Брешь в обороне

он на это не способен, по крайней мере, пока (более того, он живет вовсе не в пещере, а скорее на какой-нибудь уютной вилле). На самом деле у нас нет надежных доказательств того, что террористы когда-либо проводили кибератаки на инфраструктуру. До настоящего времени террористы не проводили крупных атак в Интернете и не использовали Интернет для атаки физических систем, но с помощью Интернета планировали и координировали атаки на посольства, железные дороги, гостиницы. Они используют Интернет для привлечения финансов, поиска новобранцев и обучения. Когда «Аль-Каида» лишилась учебных полигонов после 11 сентября, многое из того, что происходило там, переместилось в Интернет. Дистанционное обучение с видеороликами о том, как создавать взрывные устройства из подручных средств или отрубать головы, так же эффективно, как и занятия на полигонах. Кроме того, благодаря Интернету террористам не приходится собираться в одном месте, что раньше давало международным правоохранительным органам прекрасную возможность поймать предполагаемых террористов или нанести по ним ракетный удар. Интернет-обучение представляет большую опасность и приводит к многочисленным атакам «волков-одиночек» — террористов, никак не связанных с центром «Аль-Каиды». Но особенно эффективно «Аль-Каида» и другие группы используют Интернет для пропаганды. Распространяя видеоролики с отсечением голов и радикальныой интерпретацией Корана, террористические группировки сумели достучаться до широкой аудитории, сохраняя при этом относительную анонимность.

Если «Аль-Каида» до сих пор еще не проводила кибератак, все запросто может измениться. С каждым годом стоимость и прочие входные барьеры, ограничивающие использование этой технологии, снижаются. Чтобы про- [[69]](#footnote-70)

Третья мировая война: какой она будет?

вести разрушительную кибератаку, не требуется больших производственных затрат, как, допустим, для создания ядерной бомбы. Однако в контрольном программном обеспечении электросети разобраться способен далеко не каждый. Одно дело — найти способ взломать сеть, и совсем другое — знать, что делать, когда вы проникли внутрь. Хорошо спонсируемые террористические группировки могут найти профессиональную хакерскую тусовку, которая согласится провести кибератаку за большие деньги, но до сих пор такого не случалось. Вероятно, потому, что большинство хакеров считают представителей «Аль-Каиды» ненормальными, опасными и ненадежными. Если преступные хакерские группировки думают так, значит, террористам вряд ли удастся сработаться с ними.

5. Деньги решают все

Еще одна причина такой инертности заключается в том, что кое-кому хочется оставить все как есть. У некоторых уже все «куплено». Выше я упоминал, что в ответ на сообщение о возможном кризисе кибербезопасности Джордж Буш первым делом поинтересовался, что думает на этот счет руководитель компьютерной корпорации, один из главных «доноров» его предвыборной кампании. Наверное, вы уже догадались, что администрация Буша не была заинтересована занимать жесткую позицию по отношению к частному сектору. Первая «Стратегия национальной безопасности Соединенных Штатов», опубликованная в 2003 году, напоминает учебник по экономике, ратующий за свободный рынок. Возможно, вы удивитесь, но демо- [[70]](#footnote-71)

Брешь в обороне

кратическая администрация находится в плену тех же убеждений. Кто-то может предположить, что новая администрация готова решить проблему несостоятельности рынка в сфере кибербезопасности, введя новые регламенты, но это не так. Чтобы понять почему, отправимся на одно мероприятие.

Это был роскошный прием — собрались все звезды Вашингтона. Более 250 гостей пришли на празднование бракосочетания Мелоди Барнс и Мэрленда Бакнера. Барнс, советник президента Обамы по внутренней политике, знала будущего мужа много лет, прежде чем они начали встречаться. Их знакомство состоялось, когда она являлась членом клуба Капитолийского холма1 [[71]](#footnote-72), работала на Теда Кеннеди, а он служил начальником штаба Гарольда Форда-младшего. После короткой церемонии в Объединенной церкви Христа молодожены и гости переместились в особняк Андрю В. Меллона в Вашингтоне, который преобразили в стиле Южного побережья, со столовым серебром и столами, украшенными цветами орхидей. Местное безуглеводное меню состояло из жаркого на ребрышках, морских окуней и весенних овощей, элегантно разложенных по коробочкам обэнто. Гостей угощали мороженым и печеньем, чтобы те продержались до ночи, когда всех распустят по домам.

В число гостей, которых светский репортер NewYorkTimes, занимающийся свадьбами и торжествами, назвал «стаей высокопоставленных чиновников администрации Обамы», входили Рам Эммануэль, возглавляющий аппарат сотрудников Белого дома, и Валери Джарретт, глав-

Третья мировая война: какой она будет?

ная советница и помощница президента по внутрипра- вительственным делам и связям с общественностью. Мой друг Мона Сатфен, заместитель Рама Эммануэля, отплясывала весь вечер, как и бывший глава президентской администрации Клинтона Джон Подеста. Также присутствовала, хоть и не упоминалась в NewYorkTimes, еще одна высокопоставленная «стая» — Microsoft. Бакнер, бывший директор по связям с правительством крупнейшей в мире софтверной компании, а ныне независимый лоббист, тоже пригласил несколько друзей. С тех пор, как Бакнер стал работать самостоятельно, он принимал вознаграждения за лоббирование, треть которых поступала от Microsoft. Очень жаль, что репортеры MotherJonesне освещают свадьбы. Они наверняка заметили бы, что в тот вечер администрация Обамы буквально нырнула в койку к Microsoft.

Microsoftвходит в публикуемый на сайте OpenSecret. orgсписок из 30 влиятельных организаций, инвестирующих в политику. В списке преобладают торговые ассоциации, Microsoftвходит в семерку лидеров. Конечно, Microsoftнаверстывает упущенное. До поединка с Министерством юстиции по антимонопольным вопросам в конце 1990-х эта компания, устроившаяся на Западном побережье, хотела лишь, чтобы ее оставили в покое, и была вне политики. До 1998 года Microsoftи ее сотрудники не особенно стремились тратить свои фонды на поддержку политиков с Восточного побережья.

Все изменилось, когда юристы из администрации Клинтона заявили, что продажа Windowsпроводилась с намерением создать монополию. Посыпались пожертвования из вновь учрежденного комитета политических действий, равно как и от отдельных сотрудников Microsoft. С 1998-го по 2002 год большая часть этих средств адресовалась республиканцам. Затем в 2004-м [[72]](#footnote-73)

Брешь в обороне

Microsoft, то ли недовольная войной, то ли недооценившая перспективы бушевской кампании, начала спонсировать демократов почти в два раза щедрее, чем республиканцев. В 2008 году Microsoftувеличила это соотношение, предоставив 2,3 миллиона долларов демократам и только 900 тысяч республиканцам.

Возможно, комитет политических воздействий и сотрудники корпорации имеют добрые намерения, как многие американцы, которые пожертвовали деньги и потратили время на кампанию Обамы только ради того, чтобы видеть его на посту президента. Мэрлэнд Бакнер заявил корреспонденту новостной службы MediaGeneral, что он предпочел бы «беспрекословно» соблюсти все правила Белого дома, чтобы избежать любого конфликта интересов из-за новой работы Барнс, и пообещал не использовать свои отношения с супругой для привлечения клиентов. Но у корпорации Microsoftесть своя программа, и она ясна — не допустить регулирования в индустрии; не позволить Пентагону отказаться от нашего программного обеспечения, сколько бы дыр в защите там ни нашли; не обсуждать проблемы производства программного обеспечения Microsoftза океаном; не обсуждать взаимотноше- ния компании с Китаем. У Microsoftнеограниченные ресурсы, миллиарды долларов наличными или в виде ликвидных активов. Microsoft— это невероятно успешная империя, фундаментом которой является лидирующее положение на рынке и производство товаров низкого качества. На протяжении долгих лет операционная система и приложения, к примеру вездесущий EnternetExplorer, по умолчанию устанавливались на компьютеры, которые мы покупаем. Чтобы получить альтернативу, требовались время и немалые усилия, и так продолжалось до тех пор, пока в последнее десятилетие Appleне стал открывать магазины и активно рекламироваться. [[73]](#footnote-74)

Третья мировая война: какой она будет?

Честно говоря, Microsoftизначально не стремилась создавать программы для управления критическими системами. Ее целью было вывести на рынок продукт с минимальными затратами на производство. Тогда она не видела причин вкладываться в процессы, гарантирующие и контролирующие качество, чего требовало НАСА от программного обеспечения космических полетов. Проблема в том, что люди начали использовать продукцию Microsoftв критических системах, от платформ Министерства обороны до основных банковских и финансовых сетей. Эта продукция была гораздо дешевле специально разработанных программных приложений. Время от времени в правительстве возникает стремление к повышению эффективности, на фоне которого внимание правительственных организаций привлекают экономичные подходы, используемые в промышленности. Пример тому — COTS. Идея заключалась в том, чтобы заменить коммерческими коробочными программными продуктами (COTS) специализированное программное обеспечение, которое раньше приходилось заказывать. На протяжении холодной войны Пентагон инициировал появление многих таких технологических новшеств. Помню, как мне рассказывали о фотоаппаратах без пленки, которые разрабатывались для правительства. (Я не мог понять, как он будет работать, до тех пор, пока не купил такой в BestBuy1 [[74]](#footnote-75)десять лет спустя.) Сначала технология разрабатывалась в военных целях, затем проникала в коммерческую сферу. COTSперевернул этот процесс с ног на голову. До 1990-х большая часть используемых в Пентагоне программных средств изготавливалась под заказ собственными силами

Брешь в обороне

или немногочисленными доверенными военными подрядчиками. Не существовало двух одинаковых систем, что отвечало интересам производителей. Системы, которые они разрабатывали, стоили чрезвычайно дорого. Это очень осложняло возможность взаимодействия между разными структурами. COTSснизило затраты и позволило Пентагону использовать совместимые системы, поскольку все они писались на одних языках программирования и на базе одинаковых операционных систем. Разрабатывалось все больше и больше программных приложений. Была создана глобальная информационно-управленческая сеть GIGиз 5,5 миллиона компьютеров. Сетецентричные приемы ведения войны обеспечивали огромные преимущества американским военным, но вместе с тем и делали нас невероятно уязвимыми.

COTSперенес в Пентагон те же баги и уязвимые места, что есть в наших домашних компьютерах. В 1997 году ВМФ США убедился, как опасно порой полагаться на эти системы в проведении боевых операций. Военный корабль Yorktownбыл использован в качестве испытательного полигона в рамках программы ВМФ «Умный корабль». Yorktownоборудовали сетью из 27 рабочих станций на процессорах Pentiumи под управлением операционной системы WindowsNT. Работу станций координировал сервер, на котором также была установлена ОС Windows. Система контролировала все аспекты деятельности корабля, начиная с наводки орудия и заканчивая скоростью вращения двигателя. Когда система дала фатальный сбой, как часто бывает с Windows, крейсер превратился в плавающую консервную банку.

После инцидента с Yorktownи других сбоев систем на базе WindowsПентагон обратил внимание на Unixи созданные на его основе системы Linux. Linux— система с открытым кодом. Это значит, что пользователь может [[75]](#footnote-76)

Третья мировая война: какой она будет?

редактировать код операционной системы. У Windows(и большинства других коммерческих программных продуктов) исходный код считается собственностью разработчика и тщательно защищен. Открытый код дал бы Пентагону ряд преимуществ. Во-первых, программисты Пентагона и военные подрядчики могли бы модифицировать программное обеспечение под собственные нужды. То есть изменить код так, чтобы устранить ненужные фрагменты операционной системы и тем самым избавиться от лишних багов. Во-вторых, сократив размер операционной системы, они могли бы с помощью специальных средств проверить остальные строки кода на предмет обнаружения багов, вредоносного кода и прочих уязвимостей.

Microsoftвышла на тропу войны, чтобы замедлить переход правительственных организаций на Linux, и организовал ряд выступлений перед постоянными комитетами (выступал даже сам Билл Гейтс). Тем не менее, поскольку правительственные организации уже использовали Linux, я попросил Агентство национальной безопасности оценить ситуацию. АНБ, немало удивив сторонников открытого кода, влилось в их ряды, публично указав «координаты» ошибок в операционной системе Linuxс целью улучшения ее безопасности. Из Microsoftмне дали понять, что если американские власти будут содействовать Linux, Microsoftпрекратит с ними всякое сотрудничество. И если меня это не пугало, то на других могло оказать влияние. Программное обеспечение Microsoftдо сих пор приобретает большинство федеральных ведомств, несмотря на то что Linuxраспространяется бесплатно.

Банки и финансовая промышленность тоже начали искать альтернативные системы с открытым кодом после неоднократных сбоев в системах Microsoft, которые стоили им по несколько сотен миллионов долларов в год. В 2004 году банковская группа FinancialServices

Брешь в обороне

Roundtableотправила делегацию банковских специалистов по компьютерной безопасности в Редмонд (штат Вашингтон) на встречу с представителями Microsoft. Они потребовали доступа к программному коду. Им отказали. Они потребовали предоставить им требования к качеству программного продукта, которыми пользуется Microsoft, чтобы сопоставить их с нормами других производителей программного обеспечения. Им отказали. Отношение Microsoftк американским банкам противоречит объявленной в 2003 году программе. В соответствии с этой программой Microsoftдолжна предоставлять участвующим в ней национальным и международным организациям доступ к исходному коду — так Microsoftответила на претензии по поводу безопасности своей операционной системы. Первыми участниками этой программы были Россия, Китай, НАТО и Великобритания. Банки пригрозили переходом на Linux. Microsoftответила, что это будет стоить очень дорого. Более того, сейчас разрабатывается новая версия Windowsс кодовым названием Longhorn, и она будет гораздо лучше. Longhornвышел под именем Vista. Vistaпоявилась в продаже позже обещанного срока в связи с обнаружением дефектов в тестовой программе. Затем с проблемами столкнулись корпоративные пользователи. Молва шла, и многие компании решили не переходить на новую операционную систему. В ответ на это Microsoftзаявила, что прекратит поддержку предыдущих систем, заставляя клиентов пойти на замену ОС.

Сотрудники Microsoftпризнавались, что компания не воспринимала проблемы безопасности всерьез, даже когда подвергалась хакерским атакам. Да и с какой стати? Реальной альтернативы программному обеспечению Microsoftне существовало, и компания купалась в деньгах. Когда появилсяLinux, а затем Appleстал непосредственным конкурентом, в Microsoftдействительно предприня- [[76]](#footnote-77)

Третья мировая война: какой она будет?

ли меры по улучшению качества. Но сначала они наняли множество делегатов и лоббистов, которые выступали на конференциях, перед клиентами, в правительственных организациях и ратовали против совершенствования в сфере безопасности. Для Microsoftгораздо дешевле нанять делегатов и лоббистов, чем разрабатывать более безопасные системы. Это одна из нескольких влиятельных компаний, которых устраивает нынешнее положение вещей и которым невыгодны какие-либо перемены.

Б. А Я ДУМАЛ, вы этим
ЗАНИМАЕТЕСЬ

Перемены, однако, происходят. Вслед за Соединенными Штатами все больше стран создают наступательные кибервоенные организации. Киберкомандование США несет дополнительную оборонительную миссию — защищать Министерство обороны. Но кто защитит все остальное?

Министерство национальной безопасности защищает федеральные власти США, не имеющие отношения к Министерству обороны. Всем остальным приходится полагаться только на себя. Не существует федерального ведомства, в задачу которого входит защищать банковскую систему, транспортные сети или энергосистему страны от кибератак. Киберкомандование и МНВ полагают, что, защищая правительственных клиентов, они тем самым немного помогают и частному сектору. Власти считают, что задача обороны частных корпораций лежит на них самих. Правительственные чиновники скажут вам, что частный сектор все устраивает, — он не хочет, чтобы власти вмешивались в его системы. В конце концов, никто в прави- [[77]](#footnote-78)

Брешь в обороне

тельстве не знает, как управлять банковскими сетями, сетями железных дорог или энергосистем. Старшие менеджеры крупных компаний (занимающиеся программным обеспечением, безопасностью, связями с общественностью, информационной безопасностью) заявят примерно то же самое: мы готовы тратить на компьютерную безопасность, чтобы защитить себя от киберпреступности, которая грозит нам повседневно.

Однако нельзя от нас ожидать, чтобы мы знали, как защититься от кибервойны в государственном масштабе. Затем они добавляют что-то вроде: «Защита от вооруженных сил других стран — задача государства, за это мы и платим налоги».

На заре эпохи стратегических ядерных вооружений Соединенные Штаты развернули тысячи ракет ПВО наземного базирования, чтобы защитить население и промышленность, а не только военные объекты. Каждый крупный город окружало кольцо ракетных баз Nike, готовых сбить советские бомбардировщики. На заре эпохи кибервойн американские власти предлагают населению и организациям защищаться самостоятельно.

Один мой друг спросил: «Вы можете представить, чтобы в 1958 году Пентагон посоветовал U.S. Steelи GeneralMotorsприкупить ракеты Nike, чтобы защититься? А ведь, по сути, именно это сегодня и рекомендует нам президент Обама».

По фундаментальному вопросу — в чьи задачи входит защита американской инфраструктуры в кибервойне — власть и промышленность никак не могли прийти к взаимопониманию. В результате никто не защищает потенциальные мишени, по крайней мере, никто в Соединенных Штатах. В других странах, которые однажды могут стать нашими противниками, оборона, возможно, окажется несколько лучше нашей. [[78]](#footnote-79)

Третья мировая война: какой она будет?

Прорыв в киберобороне

Как мы уже отмечали, Соединенные Штаты, возможно, обладают самыми совершенными и комплексными возможностями для ведения кибервойны, за нами следуют Россия, Китай и, вероятно, Франция. Они находятся во втором эшелоне и отстают совсем немного, и еще около 20 государств, включая Иран и Северную Корею, тоже имеют киберпотенциал. Верен данный рейтинг или нет, ему доверяют сами кибервоины. Можете даже представить, как сидят после работы американские гики, попивают свой «Рэд Бул» и скандируют «Сэ-Шэ-А! Сэ-Шэ-А!», как на Олимпиаде, или «Мы са-мы-е пер-вы-е!», как на футболе. Но верно ли, что мы самые первые? Разумеется, это зависит от того, какие критерии принимать в расчет. В том, что касается наступательного киберпотенциала, Соединенные Штаты, скорее всего, действительно занимают первое место. Но кибервойна не ограничивается одним лишь наступлением. Существует такой показатель, как киберзависимость, — степень зависимости страны от киберуправляемых систем. В двусторонней войне и она имеет значение. Как я узнал, когда спросил о планах кибервойны в Афганистане в 2001 году, для кибервоинов может не оказаться мишеней. В двусторонней кибервойне это дает Афганистану определенное преимущество. Важно, способна ли страна защитить себя от кибервойны. Очевидно, Афганистан может защититься просто потому, что у него нет сетей, но теоретически у страны могут быть и сети, и возможность их оборонять. Оборонительные киберспособности, таким образом, являются существенным критерием: имеет ли страна возможность отключиться от киберпространства всего остального мира или засечь кибератаки, идущие изнутри страны, и остановить их? [[79]](#footnote-80)

Брешь в обороне

Даже если Соединенные Штаты обладают самым совершенным кибероружием, нападение не заменит дыру в защите. Как отметил адмирал в отставке Макконел, «поскольку мы самая развитая в технологическом отношении страна — нити сетей опутывают все наше общество, — мы более других зависимы от этих нитей, а значит, и более уязвимы». Наша экономика связана с Интернетом больше, чем экономика любой другой страны. Все 18 секторов гражданской инфраструктуры, которые Министерство национальной безопасности назвало критически важными, функционируют в Интернете и уязвимы перед внешними кибератаками. Сравните с Китаем, который развивает не только наступательные, но и оборонительные способности. Кибервоины Народно-освободительной армии Китая обязаны и наступать, и обороняться в киберпространстве, и, в отличие от американских военных, под словом «защита» они понимают не только защиту военных объектов.

Я не являюсь сторонником расширения полномочий Пентагона в сфере защиты гражданских систем США, но следует отметить, что не существует никаких других ведомств или подразделений федеральных властей, которые могли бы взять на себя такую ответственность. В свете воздержания от регулирования, которое началось при Клинтоне, продолжилось при Буше и передалось администрации Обамы, от частного сектора не требовалось укреплять безопасность, да и власти не стремились играть в этом активную роль. В Китае сети, образующие интернет-инфраструктуру страны, целиком контролируются правительством, которое либо напрямую владеет ими, либо состоит в тесном сотрудничестве с частным сектором. Никто не обсуждает «цену», когда китайское правительство требует ввести новые меры безопасности. Сети поделены на крупные сегменты между правительством,

Третья мировая война: какой она будет?

научным и коммерческим сообществами. Китайское правительство имеет и власть, и средства, чтобы отсоединить китайское интернет-пространство от всего остального мира, что, скорее всего, и сделает в случае конфликта с Соединенными Штатами. Американское правительство таких полномочий и возможностей не имеет. В США Федеральная комиссия по связи обладает законным правом регулировать, но большинство населения предпочитает, чтобы она этого не делала. В Китае правительство может устанавливать и вводить в действие стандарты, но идет гораздо дальше.

Интернет в Китае больше похож на интранет — внутреннюю сеть компании. Правительство является поставщиком услуг и отвечает за сетевую защиту. В Соединенных Штатах не так. Роль американского правительства не столь существенна. Как я упоминал во второй главе, наиболее обсуждаемое китайское средство интернет- цензуры — GreatFirewall— дает стране преимущество в обороне. Технологию, которую китайцы используют для просмотра электронной почты на предмет противозаконных высказываний, можно применять и для выявления вредоносного ПО. Кроме того, Китай инвестировал в развитие собственной операционной системы, которая невосприимчива к возможным сетевым атакам, хотя технические проблемы отсрочили ее ввод в эксплуатацию. Китай начал, а затем временно приостановил попытки установить на все компьютеры страны программное обеспечение, предназначенное якобы для предотвращения детям доступа к порнографическим сайтам. Истинной целью этой акции, по мнению большинства экспертов, было обеспечить китайскому правительству возможность контролировать каждый рабочий стол страны. (Когда слухи просочились в сообщество хакеров, те быстро обнаружили уязвимые места программы, которые позволяют кон- [[80]](#footnote-81)

Брешь в обороне

тролировать всю систему, и установку пришлось прекратить.) Эти попытки показывают, как серьезно китайцы воспринимают задачу обороны, а также демонстрируют, на что направлены эти усилия. Китай между тем серьезно отстает от США в автоматизации критических систем. Система энергоснабжения страны, к примеру, во многом управляется вручную, а в кибервойне это преимущество.

Как измерить кибервоенный

ПОТЕНЦИАЛ

Было бы здорово, если бы в определении кибервоенного потенциала важен был лишь один фактор — наша способность нападения на другие государства. Если бы учитывалось только это, Соединенные Штаты действительно выигрывали бы в сравнении с другими странами. К сожалению, для реалистичной оценки кибервоенного потенциала необходимо принимать во внимание два других аспекта: защиту и зависимость. Защита — это способность страны предпринимать меры в условиях нападения извне, меры, которые блокируют или смягчают атаку. Зависимость — это степень интернетизации страны, распространенности сетей и систем, которые могут подвергнуться кибератаке. Чтобы проиллюстрировать, как взаимодействуют эти факторы (нападение, защита и зависимость), я составил таблицу. В ней представлены коэффициенты по каждому из трех факторов. Софисты заявят, что это слишком упрощенный метод: я измеряю по одной шкале все три аспекта, а затем суммирую их, чтобы получить общее количество баллов для конкретной страны. Подсчет очков для каждой страны основан на моих оценках ее наступательных воз- [[81]](#footnote-82)

Третья мировая война: какой она будет?

можностей, оборонительного потенциала и зависимости от компьютерных систем. В этом заключается парадокс: чем меньше уровень интернетизации страны, тем больше баллов у нее в графе «Независимость». Развитая сеть — хороший фактор для страны, но не тогда, когда вы оцениваете ее способность противостоять кибервойне.

Общий кибервоенный потенциап

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Нападение | Независимость | Защита | Итого |
| США | 8 | 2 | 1 | 11 |
| Россия | 7 | 5 | 4 | 16 |
| Китай | 5 | 4 | 6 | 15 |
| Иран | 4 | 5 | 3 | 12 |
| СевернаяКорея | 2 | 9 | 7 | 18 |

Китай превосходит в защите отчасти потому, что имеет возможности отключить страну от всего остального киберпространства. У США, напротив, не ни подобных проектов, ни возможностей, поскольку интернет-соединения находятся в частном владении и управляются в частном порядке. Китай может ограничить использование киберпространства в случае кризиса, отключив второстепенных пользователей. США не могут. Северная Корея получает больше всего баллов по графам «Защита» и «Независимость». Ей проще всего отключить свои немногочисленные сети от киберпространства. Более того, лишь несколько систем этой страны зависят от киберпространства, так [[82]](#footnote-83)

Брешь в обороне

что любая крупная кибератака на Северную Корею не нанесет практически никакого вреда. Помните, что киберзависимость — это не процент домов с широкополосным доступом в Интернет или количество смартфонов на душу населения, это степень зависимости критических инфраструктур (электросети, железных дорог, трубопроводов, логистических цепочек) от Сети. Если рассматривать защиту и независимость в совокупности, многие страны значительно опережают Соединенные Штаты. Их способность выжить в кибервойне и обойтись малыми потерями и создает брешь в киберобороне США. Они способны начать кибервойну и причинить нам огромный ущерб и в то же время сами практически не пострадают от ответных действий США в киберпространстве. В силу существования бреши в киберобороне мысль о нападении на США для некоторых стран может оказаться весьма привлекательной. Задача ликвидировать эту брешь должна стать приоритетной для американских кибервоинов. Развивая только наступательные возможности, мы от нее не избавимся. На нынешнем этапе невозможно сократить и нашу зависимость от сетевых систем. Поэтому единственный способ увеличить наш общий кибервоенный потенциал — усовершенствовать защиту. Давайте посмотрим, как это можно сделать.

Глава 5

□ боронитепьная стратегия

В

оенные теоретики и государственные деятели, начиная с Сунь Цзы и заканчивая фон Клаузевицем и Германом Каном, на протяжении столетий определяли и переопределяли военную стратегию по-разному, но, как правило, соглашались в одном — она включает в себя цели, средства (широко трактуемые), ограничения (иногда устанавливаемые) и, возможно, последовательность действий. Короче говоря, военная стратегия — это комплексная теория о том, что мы хотим делать и как. Отчасти по тре- [[83]](#footnote-84)

Оборонительная стратегия

бованию конгресса Соединенных Штатов периодически открыто публиковали Стратегию национальной безопасности и Национальную военную стратегию. Вооруженные силы США имеют множество субстратегий, в числе которых можно упомянуть морскую стратегию, стратегию подавления восстаний, ядерную стратегию. Американское правительство публикует стратегии, которые связаны с военными опосредованно, — это стратегии контроля за нелегальным оборотом наркотиков, борьба с терроризмом и распространением оружия массового поражения. Ах, да, еще есть Национальная стратегия по безопасности киберпространства, появившаяся в 2003 году, но только она недоступна общественности. Поскольку у нас нет стратегии кибервойны, нет у нас и комплексной теории о том, как решать ее важнейшие задачи. Чтобы доказать это, давайте перечислим двадцать вопросов и посмотрим, найдутся ли ответы даже на самые очевидные из них.

О Что мы будем делать, если обнаружим, что в результате кибератаки вся западная часть Соединенных Штатов осталась без электричества?

0 Наступление кибервойны для нас выгодно или оно ставит нас в неблагоприятные условия?

0 Намерены ли мы использовать кибероружие только в ответ на его применение против нас?

0 Будем ли мы прибегать к кибероружию в малых и больших конфликтах? Станем ли мы использовать его на ранних этапах, поскольку оно дает нам исключительные преимущества в достижении наших целей — позволяет, к примеру, быстро завершить конфликт? [[84]](#footnote-85)

Третья мировая война: какой она будет?

0 Нужны ли нам планы и возможности ведения «автономной» кибервойны против другого государства? Будем ли мы сражаться в киберпространстве, когда не ведем боевых действий в реальном мире?

0 Считаем ли мы киберпространство местом (наряду с морем, воздушным пространством или космосом), где мы должны иметь военное превосходство и в котором будем проводить военные операции одновременно с действиями в других сферах?

0 Насколько верно мы должны идентифицировать, кто атаковал нас в киберпространстве, прежде чем реагировать? Какие стандарты мы будем использовать для идентификации нападающих?

0 Будем ли мы скрывать, что провели кибератаку?

0 Станем ли мы в мирное время внедряться в сети других государств? Если да, должны ли существовать какие-либо ограничения?

0 Как мы будем действовать, если обнаружим, что другие страны проникли в наши сети в мирное время? А что, если они оставят логические бомбы в сетях нашей инфраструктуры?

0 Намерены ли мы использовать кибероружие в основном против военных объектов? Что мы вкладываем в понятие «военные объекты»?

0 Насколько важно избегать сопутствующих потерь, используя кибероружие? Как может такой подход ограничить применение кибероружия?

0 Если мы подверглись кибератаке, при каких обстоятельствах мы можем или должны применять в ответ [[85]](#footnote-86)

Оборонительная стратегия

наступательное вооружение? Должен ли ответ на этот вопрос быть заранее известен?

0 Каких целей мы хотим достичь с помощью кибероружия в рамках кибервойны или в сочетании с военными действиями?

0 Нужна ли точная граница между миром и кибервойной или в наших интересах размыть эту линию?

0 Станем ли мы участвовать в кибервойне в союзе с другими странами, помогая защищать их киберпространство и делясь кибероружием, тактикой, целями?

0 На каком уровне должны приниматься окончательные решения по вопросам использования кибероружия, его выбора, утверждения целей?

0 Есть ли определенные типы целей, которые, по нашему мнению, нельзя атаковать с помощью кибероружия? Станем ли мы все же атаковать, если аналогичные американские объекты подвергнутся атаке кибероружием?

0 Как мы будем объявлять о наших намерениях относительно использования кибероружия в мирное время и в эпоху кризиса? Существуют ли способы использовать кибероружие для устрашения противника?

0 Если противник успешно проводит широкое наступление на наши военные объекты или экономическую инфраструктуру, как это должно влиять на наши военные и политические стратегии?

1 sv

Третья мировая война: какой она будет?

Можно ли найти ответы на эти вопросы в официальных документах, протоколах заседаний конгресса, правительственных выступлениях? Мне не удалось. Справедливости ради стоит сказать, что это непростые вопросы, чем отчасти и объясняется, почему они до сих пор не переросли в стратегию. Ответы на них зависят от опыта отвечающего, меры его ответственности, а также от вытекающих из этих факторов последствий. Любой генерал хотел бы иметь возможность щелкнуть тумблером и отключить силы противника, особенно если знает, что тот не сможет ответить. Современные генералы, однако же, знают, что вооруженные силы — это один из многих инструментов государства, и об успехе военных судят не по тому, какой урон они нанесли противнику, а по тому, как они сумели защитить и поддержать всю остальную страну, включая ее фундамент — экономику. Военные и дипломаты уяснили из опыта прошлых лет, что существует тонкая грань между заблаговременной подготовкой к обороне и провокационными действиями, которые могут повысить вероятность конфликта. Таким образом, создать кибервоенную стратегию не значит воспользоваться новым типом оружия, как сделали американские военные, сбросив ядерную бомбу на Хиросиму.

После Хиросимы потребовалось полтора десятилетия для того, чтобы разработать и принять комплексную стратегию применения, а точнее — неприменения ядерного оружия. В первые годы атомной эпохи несколько раз едва не начиналась война. Ядерная стратегия, которая в конце концов была принята, существенно снизила этот риск. В данной главе мы не раз будем возвращаться к ядерной стратегии. Огромная разница между ядерным и кибероружием очевидна, но некоторые концепции, найденные в ходе разработки ядерной стратегии, применимы и сейчас, другие — нет. Тем не менее, рассматривая события [[86]](#footnote-87)

Оборонительная стратегия

1950-1960-х годов, мы кое-что узнаем о том, как можно разрабатывать комплексную стратегию использования нового типа оружия. Кроме того, некоторые концепции мы можем взять и адаптировать для систематизации кибер- военной стратегии.

РОПЬ ОБОРОНЫ В НАШЕЙ СТРАТЕГИИ
КИБЕРВОЙНЫ

В начале книги я спросил, что для нас лучше — мир с кибероружием и кибервойной или идеальная вселенная, в которой подобного никогда не существовало? Последующие главы показали, по крайней мере мне, что в положении Соединенных Штатов появились новые уязвимые места по сравнению с другими странами, также обладающими киберпотенциалом. На самом деле мы больше зависим от контролируемых компьютерами систем, но при этом до сих пор не сумели создать национальную кибероборону, а значит, более уязвимы в кибервойне, чем Россия и Китай. Соединенные Штаты рискуют гораздо больше, чем Северная Корея, не имеющая такой тесной связи с Интернетом. Мы уязвимы перед странами и организациями, у которых отсутствует киберпотенциал, но есть средства, чтобы нанять команду очень талантливых хакеров. А если проанализировать, к примеру, как могла бы развиваться кибервойна между США и Китаем? Наше наступательное кибероружие, возможно, лучше, но тот факт, что мы способны вывести из строя китайскую систему противовоздушной обороны, едва ли послужит утешением американцам, если вдруг Народно-освободительная армия оставит наши города без электричества на целые [[87]](#footnote-88)

Третья мировая война: какой она будет?

недели, закроет финансовые рынки, исказив их данные, создаст повсеместный дефицит, испортив логистические системы американских железных дорог. Несмотря на то что Китай — вполне передовая страна, немалая часть его инфраструктуры до сих пор не зависит от компьютерных сетей, контролируемых из киберпространства. Китайское правительство может меньше беспокоиться по поводу временных неудобств, которые могут выпасть на долю его граждан.

Сейчас кибервойна ставит Америку в невыгодное положение. Что бы мы ни сделали кому-то, скорее всего, нам навредят больше. Мы должны изменить эту ситуацию.

Пока мы не сократим уязвимые места в нашей киберобороне, будем вынуждены сдерживать самих себя. Мы знаем, что нам могут сделать другие, и поэтому запросто окажемся в такой ситуации, когда придется ограничивать себя даже в оправданном применении обычных вооружений. Кибероружие других стран будет удерживать нас от действий, и не только в киберпространстве. Останется ли у американского президента выбор послать авианосцы, чтобы предотвратить действия Китая, если обострятся разногласия последнего с соседними странами по поводу морских месторождений, или конфликт Китая с Тайванем? Станет ли президент отправлять флот в Тайваньский пролив, как сделал Клинтон в 1996 году, зная, что блэкаут в Чикаго — это сигнал о том, что электричество отключится по всей стране, если мы вмешаемся? Или что проблемы с данными на Чикагской товарной бирже — это пример того, что может произойти со всеми важнейшими финансовыми институтами? А что, если китайцы проведут кибератаку, после которой все авианосцы останутся болтаться в океане, как пустые консервные банки? Станет ли президент рисковать и разворачивать военно-морские силы лишь затем, чтобы противник про-

Оборонительная стратегия

демонстрировал, что он способен остановить, ослепить, сбить с толку наши войска?

Тот факт, что наши важнейшие системы так уязвимы перед кибервойной, усиливает шаткость нашего положения. Пока экономические и военные системы Америки не защищены, у противников страны будет соблазн ее атаковать в периоды обострения разногласий. Наши оппоненты имеют основания думать, что у них есть возможность изменить политический, экономический и военный баланс, продемонстрировав миру, что они способны сделать с Америкой. Они могут полагать, что угроза большего вреда покажется вполне правдоподобной и помешает США предпринять ответные действия. Однако в случае кибератаки американским лидерам, скорее всего, придется реагировать. Этот отклик едва ли ограничится киберпространством, и конфликт может быстро обостриться и выйти из-под контроля.

Такое положение убеждает нас в необходимости принятия срочных мер по сокращению стратегического дисбаланса, вызванного уязвимостью США в возможной кибервойне. Для этого недостаточно только усилить наш наступательный киберпотенциал. Он едва ли устранит диспропорцию. В отличие от войны с применением обычных видов оружия, здесь превосходство в нападении не поможет обнаружить и разрушить наступательные мощности противника. Средства, способные нанести урон США, возможно, уже находятся на нашей территории. Они могли попасть сюда не только через киберпространство, но и по дипломатической почте, на CD-дисках или на USB-носителях, в портфелях бизнесменов. Что нам нужно, так это снизить риск того, что любое государство станет угрожать нам применением кибероружия, а для этого необходимо иметь надежную оборону. Мы должны заронить сомнения в умах потенциальных хакеров, что-

Третья мировая война: какой она будет?

бы они не пытались нас атаковать, осознавая мощь нашей обороны. Пусть потенциальные противники Соединенных Штатов думают, что их киберстрелы отскочат от наших щитов. Или, по меньшей мере, считают, что наши важнейшие системы достаточно защищены и ущерб, который они нанесут нам, не станет решающим. Но до этого еще далеко.

Оборона Соединенных Штатов от кибератак должна стать первой целью кибервоенной стратегии. В конце концов, первостепенная задача любой стратегии национальной безопасности США — это защита страны. Мы не развиваем оружие, направленное на расширение нашего господства на воде, в космосе, киберпространстве, а стремимся сберечь страну. На первый взгляд концепция довольно проста, но она постоянно усложняется, поскольку есть те, кто верит, что лучшая защита — нападение, уничтожение противника до того, как он успеет причинить нам вред.

Когда генерал Роберт Элдер возглавлял Киберкомандование ВВС, он как-то сказал журналистам, что хоть его подразделение и отвечает за оборону, оно планирует выводить из строя компьютерные сети противника. «Мы хотим начать атаку и нокаутировать их в первом раунде», — заявил он. Его высказывание напомнило слова другого генерала ВВС, Куртиса Лемэя, который в 1950-х руководил стратегическим авиакомандованием ВВС и объяснял аналитикам корпорации RAND[[88]](#footnote-89)[[89]](#footnote-90), что Советы не смогут уничтожить бомбардировщики на земле, поскольку «мы будем атаковать первыми».

Оборонительная стратегия

193

Такие мысли опасны. Если у нас не будет надежной оборонной стратегии, нам придется вовлекаться в киберконфликты. Агрессивно захватывать системы противника, чтобы остановить атаку до того, как он успеет нанести удар по нашим незащищенным системам. Это будет дестабилизировать обстановку и заставит нас рассматривать потенциальных врагов как реальных. Кроме того, мы будем вынуждены занимать более жесткую позицию в попытках удержать противника от нападения на наши системы, запугивая военным ударом в ответ на кибератаку, а у наших оппонентов будет больше оснований думать, что мы блефуем.

Почему американские кибервоины полагают, что лучшая защита — нападение? Отчасти потому, что, по их ощущениям, защищать, обороняясь, очень сложно. Военные видят, насколько распределены находящиеся в киберпространстве потенциальные мишени, и у них опускаются руки при мысли об обороне. Кроме того, они указывают (это удобно), что американские вооруженные силы не имеют юридических полномочий защищать находящиеся в частном владении объекты — банки, энергодобывающие компании, железные дороги, авиапредприятия.

Такой же аргумент приводила администрация Буша после 11 сентября — слишком дорого оберегать страну от террористов, поэтому нам необходимо нанести удар по «первоисточнику». Из-за подобных суждений пришлось ввязаться в две войны за последние десять лет, которые обошлись нам в 2,4 триллиона долларов и стоили более пяти тысяч жизней американских солдат.

Не существует единой меры, которая позволила бы уберечь американское киберпространство. Однако мы можем предпринять ряд шагов, которые защитят наши ключевые объекты или, по меньшей мере, заронят зерна [[90]](#footnote-91)

Третья мировая война: какой она будет?

сомнения в умах возможных нападающих, что провести успешную масштабную атаку на Америку возможно.

Уберечь каждый компьютер в США от кибератаки нереально, но вполне возможно в достаточной мере защитить важнейшие сети — потенциальные мишени противника. Мы должны защитить их так, чтобы никакая атака не лишила нас возможности нанести ответный удар и не подорвала экономику. Даже если наша оборона несовершенна, укрепленные сети смогут выдержать натиск или достаточно быстро прийти в норму, так что атака не станет разрушительной. Если мы не можем защитить каждую важную систему, то что нам оборонять? Существует три ключевых элемента в американском киберпространстве, или, пользуясь терминологией из ядерной стратегии, триада, которую необходимо защищать.

□ боронитепьная триада

Стратегия оборонительной триады отличается от того, что делали Клинтон, Буш и теперь Обама. Клинтон в Национальном плане и Буш в Национальной стратегии полагали, что важнейшие инфраструктуры должны сами себя защищать от кибератаки. Были названы 18 инфраструктур, начиная от электроэнергетики и банковской системы и заканчивая продовольственным обеспечением и розничными продажами. Как уже отмечалось, все три президента, пытаясь сократить уязвимые места нашего киберпространства, «воздерживались от регулирования» и в итоге не многого добились. Буш в последний год своего восьмилетнего пребывания в должности президента одобрил подход, в котором в значительной степени игнориру-

Оборонительная стратегия

ются частные инфраструктуры. Он сконцентрировался на защите государственных систем и создании военного Киберкомандования. Обама реализовывает план Буша практически без изменений.

Федеральное регулирование — это главный инструмент обеспечения безопасности. Оно должно, по крайней мере на первоначальном этапе, сконцентрировать оборонительные усилия только на трех секторах.

Первое — это магистраль. Как отмечалось в третьей главе, существуют сотни интернет-провайдеров, но только пять крупнейших обеспечивают так называемую магистраль Интернета. В их число входят AT&T, Verizon, Level3, Qwestи Sprint, непосредственно связанные с большинством других интернет-провайдеров страны. Эти компании владеют магистралями, оптоволоконными кабелями, которые оплетают всю страну, проникают в каждый уголок и соединяются с проложенными по морскому дну кабелями, которые связывают Америку со всем остальным миром. Более 90 % интернет-трафика США проходит по этим магистралям, и попасть в любое место страны, минуя их, практически невозможно. Таким образом, если вы защищаете магистральных интернет-провайдеров, вы заботитесь обо всем остальном киберпространстве.

Чтобы атаковать частные и государственные сети, вы должны связаться с ними по Интернету, пройдя на определенном этапе и по магистрали. Вы можете перехватить атаку на входе в магистраль и остановить ее до того, как она попала в сеть. Если это в ваших силах, вам не придется беспокоиться о том, как обезопасить десятки тысяч потенциальных мишеней кибератаки. Представьте: вы знаете, что кто-то из Нью-Джерси собирается подогнать заминированный грузовик к какому-то зданию на Манхэттене. У вас есть выбор: обеспечить оборону каждого важного здания на острове (определив, какие считаются [[91]](#footnote-92)

Третья мировая война: какой она будет?

важными) или проверять все грузовики при въезде на любой из 14 мостов и в каждый из четырех туннелей, ведущих на остров.

Проверка всего интернет-трафика до его попадания в магистраль поднимает две важные проблемы — техническую и этическую. Техническая проблема заключается в следующем: трафика много, и никто не хочет, чтобы скорость передачи падала, пока вы ищете вредоносное ПО или атакующие программы. Есть и этическая проблема — никто не хочет, чтобы его электронную почту читали или отслеживали историю посещения веб-страниц.

Техническую проблему позволяют решить уже имеющиеся технологии. Кажется, что по мере увеличения скорости все сложнее сканировать трафик без задержки, если технологии сканирования недостаточно совершенны. Однако несколько компаний продемонстрировали возможность сочетать аппаратное и программное обеспечение, способное сканировать потоки данных в Интернете — маленькие пакеты из единиц и нулей, которые образуют электронные письма или веб-страницы. Сканирование проходит так быстро, что практически не задерживает перемещение пакетов по оптоволоконной линии. При этом проверяются не только строки «куда» и «откуда» (так называемые заголовки), но и данные, в которых может находиться вредоносное ПО. Таким образом, мы можем без задержки проводить глубокое инспектирование пакетов, и технический барьер уже преодолен.

Решить этическую проблему тоже реально. Мы не хотим, чтобы правительство и интернет-провайдеры читали наши письма. Систему глубокого инспектирования пакетов, предлагаемую здесь, можно полностью автоматизировать. Она будет искать не ключевые слова, а определенные паттерны, соответствующие вредоносным программам. Это поиск сигнатур. Если система обнаружит атаку, [[92]](#footnote-93)

Оборонительная стратегия

она может просто отправить пакеты в «черную дыру» киберпространства, уничтожить или послать на карантин для последующего анализа.

Чтобы американцы не опасались, что за ними будет шпионить «Большой брат», глубокое инспектирование пакетов должны проводить интернет-провайдеры, а не государство. Более того, необходим жесткий контроль со стороны Комитета по защите частных и гражданских свобод, дабы ни интернет-провайдеры, ни власти не могли незаконно шпионить за нами.

Идея глубокого инспектирования пакетов не создает риска того, что власти начнут следить за нами, — этот риск уже существует. Как мы видели на примере незаконного перехвата сообщений в администрации Буша, если сдерживание и противовес ослабевают, власти получают возможность проводить незаконную слежку за гражданами. Это беспокоит многих, и беспокойство нужно предотвратить с помощью механизмов реального контроля и жесткого наказания тех, кто преступил закон. Наша вера в право на неприкосновенность частной жизни и гражданские свободы вполне совместима с мерами, которые требуются для защиты нашего киберпространства. Вооружая полицию, мы увеличиваем вероятность того, что некоторые полицейские в редких случаях сумеют использовать оружие неправомерно, но мы понимаем, что нам нужна вооруженная полиция, которая защищает нас, и проводим серьезную работу для предотвращения неправомерных действий со стороны ее сотрудников. Точно так же мы можем установить системы глубокого инспектирования пакетов на магистралях крупнейших интернет-провайдеров, осознавая, что эти системы нужны для нашей же безопасности, и принимая меры против злоупотребления ими.

Как установить такие системы? Системы глубокого инспектирования пакетов должны располагаться там, где [[93]](#footnote-94)

Третья мировая война: какой она будет?

оптоволоконные кабели поднимаются со дна океана и оказываются на территории Соединенных Штатов, в точках пиринга, где магистральные интернет-провайдеры связываются друг с другом и с более мелкими сетями, и на других узлах магистральных интернет-провайдеров. Платить за эти системы, наверное, придется федеральным властям, возможно, Министерству национальной безопасности, даже если работой будут руководить интернет-провайдеры и компании, занимающиеся системной интеграцией. Поставщиками сигнатур вредоносного ПО (которые должны разыскивать «черные ящики»-сканеры) станут такие компании, как Symantecи McAfee, которые занимаются компьютерной безопасностью. Интернет-провайдеры и правительственные организации также могут предоставлять сигнатуры.

Системы контроля типа «черного ящика» должны быть связаны друг с другом в закрытую сеть, так называемую внеполосную систему связи (вне Интернета), чтобы их данные можно было быстро и надежно обновлять, даже если возникли какие-то затруднения в Интернете. Представьте, что в киберпространство попадает новая вредоносная программа, с которой никто еще не сталкивался. Этот мэлвер начинает атаковать сайты. Между тем система глубокого инспектирования пакетов связана с компаниями, занимающимися интернет-безопасностью, исследовательскими центрами и правительственными организациями, которые занимаются поиском атак «нулевого дня». В течение нескольких минут, пока вредоносная программа видна, ее сигнатура передается на сканеры, которые начинают ее блокировать и сдерживают атаку.

Предшественник подобной системы уже существует. Крупнейшие телекоммуникационные компании Verizonи AT&T могут на некоторых участках отслеживать сигнатуры, которые прежде только идентифицировали, но не [[94]](#footnote-95)

Оборонительная стратегия

стремятся перенаправлять вредоносный трафик в «черную дыру» (то есть уничтожать), поскольку клиенты, обслуживание которых при этом будет прервано, могут подать в суд. Пожалуй, провайдеры выиграли бы такую тяжбу, поскольку в соглашении об уровне сервиса с клиентами обычно говорится, что они имеют право отказать в обслуживании, если деятельность клиента незаконна или наносит вред сети. И тем не менее в силу обычной юридической осторожности компании делают для защиты киберпространства меньше, чем могли бы. Вероятно, необходимы новые законы и регламенты для прояснения этого сложного вопроса.

Система «Эйнштейн» Министерства национальной безопасности, которую мы обсуждали в четвертой главе, установлена на некоторых участках сети, где правительственные учреждения соединяются с магистральными интернет-провайдерами. «Эйнштейн» контролирует только правительственные сети. У Министерства обороны имеется аналогичная система, использующаяся в 16 точках, где несекретная внутренняя сеть МО связана с общедоступным Интернетом.

Более совершенная система, с более высоким быстродействием, большей памятью, обрабатывающей способностью и с возможностью внеполосного соединения, может помочь минимизировать или пресечь масштабную кибератаку, если такую систему установить для защиты не только правительства, но и всей магистрали, от которой зависят все сети.

Защитив таким образом магистраль, мы сможем остановить большинство атак, направленных на системы гос- управления и частного сектора. Независимая Федеральная комиссия по связи обладает полномочиями вводить правила, обязывающие магистральных интернет-провайдеров устанавливать такую систему защиты. Затра-

1 *ээ*

Третья мировая война: какой она будет?

ты крупные интернет-провайдеры могут переложить на пользователей и провайдеров меньшего масштаба, с которыми они сотрудничают. Или же конгресс должен выделить фонды для полного или частичного покрытия расходов. Пока власти только начинают двигаться в этом направлении, и то лишь для того, чтобы защитить себя, а не сети частного сектора, от которых зависит наша экономика, правительство и национальная безопасность.

От интернет-провайдеров следует потребовать, чтобы они прилагали большие усилия для сохранения чистоты кибернетической экосистемы. Эд Аморосо, глава безопасности компании AT&T, рассказывал мне, что их центр безопасности видит, когда компьютеры клиентов становятся частью ботнета, рассылающего DDoS-атаки и спам. Они знают, какие абоненты заражены, но не осмеливаются информировать их (а тем более отрубать доступ) из опасения, что пользователи перейдут к другому провайдеру или попытаются преследовать их в судебном порядке за вмешательство в личную жизнь. Это уравнение нужно перевернуть с головы на ноги. Интернет-провайдеров необходимо обязать информировать клиентов сети, когда те становятся частью ботнета. Интернет-провайдеры должны отключать доступ, если клиенты не реагируют на подобные предупреждения. От них следует потребовать предоставления бесплатных антивирусных программ для абонентов, как многие уже делают, чтобы повысить пропускную способность сети. Абонентов, в свою очередь, надо обязать использовать антивирусное ПО (предоставленное провайдером или любое другое на их выбор). Мы ведь не позволяем производителям автомобилей выпускать машины без ремней безопасности. Такая же логика нужна и с Интернетом, поскольку пренебрежение компьютерной безопасностью затрагивает проблему национальной безопасности.

 2ПП

Оборонительная стратегия

Помимо глубокого инспектирования всех пакетов трафика с целью обнаружения вредоносного ПО и блокирования пакетов, которые запускали распознанные атаки, следует предпринять ряд дополнительных шагов для укрепления системы. Во-первых, затратив относительно немного времени и денег, можно разработать программное обеспечение для идентификации трансформированного мэлвера. Это позволит обнаруживать вариации известных сигнатур, которые могут использовать хакеры, чтобы проскочить глубокое инспектирование пакетов. Во- вторых, помимо магистральных интернет-провайдеров к поиску вредоносного ПО должны подключиться власти и крупные коммерческие структуры (например, банки), также заключив соглашения с центрами обработки и размещения данных. В нескольких крупных хостинговых центрах обработки данных, разбросанных по всей стране, сходятся оптоволоконные кабели крупнейших интернет- провайдеров и осуществляется коммутация. Здесь же находятся серверы некоторых крупных организаций, стоящие блестящими мерцающими рядами за ограждениями или скрытые в строго охраняемых помещениях. Операторы этих центров могут выявлять известное вредоносное ПО — это будет второй уровень защиты. Более того, операторы центров обработки данных или сотрудники фирм по обеспечению компьютерной безопасности могут просматривать данные. Центры имеют возможность предоставлять регулируемые услуги по обеспечению безопасности и отслеживать аномальную активность, причиной которой иногда являются необнаруженные вредоносные программы. В отличие от попыток блокировать мэлвер на входе регулируемые услуги позволяют отслеживать подозрительное поведение и аномальную активность пакетов данных. Тем самым увеличивается вероятность обнаружения более сложных двухэтапных атак и программ

 2D1

Третья мировая война: какой она будет?

«нулевого дня». Эти вредоносные программы можно добавлять в список программ для блокировки. Поиски разумно проводить по тем адресам базы данных, куда проник новый мэлвер, тем самым позволяя системе останавливать крупномасштабную эксфильтрацию данных.

Платя интернет-провайдерам и поставщикам услуг по обеспечению безопасности за проверку данных, власти будут удалены от процесса, чтобы гарантировать прайвеси и поощрять конкурентную борьбу. Помимо оплаты власти должны предоставлять информацию о вредоносном ПО, мотивировать компании обнаруживать атаки, создать механизм, позволяющий гражданам быть уверенными, что их частная информация и гражданские свободы надежно защищены. В отличие от единственной линии защиты, применяемой властями (например, системы «Эйнштейн», созданной Министерством национальной безопасности для защиты гражданских федеральных ведомств), это будет многоуровневая система, работу которой обеспечивают несколько провайдеров, что гарантирует инновации и здоровую конкуренцию среди IT-компаний частного сектора. Если правительству станет известно о надвигающейся или начатой кибервойне, ряд федеральных сетевых операционных центров сможет взаимодействовать с частными IT-защитниками и сетевыми операционными центрами ключевых частных организаций и координировать оборону. Для этого властям придется создать специальную коммуникационную сеть, объединяющую сетевые операционные центры, — строго охраняемую, полностью изолированную и отделенную от Интернета (тот факт, что такая новая сеть понадобится, кое-что говорит об Интернете).

Второй элемент оборонительной триады — безопасность электросетей. Спросите себя, как электрораспределительная сеть может быть связана с киберпростран- 202

□ боронитепьная стратегия

ством, — так проще всего понять эту идею. Без электричества многие вещи, от которых мы зависим, не работают вообще или работают недолго. Самое простое, что может сделать хакер, чтобы нанести серьезный удар по Соединенным Штатам, — отключить западную или восточную электросети, которые обеспечивают электроэнергией США и Канаду (в Техасе есть собственная сеть). Дублирующие энергетические системы территориально ограничены и печально знамениты тем, что не включаются, когда больше всего нужны. (Так произошло у меня дома буквально вчера, когда молния ударила по местной электростанции и свет в нашем городке отключился. Мой автоматический пусковой генератор просто не сработал.) Можно ли защитить крупнейшие североамериканские системы, состоящие из сотен компаний по производству и транспортировке электроэнергии?

Да, но не без дополнительного федерального регулирования. Первостепенной задачей такого регулирования должно стать .отсоединение управляющей сети энергетических компаний от Интернета, а затем введение обязательной аутентификации для доступа в сеть. Это было бы не так дорого, но попробуйте предложить такую идею компаниям-производителям электроэнергии. Если их спросить, какие активы наиболее важны и требуют особых мер кибербезопасности, они ответят, что 95 % их ресурсов не требуют никакого регулирования. Один специалист по кибербезопасности, сотрудничающий с крупнейшими аудиторскими компаниями, рассказал, что задавал руководству каждой из них один и тот же вопрос: «Могли ли вы во время работы с электроэнергетическими компаниями получить доступ к элементам управления электрораспределительной сети через Интернет?» Все шесть компаний ответили утвердительно. Как много времени на это потребовалось? Не более часа. За этот

203

Третья мировая война: какой она будет?

час они успевали взломать веб-сайт компании, проникнуть в закрытую корпоративную сеть, а затем добраться до систем управления. Некоторые аудиторские фирмы сокращают это время, проникая в телефонную сеть, работающую по интернет-протоколам (телефония на базе IP). Телефоны такой сети обычно связаны с Интернетом. Если они располагаются в диспетчерских, то наверняка связаны и с сетью, которая управляет энергетической системой. Удобно, правда? Более того, кое-где команды компонентам электросети посылаются в незашифрованном виде по радиоканалу. Просто сядьте неподалеку, настройтесь на ту же частоту, и, если ваш сигнал сильнее, отдавайте команды (правда, нужно знать, какое для этого используется программное обеспечение). Федеральная комиссия по управлению энергетикой (FERC) грозилась, что с 2010 года начнет наказывать энергетические компании, киберсистемы которых небезопасны. Но только никто не сказал, как комиссия будет вычислять нарушителей, ведь в FERCнет персонала, способного проводить регулярные инспекции. Однако Министерство энергетики США наняло двух экспертов по кибербезопасности, чтобы те определили, достаточно ли защищены 3,4 миллиарда долларов, выделенные на программу «Умная сеть». «Умная сеть» — идея администрации Обамы сделать электросеть более интегрированной и оцифрованной. Электроэнергетические компании могут претендовать на часть этих денег, если согласны с предложениями Министерства энергетики. В этих предложениях в том числе есть раздел, посвященный кибербезопасности. Однако Министерство энергетики отказывается сообщать, о чем идет речь в этом разделе и кто эти эксперты. Общедоступных стандартов не существует. Если бы они были, налогоплательщики вряд ли согласились бы дать какую- либо часть этих 3,4 миллиона компаниям, не обеспечива-

 204

Оборонительная стратегия

ющим безопасность своих систем. Но не ждите, что Министерство энергетики введет такие стандарты, ведь это бы означало воспользоваться этой уникальной федеральной подарочной программой и мотивировать людей работать над безопасностью. Такой намек на регулирование очень напоминает социализм, а это не по-американски. Итак, скоро у нас будет еще более «умная» сеть... и еще менее защищенная. Но как же сделать ее умной и защищенной?

Первым шагом в этом направлении могло бы стать принятие и введение серьезных регламентов для энергетических компаний, согласно которым неавторизирован- ный доступ к сети управления энергосистемой стал бы практически невозможен. Для этого необходимо закрыть все входы в систему управления через Интернет. Кроме того, в точки, где системы управления соединяются с внутренней сетью энергетических компаний, необходимо установить модули глубокого инспектирования пакетов, которые я предлагал разместить на интернет-магистралях. Затем, чтобы еще больше усложнить задачу хакерам, можно потребовать, чтобы командные сигналы, которые поступают на генераторы, трансформаторы и другие ключевые компоненты энергосистемы, были зашифрованы и аутентифицированы. Шифровка сигналов означает, что даже если кто-то проникнет в сеть и попытается дать какую-либо инструкцию генератору, без секретного кода у него ничего не получится. Аутентификация команд подразумевает, что генератор или трансформатор проверяет сигнал с помощью процедуры установления подлинности с целью убедиться в том, что полученный сигнал исходит из надежного источника. Кроме того, на случай захвата части сети в ключевых секциях должна существовать система вспомогательной связи для отправления командных сигналов — это даст возможность при необходимости восстановить питание.

*205*

Третья мировая война: какой она будет?

Многие недооценивают опасность атаки на энергосистему. Как сказал мне один чиновник, «отключение электричества происходит часто, но через несколько часов все восстанавливается». Однако так может быть не всегда. Электроснабжение восстанавливается через несколько часов, если оно отключилось вследствие грозы. Но если блэкаут — результат умышленных действий, он может продлиться намного дольше. Согласно так называемому сценарию многократного противостояния, кибератаки разрушают энергосистему, и она выходит из строя на месяцы. Если кто-нибудь разрушит генераторы, как во время проведения учений, для их замены потребуется полгода, поскольку каждый генератор производится по специальному проекту. А если атака произойдет в нескольких направлениях одновременно, а затем повторится после перехода на резервное энергоснабжение, наша экономика может разрушиться, поскольку прекратится поставка продуктов питания и других потребительских товаров, выйдут из строя фабрики, а финансовые рынки вынуждены будут закрыться.

Действительно ли нам необходимо усовершенствованное регулирование? Должны ли энергетические компании больше тратить на защиту своих сетей? Реальна ли эта потребность? Давайте спросим главу американского киберкомандования, генерала Кейта Александера, чьи кибервоины способны разрушить энергосистему любой страны. Считает ли он, зная, какой урон можем нанести мы, что нам нужно лучше защищать собственные электросети? Именно об этом его спросили в 2009 году на заседании Конгресса. Он ответил: «Энергетическим компаниям придется изменить конфигурацию своих сетей... Модернизировать сети, чтобы обеспечить их безопасность. Для этого потребуются немалые средства... А нам нужно поработать с их управляющими комитетами, договориться о повышении

206

Оборонительная стратегия

тарифов, чтобы они смогли действительно обезопасить сети... Как правительство, заинтересованное том, чтобы наши электросети были надежными, может убедиться bтом, что эта надежность обеспечивается?» Немного сумбурно, но генерал Александер, очевидно, имел в виду, что энергетические компании должны принять меры, чтобы наши электросети были безопасными и надежными, а для этого, возможно, потребуются немалые затраты, и в осуществлении этих планов им помогут регулирующие организации. Он прав.

Третьим элементом оборонительной триады является само Министерство обороны. Маловероятно, что противник в рамках крупномасштабной кибератаки не попытается подорвать работу этого министерства. Почему? Если противник нападет на Соединенные Штаты, разрушая частный сектор — энергосистему, трубопроводы, транспортную сеть и банковскую систему, вряд ли это начнется как гром среди ясного неба. Такая кибератака может произойти только в случае обострения отношений между США и атакующей страной. В такой ситуации противник будет опасаться, что вооруженные силы США перейдут к традиционным наступательным военным действиям. Более того, планируя крупную кибератаку, противник должен понимать, что США нанесет ответный военный удар. А кибератака на вооруженные силы США наверняка будет сконцентрирована на сетях Министерства обороны.

Упростим ситуацию. Предположим, что существует три главные сети Министерства обороны. Первая, NIPR- NET, — это несекретная внутренняя сеть, с адресами .mil. NIPRNETсвязана с Интернетом в 16 узлах. По NIPRNETпередаются несекретные данные, но несекретные не значит неважные. Большая часть информации по материально-техническому обеспечению (допустим, едой) циркулирует именно в NIPRNET. Большинство военных подраз-

 207

Третья мировая война: какой она будет?

делений США не смогут продержаться без поддержки частных компаний, и почти все коммуникации происходят в NIPRNET.

Вторая сеть называется SIPRNETи используется для передачи секретной информации. Многие военные приказы рассылаются по SIPRNET. Считается, что существует определенный «зазор» между секретной и несекретной сетями. Пользователи засекреченной сети скачивают данные из Интернета и загружают их в SIPRNET, а вместе с ними сюда могут проникать вредоносные программы. Специалисты по информационной безопасности Пентагона называют это проблемой «доставки ножками».

В ноябре 2008 года шпионская программа российского происхождения начала отыскивать в киберпространстве адреса .milоткрытой сети NIPRNET. Когда программа проникла в компьютеры NIPRNET, она начала искать внешние накопители и загружаться на них. Затем началась «доставка ножками». Некоторые из накопителей пользователи вставили в компьютеры засекреченной сети SIPRNET. Что было дальше, можете представить. Поскольку не подразумевается, что засекреченная сеть может связываться с Интернетом, в ней не предполагается наличие вирусов. Поэтому на большинстве компьютеров этой сети не были установлены ни антивирусная защита, ни брандмауэры, ни любые подобные программные средства защиты данных. Короче говоря, компьютеры самой важной сети Министерства обороны защищены меньше, чем, возможно, ваш домашний компьютер.

За несколько часов шпионская программа заразила тысячи засекреченных компьютеров вооруженных сил США в Афганистане, Ираке, Катаре и прочих местах, где базируются подразделения Объединенного центрального командования. Спустя несколько часов высокопоставленный американский офицер адмирал Майк Маллен, пред- 208

Оборонительная стратегия

седатель Объединенного комитета начальников штабов, понял, как уязвимы его войска. По рассказу одного высокопоставленного источника в Пентагоне, Маллен, услышав Доклад специалистов, закричал: «Вы хотите мне сказать, что я не могу полагаться на нашу рабочую сеть?» Сетевые эксперты из Объединенного штаба подтвердили вывод адмирала. Они не были удивлены. А разве адмирал об этом раньше не знал? Шокированный невероятной слабостью, которую майоры и капитаны воспринимали как должное, но скрывали от него, Маллен перевел взгляд на старшего офицера. «Где Джей-3? — спросил он, требуя начальника по военным операциям. — Он об этом знает?» Вскоре Маллен и его начальник, министр обороны Роберт Гейтс, докладывали о своем открытии президенту Бушу. Вероятно, SIPRNETвзломали. Сетецентричное преимущество, которым так гордились американские вооруженные силы, может оказаться ахиллесовой пятой. Пожалуй, Маллену не стоило так удивляться. По всему миру расположено около 100 тысяч терминалов SIPRNET. Если у вас получится остаться с одним из них наедине всего на несколько минут, вы сумеете загрузить туда вредоносное ПО или установить связь с Интернетом. Один мой друг рассказывал, что до одного терминала SIPRNETна Балканах могли спокойно добираться российские «миротворцы», оставаясь незамеченными. Точно как во время Второй мировой войны, когда союзникам нужен был только один экземпляр германской кодирующей машины «Энигма», чтобы прочитать все шифровки нацистов, так и сейчас достаточно одного терминала SIPRNET, чтобы установить программу, которая нарушит работу всей сети. Несколько специалистов, занимающихся проблемами безопасности SIPRNET, подтвердили мой вывод. Как сказал один из них, «приходится допускать, что она может не работать, когда нам это необходимо». Он объяснил, что, если во вре- [[95]](#footnote-96)

Третья мировая война: какой она будет?

мя кризиса противник выведет из строя эту сеть или, что еще хуже, отдаст фальшивые приказы, «американские вооруженные силы окажутся в очень невыгодном положении». И это мягко сказано.

Третья сеть Министерства обороны — это совершенно секретная режимная сеть JWICS. Эта более закрытая сеть служит для обмена сверхсекретной информацией. Ее терминалы располагаются в специальных секретных режимных помещениях. Доступ к ним еще более ограничен, но информация, передающаяся по сети, должна пройти по оптоволоконным кабелям, через маршрутизаторы и серверы, как и в любой другой сети. Кто-нибудь может атаковать маршрутизаторы, и связь нарушится. Аппаратное обеспечение, используемое в компьютерах, серверах, маршрутизаторах, коммутаторах, может быть взломано на этапе производства или позднее. Поэтому нельзя сказать, что эта сеть безопасна.

Согласно плану CNCI, Министерство обороны приступает к реализации программы по модернизации систем безопасности всех трех типов сетей. Некоторые аспекты этой программы секретны, многие дорогостоящи, на осуществление иных потребуется много времени. Один из вариантов — использование лазеров с высокой пропускной способностью для передачи сообщений через спутники. Если допустить, что спутники защищены от взлома, такая система способна уменьшить количество уязвимых мест, которые имеются в оптоволоконных кабелях и маршрутизаторах, разбросанных по всему миру. Однако есть несколько важных и не столь разорительных для бюджета конструктивных принципов использования доступных технологий, которые следовало бы включить в программу Министерства обороны:

О помимо защиты самой сети, нужно защищать конечные точки; устанавливать брандмауэры, анти- [[96]](#footnote-97)

Оборонительная стратегия

вирусные программы и программы предотвращения вторжений на все компьютеры сетей Министерства обороны, независимо от того, связаны они с Интернетом или нет;

Qтребовать от пользователей всех сетей Министерства обороны подтверждать свою личность при регистрации в сети как минимум по двум признакам аутентификации;

® сегментировать сети в подсети и установить для пользователей, желающих выйти за пределы своей подсети, ограниченный «принцип необходимого знания»1;

Sне ограничиваться существующей практикой группового шифрования, согласно которой шифруется весь трафик, идущий по магистральному оптоволоконному кабелю, и шифровать все файлы на компьютерах, включая информацию, находящуюся на серверах хранения данных;

<Э отслеживать все сети на предмет новых несанкционированных соединений, автоматически отключая неизвестные устройства.

Даже если сети Минобороны защищены, всегда есть риск того, что программные и/или аппаратные средства, обеспечивающие работу систем вооружения, могут быть взломаны. Мы знаем, что проектная документация [[97]](#footnote-98)[[98]](#footnote-99)

Третья мировая война: какой она будет?

нового истребителя F-35 была выкрадена в результате взлома сети военного подрядчика. А что, если хакер дополнил проекты невидимой программой, которая при поступлении определенной команды, переданной с любого истребителя противника, вызовет сбой в системе, когда самолет будет находиться в воздухе? Подобные логические бомбы могут быть спрятаны среди миллионов строк кода F-35, в любой из множества встроенных программ или в компьютерной аппаратуре истребителя. Как сказал мне один пилот: «Современный самолет, будь то „F-22 раптор" или „боинг 787“, — это просто набор программ, который, как ни странно, летает по воздуху. Напутайте что-нибудь в этих программам, и он перестанет летать». Я считаю, что аэробус AirFrance,который потерпел крушение в Южной Атлантике, разбился потому, что его компьютер принял неверное решение.

Компьютерные микросхемы, которые используются в американском вооружении, так же как и некоторые компьютеры или компоненты, производятся в других странах. Самая вездесущая операционная система в Министерстве обороны — MicrosoftWindows— разрабатывается по всему миру и славится своей уязвимостью. Проблемы с каналами поставок не так-то легко и быстро разрешить. Этой сфере в том числе уделялось особое внимание в плане Буша 2008 года. Сейчас в США строятся новые предприятия по производству микросхем. Некоторые компании частного сектора создают программы, проверяющие другие программы на наличие багов. Помимо срочного укрепления безопасности сетей Пентагон должен также разработать специальную программу по стандартизации, контролю и исследованию, чтобы гарантировать, что программное и аппаратное обеспечение, используемое в ключевых системах вооружения, командном управлении и логистике, не имеет лазеек и логических бомб. [[99]](#footnote-100)

Оборонительная стратегия

В этом и заключается стратегия оборонительной триады. Если бы администрация Обамы и конгресс согласились укрепить интернет-магистраль, разделить и обезопасить контроль над энергосистемой и добиться повышения безопасности IT-систем Министерства обороны, мы заставили бы потенциальных нападающих засомневаться в том, насколько успешной может оказаться их масштабная кибератака против нас. И даже если бы они решились на атаку, оборонительная триада смягчила бы ее последствия. На данном этапе сложно сказать, какие затраты потребуются на эти программы, но сам процесс их реализации займет около пяти лет. И на протяжении этого срока мы сумеем извлечь пользу, поскольку противникам все сложнее будет осмелиться развязать кибервойну против нас. До тех пор, пока мы не начнем осуществлять этот план или какую-либо другую подобную стратегию, охватывающую и частный сектор, кибервойна для США будет нежелательным развитием событий.

Если мы примем оборонительную триаду, то получим возможность делать заявления, которые помогут нам сдерживать противников от попыток кибератак. Иногда обычные слова, которые не стоят денег, могут обеспечить безопасность, если они обоснованы. Вершина триады — декларируемая стратегия, объявляемая тем странам, которые раздумывают о вторжении в наше киберпространство. Декларируемая стратегия — это официальное объявление стратегии и планов властей. Сейчас у нас нет официальной стратегии, объявляющей, как мы намерены реагировать на кибератаку и относиться к ней. Наши противники могут счесть, что реакция США на кибератаку будет минимальной или непрогнозируемой.

Мы не хотим оказаться в ситуации, в которую попал Джон Кеннеди после того, как обнаружил, что на Кубе размещены ядерные ракеты. Он заявлял, что любая такая

Z1 3

Третья мировая война: какой она будет?

ракета, направленная с Кубы кем бы то ни было (СССР или Кубой) на «любую страну в этом полушарии, будет рассматриваться как нападение Советского Союза на Соединенные Штаты и потребует от нас полномасштабного реагирования». Эти слова пугали, когда я услышал их в 20 лет, пугают они и сейчас. Если бы США заявили об этом до того, как ракеты были дислоцированы на Кубе, Кремль, возможно, их бы там и не стал размещать.

Публичное заявление о наших действиях в случае кибератаки тем не менее не должно ограничивать будущие решения. В словах должна быть некоторая «конструктивная неопределенность». Если кибератака произойдет, мы не будем наверняка знать, кто ее инициировал, и этот факт необходимо учитывать в декларируемой стратегии. Представьте, что Барак Обама обращается к выпускному классу одной из четырех американских военных академий. Он обводит взглядом новоиспеченных офицеров и их родителей, а затем говорит: «Позвольте мне обратиться к любой стране, которая задумывает использовать против нас кибероружие. Соединенные Штаты к любой кибератаке, которая разрушит или нанесет урон нашим вооруженным силам, нашему правительству, нашим важнейшим инфраструктурам, отнесется так же, как к наступательной, направленной на те же цели и имеющей такие же последствия. Мы будем считать это враждебным актом на нашей территории. В ответ на подобную агрессию в нашем киберпространстве я, как главнокомандующий, облачу страну в доспехи могущества и не стану ограничивать нас в масштабах и видах ответных действий». Доспехи могущества — выражение из президентского лексикона. Оно означает, что он может пустить в ход дипломатическое, экономическое, кибернетическое или наступательное оружие (которое будет соответствовать ситуации), принимая во внимание атакованный объект и последствия. [[100]](#footnote-101)

Оборонительная стратегия

Специалисты по международному праву будут спорить о словах «не стану ограничивать», замечая, что ответные действия, согласно международному законодательству, должны быть соизмеримыми с атакой.

Однако заявление о том, что отклик может быть несоизмерим, — это дополнительное средство устрашения. В ядерной стратегии эта идея — мобилизация всех сил в ответ на атаку меньшего масштаба, а затем предложение прекратить военные действия — называлась эскалацией превосходства. Она посылает сигнал, что вы не желаете вовлекаться в затяжной вялотекущий конфликт. Президент должен иметь такую альтернативу независимо от того, воспользуется он ею или нет.

А что, если (скорее всего, так и будет), возникнет проблема атрибуции и противник спрячется за «юбками» гражданских «хактивистов» или станет утверждать, что атака просто транзитом прошла через его страну, а не началась в ней? Предвидя такое заявление, Обама делает паузу в выступлении, а затем добавляет: «Нас не введут в заблуждение утверждения, что атака была делом рук гражданских „хактивистов" и ее источник установить нелегко. Мы способны определить авторство. Более того, мы сохраняем за собой право рассматривать отказ своевременно прекратить атаку, исходящую из страны, как подтверждение того, что правительство этой страны участвует в атаке. Мы также будем считать отсутствие серьезного сотрудничества в расследовании атак равноценным участию в атаке».

Доктрина Обамы должна быть доктриной киберравнозначности, согласно которой кибератаки будут оценивать по их последствиям, а не средствам. Они будут приравниваться к наступательным действиям и, возможно, повлекут за собой ответные действия — наступательные или другие. Вывод заключается в том, что государства не-

Третья мировая война: какой она вудет?

сут национальную ответственность за киберпространство и обязаны оказывать помощь, то есть в их задачи входит задача предотвращать враждебные действия, исходящие с расположенных в их стране серверов, выслеживать, изолировать и привлекать к судебной ответственности тех, кто использует их киберпространство для разрушения и повреждения систем других стран. Америка тоже будет связана этими обязательствами, и ей придется отключать ботнеты, атакующие, допустим, Грузию из Бруклина. Если бы магистральные интернет-провайдеры сканировали свои сети, обязанность содействовия было бы очень легко исполнять.

Исходя из этой доктрины, Соединенные Штаты должны будут заявить о том, что любую кибератаку, приведшую к разрушению или нарушению деятельности систем, мы не будем считать более допустимой по сравнению с наступательными боевыми действиями просто потому, что она не сопровождалась ослепительными взрывами и горами трупов. Если президент примет какую-либо программу, подобную оборонительной триаде, у США появится надежная кибероборонная стратегия.

Итак, когда мы выработаем разумную концепцию обороны, сможем ли мы тогда перейти в нападение, используя новых кибервоинов для достижения военного превосходства в киберпространстве во славу Соединенных Штатов Америки?

ГПABA6

Как наступать?

В

 фильме 1983 года о компьютерах и войне <<Военные игры» с Мэтью Бродериком в главной роли компьютерный голос задает вопрос: «Желаете поиграть в термоядерную войну?» Почему бы и нам не поиграть? Попробуем провести кибервоенные учения, чтобы разъяснить некоторые моменты. Министерство обороны ежегодно проводит подобные мероприятия, которые получили название «Кибершторм». Аналогичные учения ЦРУ, «Без- [[101]](#footnote-102)

Третья мировая война: какой она будет?

молвный горизонт», проходят регулярно с 2007 года. В целях исследования я обращусь к вам с той же просьбой, что и к своим студентам из Школы государственного управления Кеннеди Гарвардского университета и чиновникам госбезопасности, которые собираются за одним столом в оперативном штабе Белого дома: «Придерживайтесь сценария». То есть не тратьте время на рассуждения о том, что однажды в силу неких обстоятельств США окажутся на грани конфликта с Россией или Китаем. Когда американские кибервоины говорят о bigone, они подразумевают конфликт в киберпространстве с Россией или Китаем — странами, которые наряду с Соединенными Штатами обладают самым мощным наступательным потенциалом. Никто не хочет войны с такими противниками. Но, рассматривая данный вариант развития событий, чтобы разобраться, какой может быть кибервойна, мы делаем ее более вероятной. По существу, соглашаясь с рисками кибервойны, мы имеем шансы снизить вероятность ее начала. А если вопреки нашим надеждам кибервойны не удастся избежать, лучше заранее обдумать, как она может разворачиваться.

До 11 сентября я, безусловно, не хотел таких «перспектив», но немало поиграл в настольные войны — проработал ряд возможных сценариев, чтобы подготовить себя и чиновников к подобным событиям. Когда день X настал, мы уже знали, как реагировать на атаку и действовать. Мы не только прилагали невероятные усилия для предотвращения атак, но и продумывали, как действовать, если какая-нибудь из них все же начнется. Не поступи мы так, тот кошмарный день был бы еще страшнее. Так что давайте на время представим, что отношения между США и Китаем обострились. Назовем эти учения «Южно-Китайское море» и переместимся на несколько лет в будущее.

 2 1 В

Как наступать?

Почти ничего не изменилось, только в Китае возросла зависимость от Интернета. В свою очередь Соединенные Штаты не слишком много сделали для улучшения собственной киберобороны. В игре примут участие три команды — Киберкомандование США, Кибердивизия Народно-освободительной армии Китая и Наблюдатели, то есть все остальные. Наблюдатели, помимо прочего, решают, что может произойти в результате действий двух команд. Давайте для чистоты эксперимента предположим, что Китай надавил на Вьетнам и другие страны АСЕАН (Ассоциации государств Юго-Восточной Азии), чтобы те уступили свои права на обширные подводные газовые и нефтяные месторождения. (Китай на самом деле уже заявлял о своих правах на эти территории, простирающиеся на сотни километров на юг, вдоль побережья Вьетнама и Филиппин.) Условимся, что небольшие столкновения военно-морских сил этих стран уже происходили. Представим, что Вьетнам попросил США о военной поддержке (вот уж исторический анекдот), как сделали другие страны в регионе, претендующие на оспариваемые территории. В свою очередь президент Соединенных Штатов санкционировал совместные морские учения США и АСЕАН и отправил две группы авианосцев из 20 кораблей и 150 самолетов и несколько подводных лодок. Китай и США обменялись дипломатическими нотами и публичными заявлениями, и каждая страна заявила, что другой лучше воздержаться от вмешательства. Канал CNNначал передавать новости под заголовком «Кризис в Южно-Китайском море».

Наши гипотетические учения начинаются в Форт- Мид, где команда Киберкомандования США получает приказ продумать шаги, которые предпримет в случае обострения политической ситуации. Согласно приказу министра обороны необходимо:

Третья мировая война: какой она будет?

1. Убедить китайское правительство отказаться от военных действий в оспариваемых водах.
2. Если переговоры не увенчаются успехом, максимально снизить опасность, исходящую от китайских военных, для американских и союзнических сил в регионе.
3. В случае, если напряжение усилится или противник внезапно начнет боевые действия, быть готовыми нанести удар по войскам Китая, чтобы уменьшить его возможности применения силы.
4. Подорвать внутреннюю инфраструктуру Китая так, чтобы переключить внимание китайского руководства на эту проблему и подвергнуть сомнению необходимость агрессивного поведения за пределами страны.
5. На протяжении всей операции Киберкомандование США должно сотрудничать с соответствующими правительственными ведомствами, чтобы предотвратить кибератаку китайского правительства или граждан на важнейшие военные и гражданские инфраструктуры США.

В такой ситуации перед командой, выступающей в роли Киберкомандования, возникает дилемма. Они не хотят демонстрировать все доступные им приемы кибератаки. Как только тот или иной прием используется, специалисты по киберобороне могут найти решение, позволяющее заблокировать такую атаку в будущем. Хотя защитники и не в состоянии подготовить все системы, которые могут подвергнуться атаке, они подлатают важнейшие, и нападение лишится немалой части своего потенциала.

 2ZQ

Как наступать?

Поэтому Киберкомандование предпочтет воздержаться от самых интеллектуальных методов. Пока они ждут, китайцы могут предпринять меры, которые существенно осложнят Соединенным Штатам проведение кибератак.

По мере усиления напряженности Китай сократит поток информационных пакетов в страну, а прошедшие будет сканировать и фильтровать на предмет обнаружения возможных угроз со стороны США. Затем, возможно, вообще оборвет связь с внешним миром. Если США к тому времени не запустят кибератаку, пробиваться через великий китайский брандмауэр GreatFirewallбудет гораздо сложнее.

Киберкомандование должно заранее создать туннели в киберпространстве Китая, например, спрятав спутниковые телефоны на территории страны, чтобы через них начать атаку на китайский Интернет. Или же совместно с ЦРУ распределить по всему Китаю агентов с ноутбуками, на которых установлено атакующее программное обеспечение.

Если США будут тянуть с использованием своего лучшего оружия, Китай может осложнить задачу, нарушив работу или разрушив наше киберпространство и интернет-магистраль. Переустановка серверов высшего эшелона в системе имен домена, занимающихся предоставлением интернет-адресов веб-сайтам или таблицами маршрутизации (протоколами пограничных шлюзов) провайдеров первого яруса, разрушит киберпространство на долгие дни. В результате поток информации будет попадать по неправильным интернет-адресам. Как я уже отмечал в третьей главе, мало что может помешать такому развитию событий, поскольку программы, управляющие работой Интернета, не проверяют, подлинна ли та или иная команда. Если китайцы смогут заслать своих агентов в «ящики», где расположены соединения интернет- 221

Третья мировая война: какой она будет?

провайдеров первого яруса, так называемые пиринговые точки, или на любые другие участки крупнейших сетей, они смогут отдавать команды непосредственно маршрутизаторам, которые коммутируют и направляют интернет-трафик. Даже несмотря на то что у Министерства обороны и разведывательных органов США есть собственные каналы, отделенные от общедоступного Интернета, их трафик, скорее всего, идет по тем же оптоволоконным магистралям. Просто их кабель покрашен в другой «цвет» либо идет по отдельному стекловолокну, но находящемуся в той же магистрали. Очень вероятно, что есть много участков, где трафик Министерства обороны и разведки проходит через те же самые маршрутизаторы, что и трафик общедоступного Интернета. Китай должен быть хорошо знаком с этими маршрутизаторами. Большая их часть произведена фирмой Ciscoна территории Китая. Так что у Китая есть все возможности отключиться от Интернета и лишить Соединенные Штаты шанса нанести киберудар. Это означает, что на ранних этапах кризиса у Киберкомандования есть повод провести военные действия в киберпространстве за пределами США. Разумеется, это расширит масштабы кибервойны.

Чтобы начать операцию, группа Киберкомандования решит послать сигнал о своем участии, в надежде удержать Китай от дальнейших военных операций. Причастность Киберкомандования к последующим действиям будет отрицаться публично, но китайские власти должны понимать, что это вовсе не случайность. Сигнал, демонстрирующий, что США способны на технически сложные операции, должен быть достаточно явным для китайского руководства, но не настолько разрушительным, чтобы привести к полномасштабной кибервойне. Итак, взломав закрытую китайскую военную сеть, Киберкомандование рассылает старшим офицерам обработанную в фотошо-

 zzz

Как наступать?

пе фотографию горящего китайского авианосца. Это не слишком прозрачный намек на то, что гордость китайского флота, его единственный авианосец, ВМС США могут отправить на дно, поэтому китайцам стоит подумать и не развязывать конфликт, который может привести к таким последствиям.

Затем американская разведка узнает, что китайцы готовы высадить десант на оспариваемые острова в Южно- Китайском море. Пентагон просит Киберкомандование выиграть время и отсрочить операцию, помешав погрузке войск и провианта на корабли, которые все еще находятся в порту. Штаб-квартира южнокитайского флота находится в Чжаньцзян на полуострове Лэйчжоу, а военно-воздушные силы, при поддержке которых проводятся операции на море, базируются на острове Хайнань в Тонкинском заливе. Штаб-квартира флота и морская авиабаза не имеют собственной электросети, они подключены к общей системе электроснабжения. У них нет собственных электрогенераторов, только аварийные резервные установки.

С помощью спецподразделения, 10-го флота, Киберкомандование использует заранее установленные «черные ходы» в электрораспределительной сети Китая и получает доступ к системе управления местной электросетью. Посылает сигналы, вызывающие скачки напряжения, вследствие чего срабатывают предохранители и генераторы останавливаются. Впрочем, американцы не провоцируют разрушение генераторов и трансформаторов.

Команда, играющая роль Китая, понимает, что блэкаут был не случаен, и прослеживает следы атаки. Следы ведут в Эстонию и далее теряются. Никто в Пекине не подумает, что их атаковали эстонские хакеры. «Сигнал» привлекает внимание китайской команды. Им сообщают, что блэкаут на полуострове Лэйчжоу вызвал отключение электричества во всей провинции Гуандун (бывшем Кан-

ZZ3

Третья мировая война: какой она будет?

тоне), вследствие чего более ста миллионов граждан почти на сутки остались без света. Блэкаут затронет и Гонконг. Политбюро считает, что это лишь начало, и просит Киберподразделение Народно-освободительной армии предложить ответные действия. Киберподразделение рекомендует отреагировать соизмеримо и задеть города, в которых базируется американский флот, но послать сигнал о том, что Китай способен на большее. Политбюро одобряет все шесть шагов, предложенных кибервоинами:

1. Обеспечить подкрепление Южному флоту и отправить больше самолетов на Хайнань и аэродромы Южного побережья.
2. Отдать приказ китайской эскадре подводных лодок из Юйлинь, остров Хайнань, выйти в море.
3. Активировать логические бомбы, размещенные в электросетях Гонолулу, Сан-Диего и Бремертона (штат Вашингтон) — городах, где дислоцированы базы Тихоокеанского флота США. (Блэкаут распространится на Тихуану (Мексика) и Ванкувер (Британская Колумбия), хоть китайцы об этом и не знают.)
4. Разрушить открытую сеть Министерства обороны, запустив «червя», который заразит одну машину за другой и сотрет информацию с жестких дисков (атака будет запущена из внутренней сети Министерства обороны).
5. Атаковать эстонского интернет-провайдера, откуда предположительно была произведена атака на китайскую электросеть.
6. Вызвать блэкаут в японском городе Йокосука и на окружающей территории, где находится штаб- квартира 7-го флота США.

224

Как наступать?

К началу следующего этапа учений напряжение нарастает, и Киберкомандование узнает, что Китай собирается отключиться от мирового киберпространства. Поэтому команда из Форт-Мид просит Пентагон разрешить запуск еще двух волн кибератаки и приготовиться к запуску третьей. Две атаки предлагается направить на сеть ПВО Китая и систему управления военного командования. Планируется использовать сверхсекретные программы атаки и логические бомбы, заранее размещенные в этих сетях. В перспективе можно атаковать железнодорожную сеть Китая, авиадиспетчерскую службу, банковскую систему и электросети (генераторы и трансформаторы).

Странно, но Киберкомандование получает из Белого дома и Пентагона приказ воздержаться от нападений на военное командование, системы управления и средства обороны, в частности ПВО. Киберкомандованию отдают приказ избегать атак на систему управления воздушным движением и банковский сектор.

Пока Киберкомандование формулирует дальнейшие предложения, из Security Industries Automation Corporation и Deposit Trust в Нью-Йорке сообщают о том, что их базы данных серьезно повреждены и даже разрушены. Также пострадали базы данных железных дорог CSX, Union Pacific и Burlington Northern Santa Fe и авиакомпаний United, Delta и American Airlines. Нью-Йоркская фондовая биржа закрыта, остановлены товарные поезда, самолеты не могут взлететь в аэропортах по всей стране. Управление информационного обеспечения, которое управляет внутренней сетью Министерства обороны, объявляет чрезвычайное положение, поскольку в секретную сеть SIPRNET и в сверхсекретную JWICS проникли «черви», распространяющиеся с невероятной скоростью и разрушающие жесткие диски. Все эти атаки пришли не из-за границы, поэтому американская разведка и Киберкоман-

225

8 № 4595

Третья мировая война: какой она будет?

дование не обнаружили их на входе и не могли остановить. Очевидно, были использованы новые, неизвестные приемы, поэтому Киберкомандование не сумело заблокировать их, используя опыт прошлых нападений.

Выбор у Киберкомандования США невелик — нельзя атаковать китайскую систему ПВО, банки, систему управления вооруженных сил и авиадиспетчерскую службу. Более того, поскольку американское Киберкомандование должно защищать сети Министерства обороны, некоторым сотрудникам приходится переключиться на борьбу с появившимися там «червями». Учитывая масштабы действий китайской команды, американцы решают устроить блэкаут по всему Китаю и в том числе вывести из строя несколько крупных генераторов. В то же самое время они попытаются вызвать как можно больше аварий товарных поездов и устроить беспорядок в базах данных железнодорожной системы. Чтобы найти замену военным целям, которые вычеркнуло высшее командование, американская команда решает атаковать китайские военные и гражданские спутники связи.

Доклад руководящей группы о последствиях второго раунда атаки сложно назвать хорошей новостью для американцев. Китай отсоединил свои сети от глобального Интернета, тем самым ограничив возможности американского нападения. Более того, когда Соединенные Штаты впервые атаковали электросеть, Пекин приказал всем остальным ее секторам перейти в положение обороны, то есть отключиться от Интернета. Электрические сети Китая разделились на «островки», чтобы предотвратить каскадные отключения электричества. Лишь несколько генераторов, выбранные американцами в качестве мишеней, были выведены из строя, что привело к локальным отключениям электричества. Все остальное было переведено в режим обороны — железные дороги стали управ-

 226

Как наступать?

ляться вручную и по радиоканалам. Попытка нарушить работу системы товарных поездов не удалась.

США взломали китайский спутник связи, заставив его поворотный двигатель работать, пока не израсходовалось все топливо, и направив в сторону Юпитера. Однако в течение часа китайский флот привел в действие запасную, засекреченную телетайп-систему. Но атака американцев на сеть снабжения китайского флота оказалась успешной, что наряду с региональным отключением электроэнергии замедлило погрузку китайских военных подразделений на корабли.

Руководящая группа также сообщила, что китайская подводная лодка всплыла на поверхность точно между двумя американскими авианосцами. Она проникла за границу обороны, подобно тому, как произошло в 2009 году, когда подлодка класса Song оказалась рядом с американским авианосцем Kitty Hawk. Поднявшись на поверхность, подлодка выдала свое расположение, но послала США сигнал, что дислокация американских авианосцев китайцам точно известна. Если бы началась активная фаза войны, это позволило бы Китаю направить на данный участок множество крылатых ракет наземного и воздушного базирования.

Киберкомандование США проинформировали, что Белый дом приказал двум группам американских авианосцев взять курс на Австралию. Госдепартамент готов начать переговоры на высшем уровне по поводу территориальных претензий Китая. Киберкомандованию приказано прекратить наступательную операцию.

После каждых кабинетных учений в правительстве проводится собрание наблюдателей и игроков под названием «горячий душ». Пора записать полученные уроки и наметить области дальнейшего исследования. Итак. Что мы узнали из учений «Южно-Китайское море»? Намети-

 227

Третья мировая война: какой она будет?

лось десять важнейших проблем: концепция сдерживания; ненападение; предвоенная подготовка поля битвы; глобальное распространение регионального конфликта; сопутствующий ущерб; контроль эскалации; случайная война; атрибуция; кризис неустойчивости; асимметрия обороны. Давайте последовательно проанализируем каждую из них.

1. . Сдерживание

Очевидно, в этом случае сдерживание не состоялось. Какой урон Китай может нанести Соединенным Штатам? В реальном мире США, пожалуй, воздержались бы от развязывания полномасштабной кибервойны с Китаем из боязни несимметричных последствий, к которым бы привели ответные меры. И все же сдерживание — это самая неразвитая теоретическая область в современной концепции кибервойн. Теория сдерживания служила основой ядерных стратегий США, Советского Союза и НАТО в эпоху холодной войны. Страх последствий использования ядерного оружия (и опасение того, что любое его использование станет глобальным) удерживал ядерные державы от применения абсолютного оружия друг против друга. Он также удерживал государства, как ядерные, так и нет, от любых действий, которые могли бы спровоцировать ответный ядерный удар. Стратеги разрабатывали сложные теории ядерного сдерживания. В 1960-х годах Герман Кан выделил три разных типа ядерного сдерживания. Теоретические исследования Германа Кана изучались гражданскими и военными лидерами Соединенных Штатов и Советского Союза. Его сухие размышления о вероятных масштабах разрушений, изложенные в кни- 22В

Как наступать?

гах «О термоядерной войне» (1960) и «Думать о немыслимом» (1962), несомненно, помогли предотвратить ядерную войну.

Из всех ядерных концепций теория сдерживания, пожалуй, наименее применима к кибервойне. На самом деле сдерживание в киберпространстве имеет совершенно иное значение, чем в работах Кана и стратегов тех годов. Ядерное устрашение основывалось на представлении о последствиях применения ядерного оружия. Мир в 1945 году увидел два ядерных взрыва в Хиросиме и Нагасаки. Позднее проводились многочисленные надземные испытания: Соединенными Штатами и Советским Союзом в 1940-1950-х, Великобританией в 1952-м, Францией в 1960-м и Китаем в 1968-м. В общей сложности пять первых ядерных держав взорвали около 2300 ядерных снарядов над и под землей.

Никто не знает, что бы случилось, если бы Соединенные Штаты или Советский Союз запустили несколько сотен баллистических ракет с ядерными боеголовками, но изначально американские военные планировали запустить более 90 % своих ракет и задействовать все имевшееся вооружение. Чтобы удостовериться, что возможная массовая атака окажется успешной, американские военные планировали наносить ядерные удары трех разных видов (бомбардировка с воздуха, запуск ракет наземного базирования, запуск ракет морского базирования). Обе сверхдержавы развернули свои силы так, чтобы после неожиданной массированной атаки со стороны противника большая часть ядерного оружия не пострадала. Ответный удар был неизбежен. То есть существовала почти полная уверенность в том, что если одна сторона применит ядерное оружие, то от него же в той или иной степени пострадает. Последствия массированного обмена ядерными ударами были предметов дебатов, но мало кто сомневался в том,

229

Третья мировая война: какой она будет?

что обе стороны нанесут друг другу ущерб, не имеющий равного во всей человеческой истории. Многие полагали, что после атомной войны настанет ядерная зима и человечество вымрет. Почти все эксперты были уверены в том, что массированный обмен ядерными ударами приведет к быстрой смерти миллионов (Кан сухо отмечал: «Никто не хочет стать первым убийцей сотен миллионов человек»).

Все опасались, что любое применение ядерного оружия может привести к войне непрогнозируемого масштаба. Это опасение вот уже более 60 лет сдерживает Соединенные Штаты и Советский Союз от использования ядерного потенциала. Проведенные ядерные испытания создали эффект демонстрации. Некоторые теоретики полагали, что в случае масштабного кризиса (войны с применением обычных видов вооружения в Европе) Соединенные Штаты могут взорвать ядерную бомбу в целях демонстрации, предупреждая: если война не прекратится, Североатлантический союз готов перейти к использованию ядерного оружия. В НАТО планировали «сигнализировать о намерениях НАТО» такими предупредительными выстрелами. Как показывают все имеющиеся на сегодняшний день примеры кибервойн, в данном случае эффект демонстрации не работает. Как уже обсуждалось, большинство киберинцидентов представляли собой либо простые DDoS- атаки, либо тайное проникновение в сеть с целью кражи информации или размещения лазеек и логических бомб. На последствия DDoS-атак мало кто обращал внимание, помимо ее непосредственных жертв. Что же касается взломов, о них зачастую не догадываются даже жертвы.

Итак, в какой степени кибервоины уверены, что их оружие сработает, каких последствий они ожидают от его применения? Они знают, что им неоднократно удавалось проникнуть в сети других государств. Возможно, они испробовали все, за исключением нескольких финальных

 23 □

Как наступать?

нажатий кнопок, которые сделали бы в настоящей кибервойне. Они наверняка проводили разрушительные операции на моделях вражеских сетей. Такие испытания проводились на генераторе в штате Айдахо в рамках программы «Аврора». В результате экспериментаторы убедились, что с помощью кибероружия можно вызвать физическое разрушение большого электрогенератора.

Однако кибервоины не знают, какие сюрпризы может им преподнести защита страны, которую они атакуют. Что будет, если Китай отсоединит свою сеть от остального киберпространства? Есть ли у США план действий при таких обстоятельствах? Если русские разместили «черные ходы» и логические бомбы в американских сетях, как им узнать, что американцы их не обнаружили и не запланировали их устранение в случае напряжения отношений? Когда кибервоин соберется проникнуть в сеть с помощью заранее установленных «черных ходов», маршрут доступа могут заблокировать, а на его пути неожиданно встанет эффективная система предотвращения вторжений. В отличие от систем ПРО системы предотвращения вторжений в важнейшие сети могут держаться в тайне до момента их активации. Если задача кибервоина — отключить вражескую систему ПВО накануне вторжения бомбардировщиков, военно-воздушные силы атакующей страны может постигнуть глубокое разочарование. Радиолокационные станции и ракеты, которые считались бездействующими, могут внезапно активироваться и уничтожить штурмовую авиацию. Последствия ядерного взрыва знали наверняка. Если его целью была военная база, она выводилась из строя на долгие годы, если не навсегда. Когда я в 1970-х годах был аспирантом Массачусетского технологического института, мне почти сразу вручили специальный диск — калькулятор ядерного воздействия. Сделав поворот одного диска на один

Третья мировая война: какой она будет?

круг, мы устанавливали мощность ядерного взрыва, скажем, 200 килотонн. Покрутив другой — выбирали, где будет производиться взрыв (на земле или в воздухе). Затем указывали максимальное расстояние до цели, и этот маленький калькулятор определял, будет ли мощность взрыва достаточной, чтобы сравнять с землей ракетную стартовую шахту врага и превратить ее в облако радиоактивной пыли. Кибервоин может быть уверен в том, что если он нанесет удар серьезным кибероружием по какой- то системе, эта система, скажем железнодорожная, скорее всего, выйдет из строя. Но ему не известно, существуют ли у данной системы надежный план противодействия сбоям и резервная сеть управления, ведь противник держит ее в секрете и не использует. Нападению препятствует система предотвращения вторжений, а система поддержки непрерывности позволяет быстро восстановить объект после кибератаки.

В силу невозможности узнать оборонительный потенциал противника концепция сдерживания в теории кибервойны существенно отличается от концепции сдерживания в ядерной стратегии. В ядерной стратегии было предельно ясно — в большинстве случаев нападение предпочтительнее, то есть любую оборону легко разбивает своевременная внезапная атака. Гораздо дешевле направить свои ракеты на оборонные объекты противника, чем разрабатывать хоть сколько-нибудь эффективные средства ПРО. Какой бы совершенной ни была оборона, нападение давало сто очков форы. Кроме того, никто ни на секунду не мог представить, что Советский Союз или Соединенные Штаты тайно сумеют разработать и развернуть эффективную систему ПВО. Рональд Рейган надеялся, что США, потратив миллиарды долларов на исследования, сумеют изменить это соотношение и средства противоракетной обороны станут реальной силой. Спустя

232

Как наступать?

десятилетия мы этого так и не добились, и сегодня Соединенные Штаты надеются, что им удастся предотвратить небольшую ракетную атаку или нападение примитивных ракет второстепенных государств. Но даже это остается под сомнением.

В теории стратегической ядерной войны разрушительная мощь нападения была хорошо известна, и никакие средства обороны не могли воспрепятствовать ей, поэтому нападения боялись. Это сдерживало страны от применения ядерного оружия и совершения других провокационных действий, способных вызвать ответный ядерный удар. В случае кибервойны потенциал нападения в значительной мере секретен, но в случае кризиса может быть использована и эффективная оборона, так что едва ли какая-либо страна готова отказаться от применения кибероружия.

Предположим, что Соединенные Штаты (или какая- либо другая страна) обладают таким мощным наступательным кибероружием, что могут преодолеть любую защиту и нанести серьезный урон вооруженным силам и экономике противника. Если бы США объявили о таких возможностях, не раскрывая деталей, многие оппоненты сочли бы, что мы блефуем. Когда не известны подробности, когда никто не видел американское кибероружие в действии, мало кто испугается до такой степени, чтобы воздерживаться от действий. Теоретически США могут продемонстрировать свой киберпотенциал, наказав каких-нибудь злодеев. (В 1989 году США направили истребители-бомбардировщики F-117 в Панаму не потому, что боялись панамской противовоздушной обороны, а потому, что Пентагон жаждал похвастаться своим новым оружием и устрашить остальных. Вторжение получило кодовое название «Просто потому», и многие в Пентагоне саркастически замечали, что мы послали туда F-117 «просто

 233

Третья мировая война: какой она будет?

потому, что можем».) Что же касается идеи использования кибероружия в ходе очередного кризиса, проблема в том, что многие сложнейшие приемы кибератаки разрабатываются только для одноразового применения. Когда кибероружие используется, потенциальные оппоненты обнаруживают его и прилагают все усилия для разработки защиты.

Если США не в силах устрашить других секретным кибероружием, боимся ли мы сами киберугрозы со стороны других стран? Иначе говоря, удерживаем ли мы себя сегодня от обычных военных операций, помня о собственной уязвимости в киберпространстве? Если бы кризис в Южно-Китайском море начался, как в описанных выше учениях, сомневаюсь, чтобы кто-нибудь на собрании оперативного штаба сказал президенту: «Лучше не посылайте авианосцы в Китай. Если вы это сделаете, господин президент, Пекин запустит кибератаку, которая разрушит нашу фондовую биржу, заставит приземлиться наши самолеты, остановит поезда, погрузит наши города во тьму. Мы никак не сможем остановить их, сэр».

Кто-то должен это сказать, поскольку, конечно, так оно и есть. Но скажут ли? Маловероятно. Самый высокопоставленный американский офицер только два года назад узнал о том, что его сеть может быть разрушена в результате кибератаки. Белый дом под управлением президента Обамы целый год не назначает кибербосса. Американские военные считают технологии чем-то вроде козыря в рукаве, который позволяет самолетам, кораблям и танкам работать лучше всех в мире. Им сложно представить, что другие страны могут эффективно использовать технологии против нас, особенно когда эти технологии — строки компьютерного кода, а не самолеты-невидимки.

Итак, мы не способны удержать другие страны от применения кибероружия. На самом деле другие страны не

23-4

Как наступать?

сдерживают себя и регулярно взламывают наши сети. Не способны мы и удержать их от действий, которые могут спровоцировать масштабную кибератаку. Сдерживание — это всего лишь потенциал, то, что мы может создать в голове возможного взломщика, если (очень большое если) серьезно отнесемся к развертыванию эффективных средств обороны в некоторых важнейших сетях. Поскольку мы даже не приступали к этому, теория сдерживания — краеугольный камень предотвращения ядерной войны — не играет никакой роли в предупреждении кибервойны.

2. Ненападение

Наверное, вы заметили, что в сценарии наших гипотетических учений было одно условие — мы нанесли первый удар. При отсутствии любой другой стратегии американская сторона в этих гипотетических учениях делает первый шаг в киберпространстве, рассылая оскорбительное электронное письмо по внутренней почтовой системе, которую китайцы считали закрытой, а затем инициируя то, что, как надеялись американцы, будет локальной аварией энергосистемы. Стратегической целью было показать, как серьезно Соединенные Штаты относятся к данному кризису, и продемонстрировать, что США обладают некоторыми возможностями. Непосредственной тактической задачей Киберкомандования было приостановить погрузку китайского десанта, чтобы выиграть время на переговоры американских дипломатов с китайцами по поводу запланированной операции.

В ядерной стратегии Советский Союз предлагал нам согласиться на условие, что ни одна сторона в случае кон-

 235

Третья мировая война: какой она будет?

фликта не должна применять ядерное оружие первой. Американское правительство всегда отвергало эту идею, оставляя за собой свободу выбора в использовании ядер- ного оружия для того, чтобы компенсировать превосходящие неядерные силы Советского Союза. Следует ли использовать подход отказа от нападения первым в кибер- военной стратегии? В мире не существует традиционных вооруженных сил, которые превосходили бы американские, при условии, что американские войска не окажутся ослеплены и разъединены в результате кибератаки. Следовательно, нам не нужно стремиться начать кибервойну первыми, чтобы компенсировать какие-то недостатки, как приходилось делать в ядерной стратегии. Кроме того, когда мы делаем первый шаг в кибервойне, наша жертва в глазах всего мира поступает более приемлемо с политической точки зрения, когда отвечает нам тем же. Так что, учитывая нашу уязвимость к кибератаке, США, возможно, и не захотят переходить к кибернетической фазе войны.

Однако отказ от применения кибероружия до того, как оно будет использовано против нас, может означать, что, если вспыхнет обычная война, мы не сумеем защитить войска, используя кибератаку на системы противовоздушной обороны противника. Первое использование кибероружия в сценарии учений «Южно-Китайское море» было психологической операцией — мы рассылали электронное письмо с изображением тонущего китайского корабля по внутренней сети китайских вооруженных сил. Следует ли это считать первым применением кибероружия?

Более того, сценарий обнажил проблему: если вы не делаете первый шаг в киберпространстве, ваши возможности запустить кибератаку снижаются, поскольку другая сторона принимает оборонительные (Китай отключает свое киберпространство от всего остального мира)

236

Как наступать?

и наступательные (включая атаки, которые выводят из строя американские сети, которые, возможно, необходимы для запуска наших кибератак) меры. Заявлено ли это публично или считается скрытым элементом нашей стратегии, если мы принимаем решение не применять кибероружие первыми, мы должны четко понимать, что это будет означать. Считается ли актом кибервойны проникновение в сеть? Когда проникновение в сеть выходит за рамки простого сбора информации и превращается ли в этот момент разведывательное действие в кибервойну? Любой запрет на первый шаг применим лишь до начала поступательных военных действий. Как только война становится наступательной, почти все договоренности отменяются.

1. Подготовка попя боя

Вы должны были обратить внимание еще на один момент — обе стороны конфликта проникли в системы друг друга задолго до начала учений. В реальном мире, вероятно, они уже проделали то же самое.

Если ЦРУ засылает агентов в некую страну, чтобы они провели расследование на предмет возможности будущего саботажа и оставили тайники с оружием и взрывчаткой, по американскому закону эта деятельность считается секретной операцией, требует разрешения президента и формального уведомления двух разведывательных комитетов конгресса. В последние годы Пентагон придерживался мнения, что подобного рода секретные операции — эт0 всего лишь подготовка поля боя и знать о них не обязательно. Выражение «подготовка поля боя» стало

237

Третья мировая война: какой она будет?

достаточно гибким. Почти любое место когда-нибудь может стать полем битвы.

Такая гибкость стала использоваться и в кибервоен- ной сфере, к тому же, очевидно, не только в Соединенных Штатах. В наших гипотетических учениях и США и Китай использовали предварительно установленные «черные ходы» в сетях противника, а затем взорвали логические бомбы, размещенные в том числе и в сетях, управляющих электроснабжением. Помимо учений есть и другая причина верить, что кто-то уже разместил логические бомбы в сетях управления американской энергосистемой. Несколько осведомленных источников намекнули или подтвердили, что США уже готовят поле боя.

Представьте: ФБР объявило, что арестованы десятки агентов китайского правительства, которые по всей стране устанавливали взрывчатку С4 на башни высоковольтных линий передач и трансформаторные подстанции. Вся нация возмутится. Некоторые конгрессмены начнут требовать объявления войны или карательных санкций в отношении китайского импорта. Кто-то станет настаивать, что пора называть китайскую еду чипсами свободы. Ну а когда в апреле 2009 года Wall Street Journal опубликовал статью о том, что Китай разместил логические бомбы в системе электроснабжения Соединенных Штатов, реакции практически не последовало. Такой разный отклик свидетельствует главным образом о неискушенности конгресса, СМИ и публики в вопросах кибервойны. Хотя это не означает, что существует какая-либо разница между последствиями взрыва логических бомб и взрывчатки С4.

Внедрение логических бомб в системы наподобие американской сети электропередач нельзя считать разведывательной операцией по сбору информации. Можно собирать сведения о системах вооружения, проникая в сеть

23В

Как наступать?

Raytheon Company[[102]](#footnote-103)или Boeing, но в системах управления Florida Power and Light нет информационной ценности.

Даже если бы там имелись ценные данные, логические бомбы не собирают информацию, они разрушают ее. Единственное объяснение тому, что вы вторгаетесь в систему управления электросетью, размещаете «черный ход», который позволит вам быстро проникнуть туда позднее, а также оставляете компьютерный код, способный после активации испортить программное (и даже аппаратное) обеспечение сети, — вы планируете кибервойну. Это не значит, что вы уже решили ее начать, но определенно подразумевает, что вы к ней готовы.

Во времена холодной войны и даже позднее ходили легенды о том, что советские агенты проникают в США с миниатюрными (чемоданными) ядерными бомбами, которые способны стереть с лица земли американские города, даже если США нанесут внезапный удар по СССР и уничтожат все бомбардировщики и ракеты. В то время как у США и Советского Союза действительно было «малое» оружие (у нас есть несколько сотен таких устройств Medium Atomic Demolition Munitions, MADM, и Small Atomic Demolition Munitions, SADM, которые могут поместиться в рюкзак), нет никаких доказательств, что кто- либо из нас развернул его на стороне противника. Даже в разгар холодной войны стратеги полагали, что использовать MADM слишком опасно. Но почему же китайские и, вероятно, американские ответственные лица разрешили использовать логические бомбы на территории другой страны? Маловероятно, что высокопоставленные чинов-

Третья мировая война: какой она будет?

ники одной или обеих стран не знали о таких действиях. Возможно, это военные отдали такой приказ, воспользовавшись собственными полномочиями по подготовке поля боя. Существует определенный риск, что высшим должностным лицам в случае кризиса скажут, что противник разместил логические бомбы на этапе подготовки к войне и будет угрожать ими, вынуждая высокопоставленных политиков принимать ответные меры. Лидерам могут доложить, что противник намерен разрушить нашу энергосистему, и мы должны действовать первыми, пока есть такая возможность. Есть и другой риск — оружие и в самом деле можно использовать без санкции высшего руководства. Его мог разместить слишком самостоятельный военачальник, или хакер, или рассерженный сотрудник. Кибервоины оправдывают шаги по подготовке поля боя, называя их необходимыми мерами по обеспечению руководства страны свободой выбора во время кризиса: «А вы бы хотели, чтобы у президента осталось меньше вариантов, как действовать в случае кризиса?» — спрашивают они. «Если вы хотите, чтобы в будущем у него была возможность действовать в киберпространстве, вы должны позволить нам проникнуть в их сети. Если сейчас сеть уязвима перед несанкционированным проникновением, это не значит, что так будет и через несколько лет, когда нам понадобиться в нее попасть».

Сети постоянно совершенствуются. Вполне вероятно, что электроэнергетические компании однажды приобретут эффективную систему предотвращения вторжений (IPS), способную обнаруживать и блокировать методы, которые мы используем для взлома сетей. Но если мы способны проникнуть в их сеть сейчас, мы можем оставить «черный ход», который любая будущая система безопасности воспримет как санкционированный. Однако проникнуть в сети в будущем — это еще полдела, нам необходи- 240

Как наступать?

мо будет запустить код, которые заставит систему делать то, что нужно нам. Будущая система может блокировать загрузку исполняемого кода даже авторизированным пользователем. Следовательно, мы должны, проникнув в систему сейчас, оставить там код, который заблокирует защиту от скачка напряжения, заставит генераторы вращаться несинхронно, в общем, обеспечит нам шанс использовать выбранный нами способ нарушения (или разрушения) работы сети или оборудования.

Звучит убедительно, но есть ли места, в которых готовить поле боя нежелательно?

1. ГПОБАПЬНАЯ ВОЙНА

В наших гипотетических учениях ответный удар китайцев был направлен на четыре американские военно-морские базы, но затронул несколько крупных городов в четырех странах (North American Interconnects связывает энергетические системы США, Канады и Мексики).

Чтобы замести следы, США напали на китайскую сеть с эстонского компьютера. Чтобы добраться из Эстонии до Китая, американские атакующие пакеты прошли через несколько стран, включая Россию. Чтобы обнаружить источник атаки, китайцам пришлось бы проникнуть в российские маршрутизаторы, откуда поступили последние пакеты. Китай нанес ответный киберудар по Эстонии, чтобы дать понять — страну, которая позволяет проводить кибератаку, может ожидать возмездие, даже если это сделано неумышленно.

В эпоху межконтинентальных ракет и самолетов кибератака развивается быстрее и пересекает границы проще, чем любые другие формы военных действий на

24 1

Третья мировая война: какой она будет?

всем протяжении истории человечества. Как только государство инициировало кибервойну, возникает высокая вероятность того, что другие страны окажутся в нее втянуты, поскольку нападающие постараются скрыть как свою личность, так и маршруты, по которым шло нападение. Начать атаку с эстонских сайтов для США — это примерно то же, что без позволения посадить штурмовики на территории Монголии, дозаправить их, взлететь и сбросить бомбы на Китай. Поскольку некоторые средства нападения, например «черви», распространяются за считанные минуты, существует вероятность возникновения сопутствующего ущерба по мере того как эти программы будут перескать межгосударственные границы и разрушать неучтенные цели. А что насчет сопутствующего ущерба в стране, которая служит объектом атаки?

1. Сопутствующий ущерб

И ДОКТРИНА СДЕРЖИВАНИЯ

Стараясь поразить военно-морские базы, оба противника нанесли удар по электростанциям. При этом огромные регионы и миллионы людей остались без света, поскольку электросети очень уязвимы перед каскадными отключениями, которые происходят за секунды. В десятках больниц резервные генераторы так и не сумели запуститься. Международные законы вообще запрещают атаковать больницы и гражданские объекты, но невозможно разрушить электросеть, не затронув гражданские здания. В ходе последней войны в Ираке американцы провели кампанию «Шок и трепет», в процессе которой были стерты с лица земли конкретные здания, а гражданские объ- 242

Как наступать?

екты, расположенные на той же улице, остались нетронутыми. США и другие страны, соблюдающие осторожность при бомбовых ударах, разработали разрушительное кибероружие, вред от которого невозможно ограничить атакуемыми объектами.

В нашем сценарии кибервойны американское Киберкомандование не получило разрешения атаковать банковский сектор. В реальном мире мои предложения убедить Управление национальной безопасности вторгнутся в банковские системы и захватить финансы «Аль-Каиды» неоднократно пресекались Министерством финансов, когда президентом был Клинтон. Даже при Буше Министерство финансов смогло заблокировать предложение атаковать банковские счета Саддама Хусейна, в то время как администрация готовила вторжение и оккупацию, в ходе которых погибло более ста тысяч иракцев. Банкиры убеждали, что система международных финансовых отношений и торговли строится на определенном уровне доверия.

Решение США воздержаться от атак на финансовый сектор отражает понимание того, что Соединенные Штаты в кибервойне, затрагивающей банки, могут понести самые высокие потери. Даже несмотря на то что американский финансовый сектор защищен лучше всех остальных отраслей, он все же уязвим. «Мы, как приглашенные советники, проверили безопасность десяти с лишним крупнейших финансовых учреждений страны и сумели вторгнуться в систему каждого, — рассказал мне знакомый консультант по вопросам безопасности. — И каждый раз мы могли поменять цифры или перевести деньги, но, разумеется, этого не делали».

Существующие в США законы не запрещают вторгаться в системы иностранных банков для сбора разведывательных данных, но создают очень большие препят-

 243

Третья мировая война: какой она будет?

ствия для изменения данных. Министр финансов и госсекретарь должны дать разрешение на такие действия. Насколько мне известно, подобные санкции никогда не давались. По существу, мы имеем дело с объектами, на которые нацелились, но не намереваемся наносить удар. Согласно такой стратегии, мы предполагаем или надеемся, что противники будут играть по этим же неписаным правилам. В учениях «Южно-Китайское море» Народно- освободительная армия Китая не стала следовать этим правилам. В ходе последней операции она нанесла удар по базам данных фондового рынка. Это было драматическое и, надеемся, нереальное развитие ситуации. Экономика современного Китая так крепко связана с американской, что он должен воздерживаться от нападений на финансовый сектор. Можно предполагать, что в обозримом будущем страны будут воздерживаться от атак на финансовый сектор, вызывающих изменение данных, хотя некоторые американские аналитики выражают сомнения относительно Китая.

Поскольку рассчитывать на аналогичную вежливость со стороны искушенного хакера-одиночки не приходится, американский финансовый сектор совместно с федеральными регулятивными органами должен заранее прийти к пониманию, что делать в случае атаки, способной изменить хранящуюся информацию. Вероятно, следует обсудить планируемые действия с некоторыми европейскими и японскими институтами. У Федерального резервного банка, Securities Industry Automation Corporationи ряда других операторов финансовых баз данных существуют специальные системы удаленной архивации. Чтобы быть готовыми к восстановлению данных после атаки, необходимо иметь «слепок» того, «кто чем владел», который не сможет затронуть кибератака. По согласованию с федеральными органами управления банки и фондовые

244

Как наступать?

биржи в случае сбоя могут восстанавливать систему по предыдущим данным. Кто-то потерпит убытки, кто-то разбогатеет, но финансовая система продолжит функционировать.

Китайская система управления полетами (СУП) также попала в список важных целей. В то же время, модернизация привела к тому, что зависимость американской СУП от сети и, следовательно, уязвимость перед кибератакой возросла. Даже при старой системе в США происходили случаи, когда отдельные диспетчерские пункты аэропортов и даже региональные центры отключались на несколько часов из-за неисправностей компьютеров или связи. Насколько нам известно, ни одно из этих отключений не было вызвано взломом. (Одного хакера, вторгшегося в систему Федерального авиационного агентства, арестовали, хотя последствия его атаки были минимальными.)

Тем не менее возможность того, что кто-нибудь изменит данные и заставит самолеты столкнуться в воздухе, необходимо рассматривать. США подписали Монреальскую конвенцию, в соответствии с которой умышленное нападение на гражданский пассажирский самолет является нарушением международного права. Практически все взломы считаются нарушением каких-либо государственных или международных законов, но Монреальская конвенция — это выражение международного мнения о том, что определенные действия выходят за рамки допустимого поведения.

Вторгнуться в системы управления полетами становится все проще. Федеральное авиационное агенство выразило беспокойство в связи с планами Boeing использовать в новом самолете 787 Dreamliner единую компьютерную сеть для управления полетом и интерактивного развлечения пассажиров. Управление поделилось опасениями о том, что пассажир может вторгнуться в систему

245

Третья мировая война: какой она будет?

управления полетом прямо со своего места или подключиться к ней с земли через Интернет. Компьютерные сети пассажирских самолетов играют важную роль в обеспечении полета. В современных самолетах с дистанционным управлением система управления полетом посылает компьютерный сигнал для управления закрылками, элероном или рулем высоты. Авария самолета Air France в 2009 году, о которой уже упоминалось, показала широкой аудитории то, что пилоты знали давно: в современных самолетах с дистанционным оборудованием бортовые компьютеры сами решают, какие сигналы посылать на землю. При определенных условиях программа может проигнорировать решение пилота и заблокировать ручное управление, чтобы предотвратить падение самолета. Как и в случае с системой управления полетами, компьютерные сети пассажирских самолетов должны быть недоступными для посторонних.

Военная авиация хотела бы вести честную игру. Если бы Киберкомандование попросило разрешения атаковать резервные и рабочие системы китайских авиакомпаний, они получили бы, пожалуй, разную реакцию. В реальном мире из-за компьютерных сбоев в США и Канаде сотни самолетов часами ждали разрешения на взлет. Самолеты были исправными, экипаж — в полной готовности, но без работающих баз данных и операционной сети авиакомпании просто не могли знать, какие самолеты, каких пассажиров, какой экипаж, груз, какое топливо и куда направлять. Авиакомпании, как и другие крупные коммерческие организации, больше не пользуются ручными системами.

Помимо банковской системы и пассажирского авиатранспорта могут быть и другие ограничения. В наших учениях Киберкомандованию приказано было не затрагивать военную сеть управления и систему обороны. Почему же нельзя было трогать эти объекты?

246

Как наступать?

1. ЭСКАПАЦИОННЫЙ КОНТРОЛЬ

Во время холодной войны я часто принимал участие в учениях, когда команда служащих госбезопасности тайно и в спешке отправлялась по срочному заданию из Вашингтона в глухие малодоступные места. Однажды мы занимались тем же, что предлагал компьютер из фильма «Военные игры» (War Games) — разыгрывали термоядерную войну. В целом это был очень неприятный опыт, поскольку по сценарию на земле от ядерных взрывов погибли миллионы людей. Почти всегда нашей задачей было завершить войну и начать восстановление. Самое сложное в конце войны — найти тех, кто выжил и командует войсками другой стороны. Кто руководит советскими вооруженными силами и как нам переговорить, не выдав свою дислокацию? Отчасти задачу усложнял тот факт, что человек, с которым мы вели переговоры, как выяснялось, на самом деле не контролировал некоторые подразделения советских вооруженных сил, например ядерные подводные лодки. Такой неприятный опыт научил нас следующему — когда мы уничтожаем систему контроля и управления противника, мы лишаем его возможности отдать приказ войскам сложить оружие. Изолированные командующие, отрезанные от высших звеньев управления или не признающие власти преемника, берут инициативу в свои руки и часто решают продолжать борьбу. Одинокие японские воины периодически появлялись на отдаленных островах Тихого океана еще в 1950-х, не зная, что император уже много лет назад приказал им сдаться. Подобное может произойти и кибервойне. Если в результате атаки будет уничтожена система военного командования и контроля, предотвратить наступательную войну будет сложно. В большинстве вооруженных сил полномочия переходят командующему на местах, если он не может связаться с начальством. Даже при

247

Третья мировая война: какой она будет?

функционирующей системе на местах могут решить, что власть захватили враги, которые отдают ложные приказы, в связи с чем командование передадут местному генералу, пока он не установит надежную связь с начальством. Подобная ситуация ярко представлена в фильме «Багровый прилив» (Crimson Tide), где капитан атомной подводной лодки сначала получает приказ запускать ядерные ракеты, а затем — не запускать. Будучи не в состоянии установить подлинность последнего приказа он, опасаясь, что это поддельный приказ, отправленный русскими, считает, что требуется произвести запуск.

На ядерных учениях мы постоянно приходили к выводу о том, что не нужно было наносить «обезглавливающий удар», после которого военное руководство противника не может связаться ни с нами, ни с собственными войсками. В кибервойне, возможно, стоит отключить некоторые части от высшего командования или закрыть противнику доступ к информации о происходящем. Но, выбирая, какие части «отрубать», необходимо помнить, что без связи с командованием подразделение с большой долей вероятности перейдет в наступление по собственной инициативе. Поэтому кибератаки нужно проводить очень внимательно, чтобы оставался канал связи для переговоров, а командование противника имело возможность приказать прекратить борьбу.

В наших с вами учениях запрещено было наносить удар по сетям противовоздушной обороны. Основанием такого запрета служит эскалационный контроль. В шедевре военной стратегии «Об эскалации» (1965) Кан утверждал: если ваша цель — завершить войну до тотального разрушения или вынужденной капитуляции противника, вы можете просигнализировать об этом, нанося удар по одним мишеням и не трогая другие. Допустим, вы хотите дать знать, что ваши намерения ограниченны, при-

Z4B

Как наступать?

чем так, чтобы противник не предположил иное и не счел, что терять уже нечего.

Из концепции эскалационного контроля можно сделать кое-какие выводы и для кибервойны. Кибератака на национальную систему противовоздушной обороны заставила бы руководство страны сделать вывод о планируемых воздушных атаках. В учениях «Южно-Китайское море» американские авианосцы располагались совсем близко. Если китайские военные подумают, что с этих авианосцев готовы нанести удар, они наверняка пойдут на упреждающие меры и потопят их. Таким образом, кибератака на систему противовоздушной обороны привела бы к наступательной войне, которой мы так старались избежать. Даже попытка проникновения в эту сеть для размещения лазеек и логических бомб может быть обнаружена и истолкована как подготовка к надвигающейся бомбардировке. Так что в эпоху обострения даже приготовление к запуску кибератаки толкуется превратно, поэтому такие меры следует предпринимать заблаговременно. Герман Кан, Томас Шеллинг, Уильям Кауфман и другие «всадники Армагеддона» много размышляли о том, как контролировать ядерную эскалацию, которая начинается от напряжения, ведущего к кризису, проходит стадии предупреждения, первого применения и окончания войны. Первоначально специалисты по ядерной стратегии считали, что этот процесс должен развиваться медленно, сопровождаемый дипломатическими попытками остановить конфликт на каждом данном этапе. Они обсуждали также концепцию эскалационного доминирования, которую я уже упоминал. Согласно этой стратегии, одна из сторон заявляет: «Мы не хотим вести мелкие военные действия, которые постепенно будут разрастаться. Если вы хотите сражаться с нами, готовьтесь к масштабному и разрушительному сражению». Похоже на ва-банк в покере в надежде, что сопер-

 249

Третья мировая война: какой она будет?

ник сдастся, а не станет рисковать всеми своими деньгами. За одним лишь исключением: в эскалационном доминировании вы действительно перепрыгиваете несколько ступеней лестницы и наносите серьезный урон противнику. Этот шаг вы сопровождаете угрозами причинить более значительный вред, если не остановиться прямо здесь и прямо сейчас. Тот факт, что вы уже нанесли урон, может заставить противника почувствовать необходимость ответить таким же образом. Или, если он благоразумен, то поймет, что ставки слишком высоки и ему грозят более серьезные потери. В учениях «Южно-Китайское море» Народно-освободительная армия Китая решила, что стране необходимо эскалационное доминирование. В ответ на кибератаку электросети в юго-восточной части Китая они не только нанесли удар по энергосистеме Западного побережья, но и разрушили глобальную внутреннюю сеть Министерства обороны США, повредили базы данных расчетных палат и направили дополнительные военные части в зону конфликта в Южно-Китайском море.

Игра затянулась, и руководству Соединенных Штатов нужно было решить, продолжать ли нести потери в следующем раунде кибервоенной эскалации. Америка находилась в невыгодном положении, поскольку в случае продолжения и обострения кибервойны она в любом случае потеряла бы больше. Поэтому Соёдиненные Штаты стремились к быстрому дипломатическому соглашению. Эскалационное доминирование — верный ход со стороны Китая, поскольку эскалация продемонстрировала, что США гораздо чувствительнее к кибератаке и дальнейшее обострение конфликта лишь ухудшило бы положение американской команды. Америка могла бы попытаться заблокировать кибертрафик, идущий из Китая. Но поскольку источники китайских атак располагались на территории США, а системы контроля в интернет-магистра- 250

Как наступать?

лях еще не существовало, следующую, более масштабную
китайскую кибератаку остановить было бы очень сложно.

Короче говоря, если собираетесь бросить киберкамень, убедитесь, что в вашем доме меньше стекла, чем у того парня, или что окна у вас пуленепробиваемые.

7. Позитивный КОНТРОЛЬ
И СЛУЧАЙНАЯ ВОЙНА

Затронутая выше проблема — сохранение возможности противника осуществлять командование и контроль — поднимает еще один вопрос: «Кто обладает полномочиями вторгаться в сети и применять кибероружие?» Ранее в этой главе я предположил, что для изменения банковской информации может понадобиться санкция членов кабинета, и все же мы не уверены, знает ли президент о логических бомбах в сетях разных стран, которые, возможно, разместили Соединенные Штаты. Оба этих факта указывают на большую неопределенность в вопросах о том, кто обладает полномочиями вести кибервойну и заниматься подготовкой поля боя.

В ядерной стратегии поднималось два главных вопроса — кто и что может сделать, которые объединяются понятием «позитивный контроль». Первый вопрос прост: «Может ли какой-нибудь американский офицер, имеющий доступ к ядерному оружию, использовать это оружие, даже если не имеет таких полномочий?» Чтобы предотвратить такую проблему и чтобы никто не украл и не взорвал ядерную бомбу, бомба была оборудована тщательно продуманным электронным механизмом. Электроника блокировала бомбу до тех пор, пока на устройство не поступал специальный буквенно-цифровой код. Часто

25 1

Третья мировая война: какой она будет?

требовалось, чтобы два офицера подтвердили код и одновременно повернули ключи для снятия блокировки — так называемый контроль «с двумя ключами». Часть кода хранилась вдали от бомбы и высылалась тем, кто должен его разблокировать. Эти и так сложные системы с годами еще более усложнялись. Соединенные Штаты частично поделились такой технологией с некоторыми ядерными державами.

Второй вопрос позитивного контроля: «Какая высшая инстанция обладает полномочиями посылать коды разблокирования ядерного оружия?» Теоретически при нормальных условиях такими полномочиями должен обладать президент. Офицер, прикомандированный к президенту, всегда носит с собой закрытый чемоданчик, в котором хранятся коды запуска на случай ядерной атаки. Во время попытки военного переворота 1990 года в Москве я узнал, что в Советском Союзе существовала аналогичная система. Президент Горбачев, который на одном из этапов кризиса оказался заложником, взял с собой на дачу такой «ядерный» чемоданчик с кодами запуска. Этот случай с Горбачевым подчеркнул необходимость передачи полномочий, если президент в силу каких-то обстоятельств не может действовать. Американское правительство отказывается сообщать, кто, помимо президента, обладает полномочиями деблокировать и использовать ядерное оружие и при каких условиях эти полномочия передаются. Весь персонал, имеющий доступ к ядерному оружию, должен подвергаться специальным проверкам и тестированиям, разработанным для отсеивания людей с психологическими или эмоциональными проблемами.

Кибероружие оказывает значительно меньшее воздействие, чем ядерное, но его использование может привести к большим разрушениям и вызвать более широкую войну. Итак, кто решает, применять ли его, и как мы мо- 252

Как наступать?

жем убедиться в том, что эти действия санкционированы? Кто должен решать, в какие сети нам нужно вторгаться в процессе подготовки поля боя? Пока мы не накопили достаточно опыта в применении кибероружия, я настаиваю на том, что президент должен по крайней мере раз в год утверждать рекомендации о том, в какого рода сети и в каких странах нам следует вторгаться для сбора информации и размещения логических бомб. Кто-то осудит такое предложение как чрезмерно ограничивающее и заметит, что мы годами вторгаемся в различные сети с разведывательной целью без всякого надзора со стороны президента. Пусть так, но нередко лишь несколько нажатий клавиш отделяют вторжение в сеть для сбора информации от разрушительных последствий. Поскольку существует риск, хоть и небольшой, что факт размещения логических бомбы и других проникновений будет обнаружен и воспринят как враждебное действие, президент должен решать, какой риск мы готовы взять на себя и с кем.

Ответственность за решение использовать кибероружие в разрушительных целях также следует возлагать на президента или в редких случаях, когда необходимо действовать быстро, на министра обороны. Могут возникнуть ситуации, когда региональным военачальникам придется воспользоваться заранее переданными полномочиями, чтобы защититься от надвигающейся или уже происходящей атаки. Однако Киберкомандование и подчиненные ему части должны использовать какой-то программный аналог контроля «с двумя ключами», чтобы гарантировать, что никакой чрезмерно рьяный или сильно заскучавший молодой лейтенант не инициирует атаку.

Но даже в случае надлежащего управления существует риск случайной войны. Первые радиолокационные системы во времена холодной войны иногда не могли отличить огромные стаи канадских гусей от строя советских

 253

Третья мировая война: какой она будет?

бомбардировщиков. Были времена, когда Соединенные Штаты запускали группы своих бомбардировщиков по направлению к определенным целям, ожидая, когда начальство воздушной обороны прояснит ситуацию и определит наверняка, подвергаемся ли мы нападению.

В кибервойне атака может начаться случайно, если кто-нибудь использует непроверенную программу и вместо того, чтобы добавить код, копирующий данные, использует код, который их удаляет. Кроме того, существует вероятность случайного запуска логической бомбы в результате действий оператора сети или какого-нибудь хакера, обнаружившего ее. Подобные шансы невысоки, но Киберкомандование и все те, кто участвует во взломах сетей других стран, обязаны придерживаться строгих правил, гарантирующих, что ошибок не будет. Риск случайной войны особенно увеличивается, если мы неправильно определяем, кто начал кибератаку против нас, и принимаем меры против неповинной страны.

В. Атрибуция

В учениях «Южно-Китайское море» ни одна из сторон не сомневалась в том, кто атаковал ее. Был политический аспект, росло напряжение вокруг морских нефтяных месторождений. Но что, если атаку совершил не Китай, а Вьетнам? По нашему сценарию Вьетнам является союзником Соединенных Штатов. Так с какой же стати ему нас атаковать? Да хотя бы для того, чтобы втянуть США в конфликт, заставить Вашингтон выступить против Китая. А что для этого может быть лучше, чем убедить Вашингтон в том, что Китай ведет кибервойну против Аме-

Z54

Как наступать?

рики? А когда Китай начнет отрицать свое участие, США наверняка спишут это на попытку Китая оправдаться. (Если вы хотите рассмотреть подобный сценарий и готовы простить меня за некоторую саморекламу, прочитайте мой роман Breakpoint («Точка излома»), в котором затрагивается проблема кибервоенной атрибуции.)

Киберэкспертам на конференции Black Hat 2009 года задали вопрос: считают ли они проблему атрибуции столь существенной, как некоторые полагают, сложно ли выяснить, кто вас атаковал, и так ли важно, кто это сделал? Все до единого ответили, что проблема атрибуции не является такой уж важной. Нет, они не утверждают, что определить взломщика легко, просто данный вопрос их не тревожит. В большинстве своем эксперты являются сотрудниками корпораций, и после кибератаки первоочередной задачей для них будет восстановление системы и предотвращение подобных атак в дальнейшем. Опыт общения с ФБР убедил их в том, что вряд ли стоит даже сообщать правоохранительным органам о фактах взлома.

Для сотрудников ФБР, однако же, куда важнее знать, кто атаковал. Об этом может спросить президент. Возможно, понадобится послать взломщикам дипломатическую ноту протеста, как сделал секретарь Клинтон после новостей о попытках проникновения в Google из континентального Китая. Может быть, вы захотите нанести ответный удар, чтобы атаку прекратили. Один из способов найти взломщика — использовать отслеживающие программы, но есть вероятность, что вы дойдете лишь до какого-то промежуточного сервера. На этом этапе есть основания подать дипломатическую ноту с требованиями, чтобы правоприменяющий орган страны в рамках международного сотрудничества по расследованию преступлений получил ордер, осмотрел сервер и извлек записи. На это потребуется не один день, и нужные записи за это время сумеют

 255

Третья мировая война: какой она будет?

уничтожить. Либо же виновная сторона откажется помочь вам. Когда следы прерываются, вы можете совершить «ответный взлом», проникнув на сервер и проверив данные. Разумеется, это будет незаконно, если только вы не офицер разведки. Но и проникновение на чужой сервер может не сработать, если взломщик скрыл свое нахождение. Во многих случаях вам придется находиться в режиме онлайн, наблюдая за тем, как атакующие пакеты проходят через серверы. Но, проследив путь через десяток серверов в разных странах, вряд ли вы обнаружите, что атака берет начало из места под названием «Российское агентство кибервоенного наступления». Даже если российское правительство организовало атаку, в целях безопасности оно наверняка будет действовать с сервера другого государства и, если это операция по сбору разведданных, вся полученная информация будет храниться в третьей стране. Далеко не всегда удается выяснить, кто атаковал вас, если только вы не находитесь в сети, которую использует взломщик, и не наблюдаете за процессом (что тоже не всегда возможно). Есть вероятность, что спецслужбы сумеют определить, на какой «языковой» клавиатуре писался код — арабской, кириллической или корейской, но они вряд ли вычислят самого хакера. Если даже выяснится, что атака шла из России, как было в случае с Эстонией и Грузией, власти страны, скорее всего, переложат вину на гражданских «хактивистов» и ничего им не сделают.

Сложность атрибуции может означать, что для определения взломщиков стране порой необходимо полагаться на традиционные методы разведки — шпионаж или полицейские методы. Обычная разведка, в отличие от компьютерной, не действует со скоростью, приближающейся к скорости света. Быстрое реагирование не всегда возможно. В стратегии ядерной войны атрибуция не считалась важной проблемой, поскольку мы всегда могли сказать,

 256

Как наступать?

откуда запущены ракеты или бомбардировщики. Кибератака похожа на взрыв бомбы. Если мы наблюдаем за развитием атаки, видя киберэквивалент стартовой шахты или авиабазы, мы сумеем определить происхождение атаки с большой степенью достоверности. Но если атака начинается на серверах в США, пройдет какое-то время до того момента, как президент скажет: мы знаем, кто атаковал нас. Насколько уверенными мы должны быть, прежде чем нанести ответный удар? Ответ, вероятно, будет зависеть от реальной ситуации в мире.

Э. Кризис неустойчивости

Ныне покойный Билл Кауфман однажды попросил меня написать доклад на тему «Предупредительный сигнал». Стратегическое командование ВВС считало: как только мы поймем, что Советский Союз готов совершить на нас ядерное нападение, мы должны направить на него как можно больше бомбардировщиков и запустить ракеты наземного базирования. Поскольку точность наведения советских ракет росла, они могли уничтожить даже те наши ракеты, которые хранятся в укрепленных подземных стартовых шахтах. Как и все прочее в доктрине ядерной стратегии, задача «запуска в случае их приближения» усложнилась. А что, если мы или наши средства обнаружения ошибаются? А если они атакуют, но малыми силами, направленными всего лишь на несколько целей? Нужно ли нам ответить всей своей мощью? По этой причине ВВС разработали стратегию «запуск при атаке», то есть приняли решение ждать, пока картина прояснится, пока боеголовки противника не взорвутся где-нибудь на нашей

257

9 № 4595

Третья мировая война: какой она будет?

территории. Переход к стратегии предупреждения всегда считался делом опасным, поскольку обострял нестабильность и взрывоопасность ситуации во время усиления напряженности. Если не принять правильное решение быстро, вы проиграете, но если принять решение быстро, оно может оказаться неправильным. В исследовании, которое я провел по заданию Кауфмана, я смог прийти к заключению о том, что у нас достаточно ракет на «море» и эти ракеты достаточно точны, так что мы можем пережить нападение, а затем принять рациональное решение, прежде чем развернуть ответные действия.

Подобная проблема существует и в кибервойне. Считается, что Соединенные Штаты способны узнать о приближении атаки, быстро пресечь ее и лишить противника возможности нападать снова. Такое предположение не всегда необоснованно. Если предположить, что стратегия США заключается в предвидении надвигающейся атаки и переходе к действиям, то действовать нужно быстро и не размышляя о том, кто враг и куда он собирается нанести удар. Промедление, скорее всего, выльется в два неблагоприятных для нас события:

® нападающая страна, вероятнее всего, поднимет мосты, то есть сразу же после запуска большой атаки Китай сможет отсоединиться от всего остального Интернета;

<Э нападающая страна может совершить атаку на сеть Интернет и телефонную инфраструктуру Соединенных Штатов, в связи с чем Америке сложно будет предпринимать ответные меры в киберпространстве.

Таким образом, первый удар может обеспечить преимущество нападающему и ведет к кризису нестабильно-

 25а

Как наступать?

сти, молниеносности и не дает времени на размышления. А теперь вспомните наш разговор о неопределенности намерений, о том, какого типа цели выбирает одна сторона в период подготовки поля боя. Если страна уверена, что противник разместил в ее инфраструктуре (включая компьютерные и энергетические сети) разрушительные программы и логические бомбы, то эти соображения, в сочетании с преимуществами первого удара, могут во времена усиления напряженности заставить тех, кто принимает решение, нажать на заветную клавишу зудящим пальцем.

1 □. Асимметрия обороны

В наших учениях победила китайская команда, которая заставила американцев отвести войска и пойти на переговоры, чтобы сохранить лицо. Главная причина их победы заключалась в том, что им удалось преодолеть оборону Соединенных Штатов и довольно эффективно воспользоваться собственной. США ждали атаки из-за океана, а китайцы использовали американские серверы, которыми, возможно, управляли китайские «студенты», сидя где-нибудь в кафе. Американцы искали сигнатуры известных атак, а китайцы использовали программы «нулевого дня». И самое главное, у США не было механизма обороны гражданской инфраструктуры, в которую входят финансовая индустрия, энергетическая сеть и система железных дорог.

Китай, с другой стороны, имел в своем распоряжении не только систему, с помощью которой можно было управлять всей инфраструктурой страны, но и план обороны.

259

Третья мировая война: какой она будет?

Когда стало ясно, что надвигается кибервойна, китайские энергетические системы и железные дороги перешли на несетевую систему управления. Когда китайцы лишились спутниковой связи, они за час ввели в эксплуатацию резервную радиосеть. Короче говоря, Китай не выкинул старые системы, а разработал план их дальнейшего использования.

\* \* \*

Уроки, которые мы извлекли, помогли нам определить проблемы и возможные варианты их решения, и мы приблизились к определению своей военной стратегии. Однако есть еще один отсутствующий элемент. Мы почти не обсудили международные законы войны и другие договоренности. Какие международные законы касаются кибервойны и какие дополнительные многосторонние соглашения были бы в наших интересах?

Глава V

КИБЕРМИР

С

оединенные Штаты практически в одиночку блокируют идею контроля над вооружениями в киберпространстве. Ее главным сторонником является, как ни странно, Россия. Учитывая дестабилизирующую природу и потенциальный ущерб кибервойны для США, о чем шла речь в предыдущих главах, можно подумать, что Соединенные Штаты давно должны были начать обсуждение международного соглашения о контроле над вооружениями, чтобы сократить риски.

 261

Третья мировая война: какой она будет?

На самом деле с тех пор как, администрация Клинтона первый раз отвергла предложение России, Соединенные Штаты выступали последовательным оппонентом контроля над кибевооружениями. Чтобы быть предельно откровенным, пожалуй, я должен признать, что это я отверг предложение России. Многие со мной согласились — мало какие решения американского правительства принимаются кем-то единолично. Однако в число моих функций в Белом доме во времена Клинтона входила координация политики кибербезопасности, включая международные и межправительственные соглашения. Несмотря на интерес Госдепартамента к проблеме контроля над кибервооружениями, мы сказали «нет». Я считал предложение России прежде всего инструментом пропаганды, чем десятилетиями и являлись все многосторонние инициативы подобного толка. Ратификация любого киберсоглашения казалась невозможной. Более того, Соединенные Штаты еще не выяснили, чем они намерены заниматься в сфере кибервойны. Было неясно, включать ее или нет в задачи национальной безопасности. Поэтому мы сказали «нет» и продолжаем говорить «нет» уже более десяти лет.

Теперь, когда вооруженные силы и разведывательные службы двадцати с лишним стран создали наступательные киберподразделения и мы стали лучше понимать, как может развиваться кибервойна, пожалуй, для США пришло время пересмотреть свою позицию по вопросу контроля над кибервооружениями и спросить, возможно ли добиться каких-то выгод посредством международного соглашения.

Z6Z

КИБЕРМИР

Краткий критический

АНАПИЗ КОНЦЕПЦИИ КОНТРОЛЯ
НАД ВООРУЖЕНИЯМИ

Приветствуете вы или нет пересмотр нашей позиции относительно ограничения кибевооружений, зависит от вашего мнения по поводу контроля над вооружениями в целом. Поэтому давайте для начала вспомним, что такое контроль над вооружениями (поскольку эта тема больше не обсуждается в новостях) и что уже сделано в данной сфере. Международные соглашения по контролю над вооружениями существовали и в доядерную эпоху, к примеру Вашингтонская конвенция об ограничении количества линкоров, заключенная еще до Второй мировой войны. Современная концепция контроля над вооружениями сформировалась во времена холодной войны между США и СССР. Эта концепция зародилась в начале 1960-х годов и развивалась на протяжении 30 лет, она стала главной заботой двух ядерных сверхдержав. Результатом стали два класса соглашений: многосторонние договоры, к которым помимо двух сверхдержав присоединялись другие страны мира, и двусторонние соглашения, в которых они уславливались накладывать особые ограничения на собственный военный потенциал.

В 1974 году в Вене я начал заниматься проблемами контроля вооружений, а затем на протяжении почти 20 лет работал над соглашениями о стратегических ядерных вооружениях, неядерных силах в Европе, так называемом демонстрационном ядерном оружии малого радиуса, биологическом и химическом оружии. На основе этого опыта сформировался мой взгляд на проблему контроля над кибервооружениями. Есть уроки, которые Соединенные Штаты могут извлечь из истории, если собираются

263

Третья мировая война: какой она будет?

ограничить приемы ведения войны в киберпространстве с помощью ряда новых соглашений.

Мой коллега Чарльз Дьюлфер, который на протяжении десятилетия направлял усилия ООН в вопросах ограничения иракского оружия массового поражения, скептически относится к американо-советскому опыту контроля над вооружениями и к данному явлению в целом. «США и СССР, как правило, соглашались запрещать то, на что бы они не пошли в любом случае. Что касается оружия, которое им было нужно, они устанавливали настолько высокий количественный максимум, что вольны были делать все, что хотели». Многие аналитики также критикуют концепцию контроля над вооружениями в целом. Они отмечают, что пятнадцатилетние переговоры по поводу размещения вооруженных сил в Европе закончились соглашением об ограничении численности вооруженных сил до того момента, как развалился Варшавский договор. Последнее соглашение позволило Советскому Союзу держать стотысячные войска в Восточной Европе, но это было уже не нужно. Тысячи советских танков вернулись назад в Россию не ради соблюдения условий соглашения. Более известные переговоры — ОСНВ и START — длились более 20 лет и позволили обеим сторонам хранить огромное множество единиц ядерного оружия и постоянно его модернизировать. В ходе этого процесса был заключен договор по противоракетной обороне, в котором обе сверхдержавы запретили противоракетную оборону, которая, по мнению обеих сторон, все равно оказалась бы неэффективной.

На многосторонней арене две сверхдержавы заключили договор, запрещающий другим странам обзаводиться ядерным оружием в обмен на неопределенное обещание, что остальные ядерные державы ликвидируют свое. Этот договор не остановил разработки ядерного оружия в Израиле, Пакистане, Индии, ЮАР и Северной Корее, как

264

КИБЕРМИР

сейчас едва ли останавливает Иран. Советский Союз согласился на многосторонний запрет на биологические оружие, но затем секретно продолжил развивать мощный биологический арсенал, что Соединенные Штаты обнаружили только десятилетия спустя. Критики называют нарушение Советским Союзом Договора о биологическом оружии примером того, почему контроль над вооружениями не всегда в интересах Соединенных Штатов. США обычно добросовестно соблюдают ограничения, на которые дали согласие, а многие другие страны — нет. Проверки не всегда выявляют нарушения, а разрешенная деятельность позволяет странам практически доходить до последней черты, но не дает оснований применять к ним санкции (как в случае с Ираном и его программой ядерной переработки).

Несмотря на проблемы контроля над вооружениями, следует признать, что двусторонние соглашения между США и СССР и более широкие многосторонние договоры сделали мир безопаснее. Даже если не принимать во внимание ограничение вооружений, само существование площадки, на которой американские и советские дипломаты и генералы обсуждали проблемы ядерной войны, помогло элитам обеих стран прийти к консенсусу о необходимости принимать меры для предотвращения этого бедствия. Использование каналов связи и мер по укреплению доверия, рост прозрачности вооруженных сил обеих стран сократили риск случайной или ошибочной войны.

Как помощник госсекретаря я обязан был контролировать одну из мер по укреплению доверия в соответствии с требованиями Американского центра снижения ядерного риска. Моим коллегой был российский генерал из Министерства обороны. Две наши группы работали над мерами по снижению вероятности напряжений, перераставших в состояние боевой ядерной готовности. У каждой

265

Третья мировая война: какой она будет?

группы был центр, мой в Госдепартаменте, у генерала из Министерства обороны — рядом в Красной площадью в Москве. Поскольку горячая телефонная линия Белый дом — Кремль использовалась редко, нам нужен был способ быстрой связи на случай недоразумений. Поэтому мы соединили наши центры спутниковой линией связи, установили телетайп для передачи текстовых сообщений и безопасные телефоны. В безопасных телефонах должен применяться секретный код, которым мы с Советским Союзом могли поделиться, но возникала проблема. И они и мы хотели использовать кодирование, не давая ключа другой стороне. Мы опасались электронного шпионажа: по мнению некоторых, при такой связи я давал возможность Советскому Союзу прослушивать разговоры американцев. Весь наш центр, расположенный в непосредственной близости к зданиям Госдепартамента США, необходимо было обшить медью и звукопоглощающим материалом.

Центры сокращения ядерного риска были созданы для предотвращения ошибочных обострений, которые происходили в первые годы холодной войны. Когда запуск в космос с авиационной платформы был прекращен в аварийном режиме, мы поняли, что на российских радарах падающая ракета может выглядеть как нападение, возможная цель которого — обезглавить советское руководство ударом по Москве. Я быстро связался с российским коллегой по безопасной линии. Эти линии использовались в подобных случаях, а также для координации выполнения договоров по контролю над вооружениями. Хоть договоры разрешали сохранять большие арсеналы на протяжении длительного времени, они запретили дестабилизирующую деятельность. Ограничения численности вооруженных сил позволяли сторонам знать их количественный состав, что предотвращало гонку вооружений, неизбежную, когда не известны намерения оппонента. И наконец, бла-

266

КИБЕРМИР

годаря настойчивости помощника президента по вопросам национальной безопасности Брента Скаукрофта обе стороны запретили дестабилизирующие ракеты наземного базирования с разделяющимися боеголовками. Теперь США и Россия проводят значительные сокращения своих стратегических сил. Договор о ядерных ракетах средней и малой дальности (РСНД), над которым я работал в начале 1980-х, обязал Соединенные Штаты ликвидировать мобильные станции баллистических ракет «Першинг II» и крылатые ракеты наземного базирования (GLCM) в обмен на уничтожение Советским Союзом сотен легко передислоцируемых ядерных ракет SS-4, SS-5 и SS-20.

Целый класс оружия, которое могло использоваться в ограниченных пределах, был навсегда запрещен, и несколько тысяч ядерных боеголовок выводили из эксплуатации. Ограничения ядерных испытаний начались со скромного запрета взрывов в атмосфере, но со временем привели к полному их запрету. (Полный запрет испытаний еще не ратифицирован американским сенатом.) Запрет химического оружия, над которым я работал в начале 1990-х, заставил страны уничтожить существующее химическое оружие, запретил создание нового и ввел очень навязчивый инспекционный режим контроля. (Хоть мы и не согласились на проверку «в любое время и в любом месте», лишь некоторые области не подлежат контролю.)

Помимо ограничений и запретов на ядерное, химическое и биологическое оружие контроль над вооружениями подразумевает ограничения на ведение войны. Ряд договоров о вооруженных конфликтах запрещает нападения на военные госпитали и гражданские учреждения, устанавливает стандарты обращения с военнопленными, налагает запрет на пытки, объявляет незаконными противопехотные мины, запрещает использование детей в военных действиях и объявляет геноцид международным престу-

267

Третья мировая война: какой она будет?

плением. Соединенные Штаты некоторые соглашения не ратифицировали (к примеру, запрет на противопехотные мины), некоторые недавно нарушили (запрет пыток). Во время Второй мировой войны происходили более грубые нарушения законов о вооруженных конфликтах, но даже тогда некоторые страны придерживались норм обращения с военнопленными. Когда контроль над вооружениями эффективен, он уменьшает неопределенность, создавая более предсказуемую безопасную среду. Объявляя некоторые действия незаконными и запрещая некоторые виды оружия, эти соглашения помогают понять возможные намерения другой стороны. Если страна готова нарушить соглашения, устраняется двусмысленность ее политического курса. Запрет определенных вооружений и действий помогает государствам избежать расходов, на которые пришлось бы пойти из страха, что другие делают то же самое. Согласованные международные нормы полезны при необходимости объединиться против третьей стороны.

Контроль над вооружениями не ценен и даже не полезен в том случае, когда он носит увещевательный характер, когда переговоры становятся платформой для пропаганды, когда ограничения расплывчаты, а нарушения ничем не грозят нарушителю. Если страна может быстро перейти от соблюдения к существенному нарушению, стабильность и предсказуемость утрачиваются. Если страны могут нарушать соглашения, не рискуя быть обнаруженными или не опасаясь возможных карательных санкций, соглашения получаются односторонними и доверие к ним теряется.

В целом я считаю, что наш тридцатилетний опыт контроля над вооружениями во многом позитивен, но далеко не всегда он был панацеей и порой превращался в фарс. Чтобы определить, созрела ли та или иная сфера для контроля над вооружениями, нужно проверить, действитель- 26В

КИБЕРМИР

но ли обе стороны заинтересованы сократить инвестиции в нее. Если одна из сторон предлагает прекратить то, что на самом деле хочет продолжать, скорее всего, она собирается участвовать в контроле над вооружениями ради пропаганды или обманным путем старается ограничить потенциального противника в области, в которой, по ее мнению, ее могут превзойти.

Ограничить кибервойну?

Все это снова возвращает нас к кибервойне. Чтобы определить нашу государственную политику по отношению к контролю над кибервооружением или ограничениям в сфере киберактивности, мы прежде всего должны спросить себя, дает ли это новая форма ведения войны такие преимущества США перед другими странами, поскольку нам бы не хотелось испытать какое-либо международное давление. Если мы считаем, что обладаем таким односторонним преимуществом, нам не стоит задавать себе вопросы о том, какого рода ограничения можно установить, возможен ли контроль над их соблюдением и т. д. Ранее я выдвинул предположение о том, что для США было бы лучше, если бы кибероружие никогда не существовало, учитывая все наши уязвимые места. Прежде чем обратиться к теме кибервоенного контроля, давайте рассмотрим четыре фактора, в силу которых мы более уязвимы, чем страны, способные использовать кибероружие против нас.

Во-первых, сейчас Соединенные Штаты больше зависят от киберуправляемых систем, чем наши вероятные противники. Одни страны, такие как Южная Корея или Эстония, возможно, больше используют Интернет для по- 269

Третья мировая война: какой она будет?

купок. Другие, допустим Арабские Эмираты, имеют больше мобильных интернет-устройств на душу населения. Но нигде компьютерные сети так широко не используются для управления энергетическими сетями, трубопроводами, авиалиниями, железными дорогами, распределением потребительских товаров, банковской системой и работой военных подрядчиков.

Во-вторых, лишь в некоторых странах (среди которых, пожалуй, нет наших потенциальных противников) важнейшие национальные системы принадлежат и управляются частными компаниями.

В-третьих, нет других таких промышленно и технологически развитых стран, в которых владельцы и управляющие частных компаний обладают достаточным политическим весом, чтобы предотвращать или ослаблять государственное регулирование своей деятельности. Американская политическая система основана на хорошо финансируемом лоббировании и добровольном финансировании политических кампаний, и частные промышленные группы обладают в ней большой властью, особенно когда дело касается попыток государственного регулирования.

В-четвертых, американские военные весьма уязвимы перед кибератакой. Вооруженные силы США сетецен- тричны, то есть доступ возможен к базам данных и далее к управлению любой военной организации. Вместе с доступом к информационным системам появилась и зависимость от них. Маленьким предвестником грядущих проблем стали события конца 2009 года. Иракские повстанцы использовали для наблюдения за источниками видеосигнала американских беспилотных самолетов Predator через незашифрованные каналы связи программу стоимостью 26 долларов. Хоть это напрямую и не угрожало американским войскам, обнаружение проблемы подняло

27D

КИБЕРМИР

ряд вопросов об излюбленном новом оружии Пентагона. А что, если бы кто-нибудь создал помехи в незашифрованном сигнале, заставив беспилотный самолет вернуться домой? Американские военные лишились бы одного из самых ценных инструментов, а дешевая готовая программа превзошла бы продукт, в исследования и разработку которого вложены миллионы долларов. Вооруженные силы США помимо зависимости от сетей больше зависят и от частных подрядчиков, чем любой вероятный противник. Даже если сети военных были бы защищенными и надежными, подрядчики, которые часто полагаются на общедоступный Интернет, этим могут похвастаться не всегда. Все эти асимметрии, взятые вместе, говорят о том, что если бы мы начали кибервойну, противник нанес бы нам больший ущерб, чем мы ему. При таких асимметричных уязвимостях некоторые эффективные ограничения возможных действий противника отвечают интересам США. Однако чтобы перевести теорию в практику, потребуется определить, какого рода деятельность должна быть разрешена, а какая запрещена.

Нередко в переговорах о контроле над вооружениями сложно достичь соглашения по поводу самых основ, например, что именно мы хотим ограничивать. Я месяцами сидел за столом переговоров со своими советскими коллегами, пытаясь дать определение понятию «военный персонал». Здесь нам не нужны такие промедления. Давайте примем определение, использованное мною в первой главе, но сформулируем его на языке договоров: «Кибервойна — это несанкционированное проникновение, предпринятое правительством, по его поручению или при его поддержке, в компьютерную сеть другой страны или любая другая воздействующая на компьютерную систему деятельность, цель которой — добавить, изменить, фальсифицировать данные или вызвать нарушение ра- 27 1

Третья мировая война: какой она будет?

боты или повреждение компьютера, сетевого устройства или объектов компьютерных систем управления».

Учитывая это определение и асимметричные уязвимости США, рассмотрим, можно ли применить к киберпространству успешный опыт контроля над другими формами вооружений или нужны новые идеи, применимые только к данной сфере, чтобы сформировать базис для контроля над кибервооружениями? На какие просчеты прошлого мы должны обращать особое внимание, думая об ограничениях кибероружия? Какие международные соглашения, ограничивающие некоторые аспекты кибервойны, были бы выгодными для США, а также выполнимыми и поддающимися адекватной проверке?

Граница... шпионаж ипи война?

Любое возможное международное соглашение об ограничении или контроле над кибервооружением должно начинаться с определения рамок. Что оно охватывает и что обходит вниманием? В определение кибервойны, которое я привел выше, не входит кибершпионаж. Грамотный хакер, проникающий в сеть с целью сбора информации, не добавляет и не изменяет данные, не стремится повредить или вывести из строя сеть или физические объекты, которыми управляют из киберпространства.

Однако же российское предложение о контроле над кибервооружениями имеет очень широкие рамки и предусматривает запрет того, чем Российская Федерация занимается каждый день, — шпионажа посредством хакерства. Главный пропагандист российского предложения Владислав Шерстюк в прошлом руководил работой хакеров. Будучи директором ФАПСИ, генерал Шерстюк был

 Z7Z

КИБЕРМИР

коллегой директора Агентства национальной безопасности США. Его карьерный опыт не обязательно означает, что генерал Шерстюк неискренен в своем стремлении запретить то, чем он долгие годы занимался. Технические различия между кибершпионажем и деструктивной кибервойной настолько минимальны, что, возможно, генерал Шерстюк считает, что четкую грань провести невозможно. Или же он пересмотрел свои взгляды. Может быть, он полагает, что кибершпионаж ставит Россию в невыгодное положение. Однако, вероятнее всего, генерал, как и все, кто видел кибершпионаж в действии, с большой неохотой согласился бы отказаться от него.

Кибершпионаж, с одной стороны, значительно проще традиционного шпионажа. Сложно преувеличить, как трудно завербовать надежного шпиона и внедрить его в организацию, чтобы он (или она) смог копировать и прорабатывать существенные объемы ценной информации. К тому же всегда есть опасения, что предоставленный материал сфальсифицирован, а шпион является двойным агентом. Лучшие операции контрразведки всегда начинались с предположений о том, куда противник мог внедрить своих шпионов, после чего с ними выходили на контракт. Агент отсылал не самые важные данные, добавлял кое- какие сфальсифицированные материалы, вследствие чего сведения становились как минимум бесполезными.

Как я проанализировал в книге «Ваше правительство подставило вас» (Your Government Failed You), Соединенные Штаты не особенно сильны в использовании шпионов, или, как называют американцы, «разведке людьми». Причины этого в сложности задачи, нашем нежелании доверять людям, которые могли бы стать хорошими шпионами, нежелании многих американцев становиться внедренными агентами и способности других стран обнаруживать наши попытки шпионажа. Эти особенности глубоко укоренились

10 №4595

Z73

Третья мировая война: какой она будет?

и обусловлены культурой, они подтверждались шестьдесят с лишним лет и вряд ли изменятся.

Но мы необыкновенно сильны в электронном шпионаже. По сути, наши способности в кибершпионаже компенсируют несостоятельность традиционной разведки. Таким образом, если заставить Соединенные Штаты отказаться от кибершпионажа, это значительно снизит наши возможности сбора данных и поставит нас в невыгодное положение по сравнению с другими странами.

Идея ограничить кибершпионаж требует разобраться, почему к нему не следует прибегать и какие проблемы должен решить его запрет. Хотя Генри Стимсон, госсекретарь при президенте Герберте Гувере, сумел приостановить шпионаж на том основании, что «джентльмены не читают чужие письма», американские президенты в большинстве своем считали сбор разведывательных данных немаловажной основой обеспечения национальной безопасности. Знания — сила. Шпионаж — способ овладения знаниями. Народы шпионят друг за другом как минимум с библейских времен. Знание о возможностях другой страны и о том, как они ведут себя за закрытыми дверями, как правило, способствует стабильности. Необдуманные заявления о противнике приводят к гонке вооружений. Шпионаж избавляет от подобных рисков, как было в 1960- м, когда обсуждался вопрос про «отставание по ракетам», суть которого заключалась в том, что советской ракетный арсенал существенно превосходит наш. Первые американские спутники-шпионы помогли рассеять эти сомнения. Шпионаж предотвращает сюрпризы и необходимость пребывать в состоянии боевой готовности, держать палец на спусковом крючке, постоянно ожидать неожиданностей. И все же существуют некоторые существенные различия между традиционным и кибершпионажем, на которые, вероятно, стоит обратить внимание.

 ZV4

КИБЕРМИР

Во время холодной войны Соединенные Штаты и Советский Союз тратили миллиарды на шпионаж друг за другом. Мы очень старались, как и они, вербовать шпионов из тех, кто имел доступ к государственным тайнам, чтобы знать об их намерениях, возможностях и слабостях. Иногда нам это удавалось и мы пожинали богатый урожай, но чаще мы терпели неудачу. Эти провалы нередко имели разрушительные последствия. В конце 1960-х годов американские попытки шпионажа против Северной Кореи дважды чуть не привели к конфликту. В январе 1968 года северокорейским флотом был захвачен Pueblo — разведывательный корабль ВМС США вместе с 82 членами экипажа. Одиннадцать месяцев, до освобождения экипажа, войска на Корейском полуострове пребывали в состоянии высокой боевой готовности, опасаясь вооруженного конфликта. Спустя пять месяцев после освобождения экипажа у побережья Северной Кореи был сбит ЕС-121 — разведывательный самолет ВВС США, погиб 31 член команды (что любопытно, это произошло в день рождения северокорейского лидера Ким Ир Сена). Президент Соединенных Штатов Ричард Никсон предполагал провести ответную бомбежку, но шли боевые действия во Вьетнаме, и он решил повременить, иначе бы в Азии развязалась еще одна война. Через семь месяцев подводная лодка ВМФ США, проводившая операцию в территориальных водах Советского Союза, столкнулась с советской подлодкой. Шесть лет спустя Сеймур Херш докладывал: «Американская субмарина Gato выполняла особо секретную разведывательную миссию в рамках программы Holystone, когда примерно в 15-25 милях от входа в Белое море произошло столкновение с советской подводной лодкой». Как пишет Питер Сасген в своей замечательной книге «Выслеживая медведя» (Stalking the Bear), «операция Holystone состояла из нескольких мис- 275

Третья мировая война: какой она будет?

сий, которые выполнялись на всем протяжении холодной войны и охватывали все, начиная с записи акустических сигналов советских подлодок и заканчивая перехватом сообщений, передаваемых по электронным средствам связи, и видеозаписью испытаний разного оружия». Оба эти инцидента могли привести к реальному и опасному конфликту.

В начале 1992 года я был помощником госсекретаря США, и мой начальник, госсекретарь Джеймс Э. Бейкер, участвовал в непростых переговорах с Россией о контроле над вооружениями и окончании холодной войны. Бейкер полагал, что ему удалось преодолеть чувство поражения и паранойю, царившие в руководстве и военной элите в Москве. Он рассчитывал укротить опасения, воспользовавшись преимуществами развала Советского Союза. Но 11 февраля американская атомная подводная лодка Baton Rouge столкнулась с «Костромой» (субмариной класса Sierra) недалеко от побережья Североморска. Возмущенные русские обвинили американцев в сборе разведывательных данных на российской территории.

Помню, в какой ярости был Бейкер, требуя ответа, кто в Госдепартаменте санкционировал миссию Baton Rouge и какую ценность имели бы ее результаты в сравнении с ущербом, принесенным ее раскрытием. Бейкер срочно выступил с дипломатической миссией, обещая своему коллеге Эдуарду Шеварнадзе, что США отказываются от любых подобных операций в будущем. Американская Baton Rouge с большими повреждениями вернулась в порт и вскоре была списана и переведена в резерв. Те, кто в Москве заявлял, что Америка их дурачит, получили подтверждение. Недоверие, которое хотел прекратить Бейкер, только возросло.

Мы не должны считать кибершпионаж просто новым методом перехвата. Кибершпионаж во многих отноше-

 276

КИБЕРМИР

ниях значительно проще, дешевле, эффективнее традиционного шпионажа, к тому же он имеет меньше последствий. А значит, больше стран будут шпионить друг за другом и смогут сделать больше, чем было бы при иных обстоятельствах. До появления кибершпионажа имелись физические пределы того, сколько информации может выкрасть шпион, и по причине возможных разрушительных последствий в некоторых сферах существовали ограничения доступа к информации. Случай с истребителем F-35 (о котором упоминается в пятой главе) демонстрирует, что количественный аспект с появлением кибершпионажа изменился настолько, что считать последний просто новым методом перехвата нельзя. Скорость, объем и глобальный охват киберактивности обусловливают фундаментальное и качественное отличие кибершпионажа от всего, что было ранее. Давайте еще раз вернемся к примеру с F-35 и посмотрим почему.

F-35 — истребитель пятого поколения, разработанный на Lockheed Martin. Предполагалось, что F-35 будет отвечать современным требованиям ВМФ, ВВС и морской пехоты и заменит устаревшие F-16 и F-18. Самое главное преимущество F-35 по сравнению с истребителями четвертого поколения — его электронное «умное» оружие. Грузоподъемность F-35 ниже, чем у предшественников, поскольку он должен функционировать по принципу «один выстрел, одно попадание» благодаря усовершенствованным системам наведения. ВВС, ВМФ и морская пехота вместе заказали почти 2,5 тысячи этих самолетов общей стоимостью более 300 миллиардов долларов. Страны НАТО также решили приобрести этот истребитель. F-35 будет обеспечивать превосходство над любым возможным противников на протяжении ближайших 30 лет. Но это превосходство может быть оспорено, если враг найдет способ взломать его компьютеры.

277

Третья мировая война: какой она будет?

В апреле 2009 года кто-то проник в системы хранения данных и скопировал терабайты ценной информации, связанной с разработкой F-35. Украденная информация имела отношение к чертежам самолета и его электронным системам, хотя никто не может точно сказать, какие именно данные были похищены, поскольку хакеры замели следы, зашифровав информацию, прежде чем ее скопировать. Согласно заявлениям некоторых должностных лиц из Пентагона, доступ к самой важной секретной информации невозможен, поскольку она хранится не в сети. По их уверенным заявлениям, следы проникновения ведут на IP- адрес в Китае, а сигнатура атаки указывает на причастность китайского правительства. Это не первый случай успешного взлома программы F-35. Кража данных по F-35 началась в 2007 году и продолжилась в 2009-м. По сообщениям, было украдено несколько терабайтов информации. Давайте предположим, что это был один терабайт. Итак, сколько же было украдено? Примерно десять экземпляров «Британской энциклопедии» — 32 тома, 44 миллиона слов, помноженные на десять.

Если бы во времена холодной войны шпион захотел выкрасть столько информации из секретного учреждения, ему потребовался бы небольшой фургон для перевозки мебели и погрузчик. К тому же ему пришлось бы рисковать собственной свободой и жизнью. Роберт Ханссен, сотрудник ФБР, который с 1980-х годов шпионил на Советский Союз, а затем на Россию, не выкрал столько информации за всю свою двадцатилетнюю карьеру. Он тайно выносил документы из штаб-квартиры ФБР, заворачивал их в полиэтиленовые пакеты и оставлял в тайниках неподалеку от своего дома в Вирджинии. В общей сложности Ханссен выкрал не более нескольких сотен страниц документов.

Теперь Ханнсен проводит 23 часа в день в одиночной камере тюрьмы Supermax в Колорадо-Спрингс. Ему за-

 27В

КИВЕРМИР

прещены переписка, посещения, телефонные разговоры, а тюремщики называют его просто «заключенный» и говорят о нем в третьем лице («заключенный готовится на выход из камеры») Но Ханссену сохранили жизнь. По крайней мере трое россиян, которые работали на Американское разведывательное сообщество и были сданы Ханс- сеном, убиты русскими, а четвертый посажен в тюрьму. Шпионаж всегда был опасным делом для шпионов. Теперь все иначе.

Шпионам, выкравшим информацию о F-35, не нужно было вербовать того, кто смог бы предать страну и предоставить им доступ к нужным данным, они не рисковали, что их поймают и посадят в тюрьму или того хуже. Однако украденная информация позволит найти слабые места в схеме или системах F-35. Возможно, они обнаружат уязвимые места нового вида кибероружия, которое будут использовать в будущей войне, чтобы лишить нас превосходства в воздухе превосходством в киберпространстве. И это еще не самый худший сценарий. А что, если, пока хакеры, находясь в наших системах и собирая информацию, загрузили туда пакет программ? Возможно, чтобы подготовить «черный ход» для доступа в сеть, когда их первоначальный путь выследят и закроют. Или разместить логические бомбы, которые в случае необходимости разрушат сеть Пентагона. Шпионаж от саботажа отделяет всего лишь несколько щелчков мышкой. Кем бы они ни были, возможно, сейчас они внедряются в наши системы просто для сбора информации, но имеющийся доступ позволяет им повредить или разрушить наши сети. Так что знание о том, что наши сети кто-то посещал, чтобы «просто пошпионить», может дать Пентагону и президенту повод потянуть время во время следующего кризиса.

Эффективно запретить кибершпионаж было бы нелегко. Определить, какая страна занимается кибершпи- 279

Третья мировая война: какой она будет?

онажем, практически невозможно. Методы, которые используют сейчас США и Россия, как правило, невыяв- ляемы. Даже если бы у нас были средства обнаруживать самые изощренные формы проникновения в сеть, было бы чрезвычайно сложно доказать, кто сидел за клавиатурой на другом конце оптоволокна и на кого он работает. Если бы мы согласились заключить договор, запрещающий кибершпионаж, американские агентства, вероятно, прекратили бы такую деятельность, но очень сомнительно, что так же поступили бы другие страны.

Используемые нами способы сбора информации, включая кибершпионаж, порой оскорбляют чьи-то чувства и нарушают международные и государственные законы, но за некоторыми примечательными исключениями американская шпионская деятельность в целом необходима и полезна для США. Более того, убеждение в необходимости шпионажа широко распространено среди американских экспертов по национальной безопасности и законодателей. Когда я занимался контролем над вооружениями, я всегда задавал своим подчиненным вопрос: «Когда придет время давать показания в пользу ратификации этого соглашения, как вы объясните американскому сенату, каким образом вы пришли именно к таким положениями? Как я должен объяснять, почему мы договорились об этом?» Если бы мне пришлось выступать по вопросу ограничения шпионажа, я не знал бы, с чего начать. Поэтому, размышляя о российском предложении запретить кибершпионаж, я не перестаю удивляться, почему они выдвинули его и что это говорит об их намерениях и целях пропаганды кибервоенного договора. Предложение запретить кибершпионаж поступило из страны с очень высоким уровнем мастерства в данной деятельности, из страны, которая регулярно организует кибероперации против других государств, едва ли не хуже всех ведет междуна- 280

КИБЕРМИР

родную борьбу с киберпреступностью и не подписала ни одного серьезного международного соглашения о разрушительной киберактивности (Конвенцию о киберпреступности Совета Европы).

Отвергая предложенное Россией международное соглашение о запрещении кибершпионажа, я сознаю, что кибершпионаж действительно может быть разрушительным, провокационным и даже дестабилизирующим. Как сказал мне бывший директор АНБ Кен Минихэн, «мы ведем военные действия, не думая о том, что это война». Это опасно, но есть и другие поводы для беспокойства. На протяжении всей холодной войны ЦРУ и КГБ тайно встречались и устанавливали «правила дорожного движения». Обе страны обязались не убивать агентов друг друга. Определенные вещи были вообще запрещены. Нечто подобное можно использовать и в кибершпионаже. Государства должны сознавать, что шпионаж легко может быть принят за подготовку поля боя, и тогда подобные действия сочтут провокационными. Государства не должны делать в киберпространстве то, чего они не стали бы предпринимать в реальном мире. Если бы вы не стали отправлять группу агентов куда-нибудь для добычи информации, надеясь выкрасть ее через сеть, возможно, не стоит этого делать и электронным способом.

Поскольку разница между добыванием данных и саботажем невелика, страны должны очень внимательно относиться к тому, в какие сферы киберпространства они внедряются и что предпринимают. В то время как шпионаж, целью которого являются государственные системы, может выйти из-под контроля, настоящими драгоценностями американской короны являются не государственные тайны, а наша интеллектуальная собственность. Американские акционеры и налогоплательщики тратят миллиарды долларов на финансирование исследова- 2S 1

Третья мировая война: какой она будет?

ний. Китай крадет результаты, тратя один цент на наш миллиард, а затем выводит продукт на рынок. Главная экономическая мощь Соединенных Штатов, мастерство в технологических исследованиях, исчезает в результате кибершпионажа. Преступление остается преступлением, пусть даже мы называем его кибершпионажем. Вторжение в коммерческие организации по всему миру для кражи незащищенных данных повышает доходы Китая, и Пекин давно уже превратился в столицу клептократии глобального масштаба. Даже если крупной кибервойны с участием Соединенных Штатов никогда не будет, китайский кибершпионаж и война за интеллектуальную собственность могут сместить политическое равновесие в мире не в пользу Америки. В первую очередь мы должны защитить информацию и противостоять активности Китая в данной сфере.

Если определенные виды дестабилизирующего кибершпионажа будут иметь последствия, государства смогут более жестко контролировать, кто, почему и где им занимается. Большинство чиновников не жаждут объяснять разъяренному госсекретарю или министру, почему считалось, что разведывательная ценность раскрытой секретной операции перевесит вред, причиненный ее обнаружением. Таким образом, хоть я и признаю, что в кибершпионаже игра порой не стоит свеч, я считаю, что риск проведения разведывательных операций должен определяться спецслужбами совместно с властями в двустороннем закрытом режиме. Соглашение о контроле над вооружениями, ограничивающее кибершпионаж, не в полной мере соответствует нашим интересам, может регулярно нарушаться другими странами и ставит перед нами ряд серьезных проблем, связанных с его соблюдени- ем/принудительным применением.

2SZ

КИБЕРМИР

Запретить кибервойну?

Стоит ли соглашаться на полный запрет кибервойны (за исключением кибершпионажа)? Полный запрет теоретически мог бы воспрепятствовать разработке и приобретению кибероружия, но обязать или проверить соблюдение этого запрета невозможно. Можно сформулировать запрет на использование кибероружия против определенных объектов или размещение оружия до начала военных действий, а не на обладание им и использование в шпионаже. Чтобы оценить, отвечает ли запрет кибервойны нашим интересам, предположим, что он принят, и рассмотрим некоторые гипотетические прецеденты.

Представим сценарий, аналогичный израильскому налету на сирийскую ядерную установку, с которого началась эта книга. Слегка изменим его — пусть это США хотят остановить развитие ядерного оружия в неконтролируемой стране и решают сбросить бомбу на то место, где собираются производить ядерное оружие. США наверняка обладают возможностью выключить радары ПВО противника с помощью кибероружия. Если бы мы согласились бы запретить использование кибероружия, перед нами встал выбор: посылать американских пилотов, не сделав все, что в наших силах, чтобы их защитить, или нарушить международное соглашение. Мало кто из гражданского и военного руководства страны вызовется потом объяснять, почему были сбиты американские самолеты, почему пилоты попали в тюрьму или были убиты, ведь мы могли отключить противовоздушную оборону противника.

Представьте, что США уже участвуют в ограниченном вооруженном конфликте с некой страной, как в недавнем прошлом с Сербией, Ираком, Панамой, Гаити, Сомали и Ливией. Американские вооруженные силы оказываются в ситуации, в которой традиционное оружие они могут за-

 ZB3

Третья мировая война: какой она будет?

менить кибернетическим. Кибероружие приносит меньше смертей и физических повреждений и имеет менее продолжительные последствия. Полный запрет на использование кибероружия снова заставит Соединенные Штаты выбирать между нарушением соглашения и нанесением излишнего вреда противнику.

Рассмотрим еще более простой сценарий, без вооруженного конфликта или упреждающего удара: американский корабль мирно ходит в международных водах. И вот на этот эсминец, идущий параллельно северокорейскому побережью, нападает северокорейский патрульный катер, запуская ракеты. Если бы американский корабль использовал кибероружие, он мог бы вторгнуться в систему управления приближающихся ракет и заставить их отклониться. А при существовании полного запрета на использование кибероружия американцам, возможно, нельзя будет применять его для защиты своих сил от неспровоцированной атаки.

Сложнее всего сохранить сдержанность в том случае, если кибероружие уже использовали против нас. Когда противник попытается вывести из строя американскую военную сеть или систему вооружения, у наших военных появится большое искушение проигнорировать международное соглашение и ответить тем же.

Итак, «за» и «против» полного запрета на использование кибероружия ясны. Если мы действительно считаем, что такой запрет в наших интересах, нужно быть готовыми заплатить некоторую цену за поддержание такого международного стандарта. В прошлом были ситуации, когда мы могли воспользоваться военным превосходством, используя ядерное, химическое или биологическое оружие, но решали, что для США важнее соблюдать международное решение и не применять его. Тем не менее, поскольку кибероружие не столь смертоносно, запрет на

 284

КИБЕРМИР

его использование в условиях вооруженного конфликта, пожалуй, будет сложно оправдать. Если боевые действия уже начались, использование кибероружия не обязательно приведет к дестабилизации и эскалации. Американские военные приведут доводы (притом сильные) о том, что технологические преимущества компенсируют довольно неравномерное распределение наших вооруженных сил в мире и изощренность обычного оружия, которое может оказаться в руках наших потенциальных противников.

Чтобы уравновесить наше желание сохранить военную гибкость и необходимость учитывать тот факт, что кибервойна способна нанести существенный ущерб Соединенным Штатам, можно было бы ввести международные ограничения без полного запрета. Соглашение, в котором без всяких оговорок запрещается использовать кибероружие, — это самая крайняя форма запрета.

В предыдущей главе мы вкратце рассмотрели концепцию ненападения — менее масштабный вариант. Соглашение о ненападении может быть как серией взаимных деклараций, так и обстоятельным международным договором. Почему бы не сконцентрироваться на предотвращении развязывания войны посредством кибератак, а не на ограничении использования кибероружия, когда конфликт уже начался? Такое обязательство могли бы взять на себя все страны или только те, которые сделали аналогичное заявление или подписали соглашение. Заявление о ненападении — это больше чем дипломатический призыв. Существование данного обязательства может снизить вероятность того, что какая-либо страна инициирует использование кибероружия, поскольку тем самым она нарушает международную норму. Страна, которая применяет кибероружие первой и нарушает договор, компрометирует себя в глазах мировой общественности и совершает неправомерные действия. Возможность междуна- [[103]](#footnote-104)

Третья мировая война: какой она будет?

родной поддержки этой страны в конфликте снижается, а вероятность международных санкций возрастает.

Декларация о ненападении может снизить гибкость многих сценариев, подобных тем, что я обсуждал выше. Пока мы ждем повода нанести ответный удар после использования противником кибероружия, мы ставим себя в невыгодное положение в кибервоенной фазе конфликта.

Запрет атак на гражданское

НАСЕПЕНИЕ?

Есть не столь ограничивающие подходы, как запрет на использование кибероружия или отказ от ненападения. Один из возможных вариантов — принятие односторонней декларации или международного протокола о запрете атак на гражданские объекты. В международном военном праве была масса подобных прецедентов — запрещалось использование определенных вооружений или действий, заключались соглашения, обязывающие защищать гражданское население, вовлеченное в войну.

Во время Первой мировой войны в сражениях впервые использовались самолеты. Они главным образом применялись в целях разведки, в пулеметных обстрелах войск противника, воздушных боях, но некоторые самолеты сбрасывали бомбы на врага. Это первое использование авиабомб открыло перспективы создания самолетов, способных в будущем взять на борт больше бомб. В следующее десятилетие появилась бомбардировочная авиация. Один из первых писателей-фантастов Герберт Уэллс в романе 1933 года «Грядущие события» описал, во что такая авиация способна превратить город. К 1936 году он написал на основе книги сценарий, а кинорежиссер Алек- 2В6

КИБЕРМИР

сандр Корда снял фильм, который шокировал зрителей. 1938 году в Амстердаме участники международной конференции согласились ограничить «новые машины войны». На основе этого соглашения в том же году была заключена Конвенция о защите гражданского населения от бомбардировок с воздуха.

К сожалению для Амстердама и большинства других крупнейших городов Европы и Азии, эта конвенция не остановила Германию, Японию, Соединенные Штаты, Великобританию и Советский Союз, использовавших ковровые бомбардировки городов в войне, которая началась год спустя. После Второй мировой страны мира предприняли очередную попытку и подписали несколько соглашений, ограничивающих условия ведения будущей войны. Эти договоры, заключенные в Швейцарии, получили название Женевских конвенций. Четвертая конвенция посвящена защите гражданского населения во время войны. Тридцать лет спустя Организация Объединенных Наций поддержала еще одну серию соглашений. Согласно им не только гражданские лица, но и военный персонал должны быть защищены от определенных видов оружия, которое считается бесчеловечным. Конвенция получила громоздкое название Конвенция о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие. Было подписано пять протоколов, запрещающих или ограничивающих использование осколочного и зажигательного оружия, противопехотных мин и мин-ловушек, согласно дополнительному протоколу запрещается также использование лазерного оружия.

Не так давно (в 2002 году) Международный уголовный суд запретил использование гражданского населения в качестве военной цели. Соединенные Штаты вышли из до- 287

Третья мировая война: какой она будет?

говора и добились соглашения со многими странами о том, что они не станут оказывать поддержку судебным преследованиям американских военных. В Женевскую конвенцию о защите гражданского населения или конвенцию ООН об оружии с «непредсказуемыми последствиями» можно добавить и новый вид военных действий. Кибероружие, используемое против инфраструктуры страны, неминуемо оказывает разрушительное воздействие на гражданские системы. Нет ничего более непредсказуемого, чем атака на энергетическую или транспортную систему. Если такие масштабные нападения и снижают военный потенциал страны, он, скорее всего, страдает меньше, чем гражданская инфраструктура. У военных наверняка есть вспомогательные энергосистемы, запасы еды, полевые госпитали. Масштабная кибератака на инфраструктуру страны может вывести из строя электросети на недели, нарушить работу газо- и нефтепроводов, направить поезда на запасные пути, запретить полеты, помешать банкам выдавать наличные, запутать системы поставок, ограничить возможности больниц. Гражданское население может остаться без света, тепла, пищи, денег, медицинского обслуживания и новостей о происходящем. В результате возрастет уровень преступности и начнется мародерство. Масштаб бедствий будет зависеть от продолжительности и территориальных масштабов энергетической катастрофы. Хотя последствия окажутся намного менее плачевными, чем при бомбардировке городов с воздуха, изощренная кибератака определенно затронет гражданское население, а возможно, с этой целью и будет проводиться.

Расширение существующих международных соглашений в целях защиты гражданского населения от кибератак выгодно для Соединенных Штатов. Это позволит США продолжить заниматься тем, что у нас хорошо получается — вести кибервойну против военных объектов,

ZBB

КИВЕРМИР

включая концепцию первого удара. Высокотехнологичное кибероружие, вероятно, позволит США сохранять технологическое превосходство в потенциальных военных конфликтах, даже если другие страны смогут использовать современное обычное оружие, практически равное по мощности американскому. Кибероружие, наверное, поможет США компенсировать численное превосходство противника в локальных и региональных боевых действиях.

Для США запрет атаки на гражданские объекты будет означать, что ликвидация вооруженных сил противника не будет побочным эффектом генерального кибернаступления на гражданскую энергосистему или систему железных дорог. Возможно, что американские кибервоины смогут атаковать непосредственно военные объекты — сети управления и контроля, системы ПВО, конкретные системы вооружения. Таким образом, выполняя запрет на атаку гражданских объектов, США не потеряют своих мощностей, необходимых для победы над противником.

Соединенные Штаты, как и другие страны, не слишком хороши в киберобороне, но американская гражданская инфраструктура более уязвима, и поэтому в случае крупной кибератаки США понесут больше потерь, чем другие страны. Поскольку американские военные зависят от гражданской инфраструктуры, запрет кибератак на гражданские цели защитит и американских военных, а также поможет избежать нанесения вреда населению в целом и экономике.

Предположим, Соединенные Штаты считают, что такой ограничительный запрет на кибероружие отвечает их интересам, и готовы подписать или внести соответствующее предложение — тогда сразу возникают два вопроса. Во-первых, как мы собираемся контролировать соблюдение этого запрета? И во-вторых, что делать с «подготовкой поля боя»? Является ли атакой проникновение в сеть

 289

Третья мировая война: какой она будет?

и размещение логической бомбы или только использование логической бомбы и другого оружия? То есть какие свои действия мы готовы приостановить?

Ранее мы пришли к выводу о том, что формальное международное соглашение, запрещающее кибершпионаж, пожалуй, не лучшая идея для Соединенных Штатов. Следовательно, нам не имеет смысла запрещать проникновение в сети для сбора разведывательных данных, например в сети системы управления железными дорогами. Но какова ценность разведывательной информации, добытой из системы управления электросетями? Внедрение в управление электросетями и оставленные там «черные ходы» имеют единственную цель — подготовиться к атаке. Логические бомбы — еще более очевидное проявление кибервойны. Теоретически можно запретить кибератаку на гражданскую инфраструктуру, не запрещая в явном виде размещение лазеек и логических бомб, но не лучше ли наложить запрет на любые действия, которые могут послужить причиной разрушений? Такой узконаправленный запрет позволит США, в случае атаки на нашу гражданскую инфраструктуру, быстро ответить противнику тем же. При данном подходе атаковать чужие сети без заблаговременного размещения кибероружия было бы сложно и трудоемко. Но если мы позволим странам размещать логические бомбы в сетях друг друга, то лишимся главной ценности, которую несет в себе запрет на кибератаку гражданской инфраструктуры. Главная задача запрета кибервойны против гражданских инфраструктур — снизить текущую (невысокую, но опасную) напряженность, выйти из ситуации, когда всего лишь несколько нажатий кнопок отделяют нас от начала разрушительных атак, грозящих перерасти в полномасштабную кибервойну или даже в настоящий вооруженный конфликт. Логические бомбы в наших электросетях, размещенные, по

**290**

КИБЕРМИР

всей вероятности, китайскими военными, и аналогичные устройства, которые мы оставили или оставим в сетях других стран, оказывают такое же дестабилизирующее воздействие, как и секретные агенты, которые закладывают взрывчатку в опоры высоковольтных линий, трансформаторы и генераторы. Кибероружие сложнее обнаружить, но всего лишь несколько клавиш, которые нажмет на другом конце мира раздраженный или бесчестный кибервоин, могут начать конфликт, перерастающий в войну, масштабы которой мы даже не представляем.

Хоть мы и можем представить ситуацию, в которой США получат преимущество, заблаговременно разместив логические бомбы в гражданских сетях потенциального противника, риски, которые несет такая же практика со стороны других стран, значительно превышают возможную выгоду. Поэтому в рамках запрета нападения на гражданскую инфраструктуру с использованием кибероружия нам следует согласиться, что это табу должно распространяться и на проникновение в сети гражданской инфраструктуры с целью размещения логических бомб или лазеек.

Начнем с банков?

Даже соглашение, ограничивающееся защитой гражданской инфраструктуры, может вызвать ряд проблем. Для некоторых стран, к примеру России, готовность США принять такое соглашение подтвердит их уверенность в опасности кибероружия. И они продолжат добиваться его полного запрета. Переговоры о ратификации соглашения по защите гражданских объектов могут открыть ящик Пандоры, полный проблем. Поэтому Соединенным Шта- 291

Третья мировая война: какой она будет?

там стоит еще больше ограничить рамки первого международного соглашения по кибероружию. Один из вариантов — предложить договор, предотвращающий кибератаки на международную финансовую систему. Каждая развитая страна заинтересована в надежности данных, на которые опираются международные и национальные банки, финансовые и товарные биржи. От кибератаки, направленной на международную финансовую систему, пострадают практически все государства, за исключением стран, похожих на нищую и неконтролируемую Северную Корею. Урон, нанесенный системе, затронет самого нападающего, а если он будет «пойман», у международного сообщества испортятся финансовые отношения с его страной, что подорвет национальную экономику.

В силу взаимосвязи крупнейших финансовых институтов мира, в том числе и частных банков, кибератака на финансовую инфраструктуру одного государства может вызвать стремительный волновой эффект, подрывая доверие к мировой финансовой системе. Как сказал мне директор одной компании с Уолл-стрит, «именно уверенность в данных, а не золотые слитки Федеральной резервной системы Нью-Йорка, лежит в основе работы финансовых рынков мира».

Убеждение в том, что кибератака на банки способна разрушить мировую финансовую систему, не позволило представителям предыдущей администрации одобрить предложение взломать банки и украсть денежные фонды террористов и диктаторов, например Саддама Хусейна. Как отметил генерал Макконел: «Что будет, если кто- нибудь совершит атаку на большой нью-йоркский банк, изменит или уничтожит данные? Возникнет неуверенность и утратится доверие. Без уверенности в надежности и точности финансовых операций никто не станет их совершать». Таким образом, мы в интересах США сами

292

КИБЕРМИР

выбрали предложить и поддержать международное соглашение о запрете кибератак на финансовые институты. (Запрещать кибершпионаж при этом не нужно. Сведения о финансовых операциях банков обладают разведывательной ценностью и позволяют отслеживать деньги террористов. Соединенные Штаты, вероятно, этим уже занимаются. Европейские финансовые институты были шокированы, узнав в 2006 году, что США, отыскивая следы принадлежащих террористам фондов, вполне возможно, тайно отслеживали международные финансовые транзакции системы банковского клиринга, — SWIFT, Society of Worldwide Interbank Financial Telecommunications.)

Инспекция в киберпространстве

Ценность международных соглашений о запрете определенных видов кибервоенной деятельности или о ненападении отчасти зависит от нашей способности выявлять нарушения и возлагать на нарушителей ответственность. Принципы контроля над традиционными вооружениями едва ли применимы в киберпространстве. Чтобы удостовериться в соблюдении ограничений на количество подводных лодок или ракетных стартовых шахт, достаточно нескольких снимков из космоса. Сложно спрятать судостроительный завод, на котором производятся подводные лодки, или ракетную базу. Для проверки количества более мелких объектов, таких как боевые машины, на военные базы отправляется инспекция. Чтобы убедиться в том, что на ядерных реакторах не ведется незаконная деятельность, инспекторы МАГАТЭ (Международного агентства по атомной энергетике) устанавливают камеры наблюдения в помещениях, ставят пломбы и идентификаторы

293

Третья мировая война: какой она будет?

на ядерных материалах. Международные группы берут пробы химических веществ на химзаводах, отыскивая доказательства незаконного производства химического оружия. Для того чтобы отслеживать испытания ядерного оружия, существует международная сеть сейсмических датчиков, а страны делятся друг с другом полученными данными. Только эта сейсмическая сеть да, пожалуй, команды МАГАТЭ могут служить образцом в случае контроля над кибервооружениями. Нереально обнаружить кибероружие из космоса и даже в ходе непосредственного осмотра военных баз. Ни одно государство не согласится, чтобы международные группы инспекторов проверяли, какие специальные программы используются в его компьютерных сетях для защиты секретной информации. Даже если в какой-нибудь параллельной вселенной какая-нибудь страна согласилась бы на такую проверку военных и гражданских компьютерных сетей, она могла бы спрятать кибероружие на флэш-карте или компакт-диске где угодно. Соблюдение запрета на разработку, обладание или испытание кибероружия в закрытых сетях (таких, как National Cyber Range, разработанная Университетом Джонса Хопкинса и корпорацией «Локхид») сложно проконтролировать.

Фактическое использование кибероружия отследить уже проще, последствия атаки часто вполне заметны. Специалисты по судебной компьютерной экспертизе, как правило, способны определить, какие методы были задействованы, даже если не удается выяснить, как злоумышленники проникли в сеть. Но проблема атрибуции остается, даже когда атака состоялась. Техники отслеживания и журналы интернет-провайдера порой помогают узнать, какая страна причастна ко взлому, но этого недостаточно для того, чтобы доказать вину конкретного правительства. К тому же существует риск ложных обвинений. Киберата-

294

КИБЕРМИР

ки против Грузии наверняка организовала Россия, но компьютер, управляющий ботнетом, находился в Бруклине.

Даже если страна признает, что атака была произведена с компьютеров, расположенных на ее территории, вину можно переложить на анонимных граждан. Именно так и поступило российское правительство во время кибератак на Эстонию и Грузию. Так же поступило китайское правительство в 2001 году, когда было обнаружено проникновение в сети США после инцидента с американским самоле- том-шпионом, который якобы вторгся в китайское воздушное пространство. Хакеры и в самом деле могут оказаться простыми гражданами, хотя такие действия наверняка совершаются с благословления и разрешения правительств.

Один из способов решить проблему атрибуции — переложить бремя доказывания со следователя и обвинителя на страну, с территории которой была запущена атакующая программа. Подобный ход использовался в практике борьбы с международной преступностью и терроризмом. В декабре 1999 года Майкл Шихен, тогда представитель США, должен был передать Талибану простое сообщение. Шихену поручили дать понять представителям Талибана, что именно они понесут ответственность за любую атаку, предпринятую «Аль-Каидой» против Соединенных Штатов или их союзников. Поздно вечером Шихен через переводчика передал это сообщение по телефону представителю Мулла Моххамед Омара, лидера Талибана. Чтобы донести суть, Шихен нашел такую простую аналогию: «Если в вашем подвале живет поджигатель, который каждую ночь выходит и сжигает дотла дома ваших соседей, а вы знаете, что происходит, нельзя утверждать, что вы за это неответственны». Мулла Моххамед Омар не выселил поджигателя из своего подвала, он продолжал укрывать Бен Ладена и его последователей даже после 11 сентября. Мулла Моххамед Омар во время написания этой книги

Z95

Третья мировая война: какой она будет?

прячется где-то в подвале, а его ищут армии НАТО, США и Афганистана.

«Принцип поджигателя» вполне применим к кибервойне. Хоть мы и рассуждаем о киберпространстве как об абстрактном пятом измерении, оно вполне материально. Его физические компоненты — высокоскоростные оптоволоконные магистрали, каждый маршрутизатор, сервер — располагаются на территории конкретных стран, за исключением разве что подводных кабелей и телекоммуникационных спутников. Но даже ими владеют страны или компании, у которых есть реальные физические адреса. Некоторые любят порассуждать о проблеме суверенитета в Интернете — никто не владеет киберпространством во всей его полноте и никто не несет ответственности за его целостность и безопасность. «Принцип поджигателя» можно использовать под названием «национальная ответственность за киберпространство». Он сделал бы каждого человека, компанию, интернет-провайдера, страну ответственными за безопасность своей части киберпространства.

Тогда страны вроде России больше не имели бы права утверждать, что они не контролируют своих так называемых патриотических «хактивистов». Международное соглашение позволило бы государствам совместно отстранять таких хакеров от участия в незаконной международной деятельности или, по крайней мере, потребовать от конкретных стран прилагать максимальные усилия для этого. Кроме того, страна, подписавшая международное соглашение, должна соблюдать гарантию содействия. Там могут содержаться требования быстро реагировать на запросы международного следствия, изымать и хранить журналы серверов и маршрутизаторов, принимать международных следователей и содействовать им, вызывать граждан своей страны на допросы, преследовать граждан в судебном порядке за определенные пре- 296

КИБЕРМИР

ступления. Существующая с 2001 года Конвенция Совета Европы по киберпреступности включает многие из перечисленных гарантий, и Соединенные Штаты входят в эту конвенцию. Наш суверенитет не пострадал от бюрократической системы Старой Европы. Наоборот, подписав конвенцию, Соединенные Штаты пообещали принимать любой новый закон, необходимый для наделения правительства США полномочиями для выполнения гарантий этого соглашения.

В отличие от существующей конвенции по киберпреступности конвенция по кибервойне обяжет страны следить за тем, чтобы интернет-провайдеры прекращали обслуживать людей и устройства, участвующие в атаках, и сообщали о них властям. Такое условие означало бы, что интернет-провайдерам придется выявлять и блокировать «черви», ботнеты, DDoS-атаки^и прочую злоумышленную деятельность. (Процесс идентификации вредоносного ПО не так сложен, как проверка информационных пакетов, он может быть реализован через анализ потоков — вы просто продвигаетесь по сети и обращаете внимание на «острые» импульсы или критические паттерны.) Если стране не удается успешно привлекать интернет-провайдеров к сотрудничеству, в международном соглашении должна быть предусмотрена процедура, которая перекладывает ответственность на другие государства. Интернет-провайдер может быть занесен в международный черный список, и тогда все страны — участники конвенции обязаны будут заблокировать работу этого провайдера до тех пор, пока он не подчинится и не разберется с ботнетом и другими вредоносными программами.

Такое международное соглашение отчасти решило бы проблему атрибуции с помощью перекладывания ответственности. Даже если взломщика определить не удастся, появится кто-то, ответственный за прекращение атаки

**297**

Третья мировая война: какой она будет?

и расследование. Большинству стран даже не придется создавать новые отделы для киберрасследований. Такие страны, как Китай и Россия, способны устанавливать личности хакеров и быстро пресекать их деятельность. Как сказал Джим Льюис из Центра стратегических и международных исследований, «если какой-нибудь хакер из Петербурга попробует взломать сеть Кремля, ему хватит пальцев на одной руке, чтобы сосчитать оставшиеся часы жизни». Будьте уверены, то же самое ждет любого жителя Китая, который попытается проникнуть в сеть Народно- освободительной армии. Если Китай и Россия подпишут подобное соглашение о кибервойне, они не смогут больше обвинять в DDoS-атаках своих граждан и спокойно бездействовать. Неспособность быстро действовать против хакеров приведет к тому, что страна будет признана нарушителем и, что более важно, другие государства откажутся от услуг проблемных интернет-провайдеров. Государства имеют возможность остановить такой дефектный трафик, но в отсутствие правовых рамок делают это очень неохотно. Соглашение не только позволит странам блокировать такой трафик, но и обяжет их это делать.

Но этого недостаточно, чтобы полностью решить проблему атрибуции. Российская ботнет-атака может пойти из Бруклина. Тайваньский хакер способен атаковать сайты китайского правительства, сидя в интернет-кафе в Сан-Франциско. Но по условиям такого соглашения Соединенным Штатам пришлось бы пресечь действия ботнета и начать активное расследование. В случае с гипотетическим тайваньским агентом, вторгшимся в китайскую сеть, Китай, обнаружив это, должен будет обратиться в ФБР и Секретную службу США с просьбой помочь китайской полиции отследить преступника в Сан- Франциско. Если его найдут, то привлекут к суду за нарушение американского закона. Конечно, любая страна мо- 29В

КИБЕРМИР

жет сказать, что ищет хакера, а в действительности этого не делать или провести расследование и не обнаружить виновного. Когда обнаружен ботнет, управляемый через интернет-провайдера конкретной страны, государство может потребовать время на принятие мер. Чтобы понять, действительно ли что-то предпринимается, понадобится международная следственная комиссия. Специалисты, действующие в рамках этой комиссии, будут представлять отчеты странам — участницам конвенции о том, действует или нет конкретное государство в духе соглашения. Можно создавать международные инспекционные группы, сходные с группами, работающими в рамках Договора о нераспространении ядерного оружия, запрета на химическое оружие и Европейского соглашения о безопасности и сотрудничестве. Такие группы могут приглашаться для содействия в проверке кибератаки, нарушающей соглашения. Они помогут определить, из какой страны была запущена атака. При добровольном согласии стран-участниц международные эксперты могут размещать отслеживающее потоки оборудование на ключевых узлах, ведущих в сети стран, чтобы облегчить обнаружение и поиск атак.

Международные эксперты могут руководить центром, с которым будут связываться государства, считающие, что подвергаются кибератаке. Представьте, что на израильскую сеть в три часа утра по тель-авивскому времени обрушивается DDoS-атака с ботнетов провайдера в Александрии (Египет). В Израиле, как и во всех странах — участницах нашей гипотетической конвенции, есть постоянно действующий центр кибербезопасности. Сотрудники израильского центра информируют международный центр, расположенный, скажем, в Таллинне, что кибератака началась с конкретного интернет-провайдера в Египте. Международный центр связывается с египетским центром в Каире и требует немедленно расследо- 299

Третья мировая война: какой она будет?

вать, обнаружены ли ботнеты этого интернет-провайдера в Александрии. Международные эксперты могут засечь, сколько времени понадобится Египту на обнаружение и пресечение атаки. Возможно, они смогут проследить потоки трафика, идущего через маршрутизаторы, соединяющие Египет с остальным миром, и обнаружить ботнет. Египет будет обязан представить отчет о расследовании. Если инцидент подтвердится, международные эксперты вышлют следственную группу для помЛци и наблюдения за действиями властей, которая подготовит отчет для стран — участниц соглашения.

К странам, пренебрегающим правилами, следует применять санкции. Помимо отказа других стран работать с провайдером-нарушителем могут последовать санкции со стороны международных организаций. В качестве более решительных мер предложим отказ в предоставлении виз должностным лицам страны-нарушителя, ограничение исходящего и входящего в страну кибертрафика или отключение страны от международного киберпространства на определенный срок.

Такие проверки и меры не решают проблему атрибуции. Они не помешают злоумышленникам представить невиновную страну источником кибератаки. Однако они осложнят возможность проведения некоторых видов кибератак, установят международные нормы, обяжут страны оказывать содействие и создадут международное сообщество экспертов для совместной борьбы с кибервойной. Важно помнить, что организация атак такого масштаба требует усилий государственного уровня, и только несколько государств обладают такими возможностями. Список потенциальных нападающих невелик. Атрибуция — главная проблема киберпреступности, но что касается войны, расследование и традиционная разведка быстро сократят число подозреваемых.

 ЗСШ

КИБЕРМИР

Из нашего обсуждения проблем контроля над вооружениями можно сделать пять выводов.

Во-первых, в отличие от других форм контроля над вооружениями, которые предусматривают ликвидацию определенных видов оружия, контроль над кибервооружениями не сокращает арсенал. Он просто запрещает конкретные действия, а страна может как соблюдать условия соглашения, так и внезапно нарушить их без всякого предупреждения.

Во-вторых, расширенное определение кибероружия, включающее кибершпионаж, делает его неверифицируе- мым и невыгодным для нас. Тем не менее национальные службы разведки и правительства должны создать каналы для дискуссий, чтобы разведывательная деятельность не вышла из-под контроля и не истолковывалась как имеющая враждебные намерения.

В-третьих, международные соглашения, запрещающие определенные действия, например кибератаки на гражданскую инфраструктуру, отвечают нашим интересам. Но поскольку такие атаки все равно могут произойти, в соглашениях нельзя принижать необходимость оборонительных мер для защиты гражданской инфраструктуры.

В-четвертых, полная уверенность в соблюдении ограничений, сформулированных в соглашении, невозможна. Мы, вероятно, сумеем подтвердить факт нарушения, но атрибуция атаки — вопрос сложный, к тому же атакующие намеренно могут запутать следы. Тем не менее существуют меры, которые могут содействовать соблюдению международного запрета кибератак на гражданские объекты, в частности создание международного экспертного совета, ответственность федеральной власти за нарушения, происходящие на ее территории, и гарантия содействия в пресечении и расследовании атак.

 **за** 1

Третья мировая война: какой она будет?

Запрет кибератак на гражданскую инфраструктуру, вероятно, приведет к тому, что нам и другим странам придется прекратить любую деятельность, связанную с установкой логических бомб и лазеек в гражданских сетях других стран. Эти вопросы мало обсуждаются СМИ и населением, на самом деле они очень опасны и провокационны, поскольку последствия их применения сопоставимы с результатами войны, но без солдат и смертей. Однако при этом они свидетельствуют о враждебных намерениях больше, чем любое другое оружие в арсенале страны. Применить их можно легко и просто, без всякого разрешения и без осознания масштабов возможного обострения политической обстановки. Даже если война начнется в киберпространстве и будет вестись без солдат и кровопролития, едва ли она останется такой навсегда. Если мы устанавливаем кибероружие в инфраструктурных сетях других стран, война может разгореться очень легко.

**Глава В**

Повестка дня

В

оенные подразделения двух десятков стран незримо перемещаются на новое поле битвы. Поскольку они невидимы, парламенты и общество не замечают их приближения. Первые схватки были локальными и не отличались изощренностью оружия, поэтому мало кто считает, что кибервоины способны на большее. Поскольку крупнейшие военные державы являются торговыми партнерами, политические обозреватели не могут даже представить обстоятельства, которые могли бы сделать их отношения враждебными. Соединенные Штаты в течение семи лет

 303

Третья мировая война: какой она будет?

\

\

вели войну с одной страной и девяти — с другой, а теперь преодолевают самую тяжелую рецессию и склонны к излишней подозрительности. Таким образом, переключая внимание на другие вопросы, мы, возможно, закладываем предпосылки для кибервойны. Нечто подобное наблюдалось в начале прошлого столетия. Барбара Тучман в книге The Proud Tower («Башня высокомерия») описывает мир, не догадывающийся, что войска уже готовы к разрушительным действиям, не задумывающийся, к каким ужасным последствиям это приведет. В следующем романе, The Guns of August («Августовские пушки»), одна маленькая искра приводит эти силы в действие. Тщательно подготовленные войска фон Шлиффена используют новую железнодорожную сеть, чтобы привести в движение механизм, который ничто уже не сможет остановит. Военные используют возможности новой химической промышленности, ведь химическое оружие наносит гораздо больший ущерб, чем кто-либо мог ожидать. Сегодня наши военные тщательно продумывают планы ведения нового типа войны и применяют технологии, разработанные для коммерческого использования. Как и сто лет назад, эти планы мало известны общественности. А ведь в нашей истории были случаи, когда американское академическое сообщество, средства массовой информации и конгресс фокусировались на проблеме, исследовали ее, вводили необходимое регулирование и в итоге предотвращали серьезные бедствия. Проблема стратегической ядерной войны, к которой мы неоднократно обращались в этой книге, яркий тому пример. В мире появилась новая технология, и американские военные увидели в ней способ достичь военного превосходства и тем самым мира. На авиабазах, под транспарантами «Мир — наша профессия», разрабатывали планы массированного применения ядерного оружия на начальном этапе войны — против городов и гражданских

304

Повестка дня

объектов. Только после того, как научное сообщество привлекло внимание общественности к этим планам и проблеме ядерной войны в целом, появились разумные ограничения и были разработаны и приняты соответствующие программы.

В наше время Киберкомандование США и связанные с ним ведомства, где работают самые умные, патриотически настроенные и недооцениваемые гражданские и военные государственные служащие, разворачивают планы по достижению превосходства в киберпространстве, чтобы обеспечить безопасность страны и сохранить мир. Также готовятся киберподразделения и в других странах. В рамках этой подготовки кибервоины размещают «черные ходы» в гражданских сетях, устанавливают логические бомбы в энергетических сетях. Они считают свое оружие передовым, и не только потому, что применяют новейшие технологии, но и потому, что они не видят взрывов и смертей. Как и люди, управляющие беспилотным летательным аппаратом Predator, которые сидят в Соединенных Штатах и убивают талибов в Пакистане с помощью дистанционного управления, они подсознательно думают — раз они живут в мирном пригороде, то разрушения на другом конце мира выглядят чистенькими и аккуратными, вовсе не такими, как последствия «настоящей войны».

Когда отношения во время какого-нибудь будущего кризиса обострятся и кибервоины одной страны получат приказ послать сигнал потенциальному противнику с помощью размещенной заранее логической бомбы, предотвратит ли это надвигающуюся войну или, напротив, спровоцирует? Возможно, другая сторона пойдет по ложному следу и не сумеет понять, кто начал войну, в результате чего в конфликт будут втянуты другие страны. Инициировать войну способны кибервоины любой из стран, обладающих киберпотенциалом. С другой стороны, это может

305

11 № 4595

Третья мировая война: какой она будет?

сделать и хакер, который решит воспользоваться кибероружием для развлечения, а не просто ради собственной выгоды, или же обнаружит и взорвет логическую бомбу, оставленную кем-то другим. А в результате разгорится кибервойна, невероятно стремительная и глобальная.

Когда американский президент посылает военных разбомбить лагерь террористов или завод по производству ядерного оружия в какой-нибудь стране, которая, быть может, и не сумеет дать отпор нашим вооруженным силам, но при небольших вложениях в собственный киберпотенциал они смогут в ответ разрушить международную финансовую систему, в целостности которой не слишком заинтересованы. Несопоставимость огромных затрат на вооружение и небольших в киберпотенциал побудят другие страны, а также, вероятно, преступные картели и террористические группировки развивать именно его.

Поскольку США изобрели Интернет, кибершпионаж и кибероружие, нам свойственна неявная заносчивость, в силу которой мы полагаем, что никто не способен победить Америку в кибервойне. Наши кибервоины и руководители из сферы кибербезопасности, наверное, успокаивают себя, полагая, что мы можем заметить надвигающуюся кибератаку. Может быть, они думают, что мы сумеем ее частично заблокировать, а потом ответить, и даже больше того. Но реальность такова, что крупная кибератака другой страны, скорее всего, начнется в США, так что мы не сможем увидеть ее приближение и заблокировать с помощью систем, которые имеются у нас сейчас или которые мы намерены ввести в эксплуатацию. Да, мы, пожалуй, сможем отреагировать таким же образом, но наша страна пострадает от масштабной кибератаки на гражданскую инфраструктуру, которая на недели выведет из строя энергосистему, остановит движение поездов и самолетов, взорвет трубопроводы и воспламенит нефтеперегонные заводы.

 зов

Повестка дня

Реальность такова, что если американский президент захочет ответить тем же, ему придется обострить конфликт — придется пересечь границу кибернетической и наступательной войны. А сделав это, он обнаружит, что даже наши обычные силы киберзависимы. Зависимость американских вооруженных сил от киберсистем превосходит всестороннюю зависимость от них коммерческих инфраструктур. Подрядные организации, необходимые Америке для того, чтобы вести войну, может обездвижить кибератака. «Герметизированная» компьютерная сеть Министерства обороны может оказаться проницаемой и непригодной. Самые передовые технологии обычного вооружения, которые обеспечивают военное превосходство США (истребитель F-35 и GPS) могут внезапно выйти из строя. Мы не единственная страна, способная устанавливать логические бомбы.

Когда страна погрузится во мрак, жители будут дрожать от холода, исчезнут с прилавков продукты, а банкоматы перестанут выдавать наличные, когда все военные подразделения окажутся беспомощными и дела пойдут совсем скверно, что будет делать главнокомандующий? Вероятно, он назначит комиссию, которая станет расследовать, что пошло не так. Эта комиссия примется читать доклады других комиссий, одну из которых в 1996 году назначил Билл Клинтон, и с удивлением обнаружит, что это бедствие прогнозировали еще тогда. Они обратят внимание на совет, который дала президенту неправительственная комиссия 2008 года, — серьезно отнестись к угрозе кибервойны. При должном усердии они обнаружат и проведенное Национальной академии наук в 2009 году исследование о наступательной информационной войне, в котором политика в отношении кибервойны характеризовалась как «плохо согласованная, неразвитая и в высшей степени неопределенная».

307

Третья мировая война: какой она будет? .

Комиссия, собранная после катастрофы, специальный комитет конгресса или следующий президент, скорее всего, порекомендуют принять план, чтобы «подобное больше никогда не происходило». Поскольку мы сейчас знаем, что уже рекомендовано, что не сработало и почему, может быть, не стоит ждать катастрофы, чтобы принять план на случай кибервойны? Если отбросить все излишества и просто желательные аспекты, останется шесть простых шагов, которые нужно совершить сейчас и сразу, чтобы предотвратить беду.

1 . Думать о невидимом

Во-первых, мы должны начать широкое общественное обсуждение проблемы кибервойны. Недавно одна студентка, желавшая поступить в аспирантуру, спросила меня, где она могла бы пройти соответствующий курс. Мы внимательно просмотрели учебные планы и не нашли ни одного такого курса в университетах, готовящих специалистов по политике безопасности, включая Школу Кеннеди в Гарварде, Школу Вудро Вильсона в Принстоне и Школу Линдона Джонсона в Техасе. Тогда она поинтересовалась, какие книги ей стоит почитать, и мы нашли несколько интересных изданий, но мало где глубоко рассматривались вопросы политики и технологии кибервойны. Во многих книгах под фразой «информационная война» чаще всего понималось психологическое оружие или публичная дипломатия.

Книг, посвященных кибервойне, возможно, мало потому, что тема эта остается закрытой. Необходима открытая дискуссия, ведь немалая часть важных данных остается под грифом «секретно». В 1950-1960-х годах таким людям, как Герман Кан, Билл Кауфман и Альберт Вольстет- тер, тоже говорили, что проблемы ядерной войны совсем

 ЗОВ

Повестка дня

не стоит обсуждать публично. Кан в ответ на это написал книгу под названием «Думать о немыслимом» (Thinking About the Unthinkable, 1962), которая содействовала здравому общественному диалогу о моральных, этических и стратегических аспектах ядерной войны. Публикация результатов исследований, проводимых в Массачусетском технологическом институте (МТИ), Гарварде, Принстонском университете и Брукингском институте, также внесла свой вклад.

Курсы Билла Кауфмана в МТИ, Гарварде и Брукингском институте сформировали взгляд на проблему ядерной стратегии двух поколений студентов, научили их ставить аналитические вопросы и благодаря этому мыслить самостоятельно. Сегодня в Гарварде и МТИ запущен проект «Минерва» (весьма кстати так названный) — финансируемая Министерством обороны открытая исследовательская программа по проблеме кибервойны. (Вспоминаю изречение Гегеля: «Сова Минервы всегда прилетает в сумерках» — мудрость всегда приходит слишком поздно.)

Основные СМИ стали уделять больше внимания вопросам кибервойны. Обозреватели Wall Street Journal и New York Times пишут на эту тему с 2008 года. В 2003 году программа под названием «Кибервойна» вышла в рамках популярной телепередачи Frontline. Телевидение гораздо больше фокусируется на проблеме «кражи личности», поскольку многие зрители и читатели уже стали жертвами подобных киберпреступлений. Кинорежиссеров, однако же, тема кибервойны очень привлекает. В фильме «Крепкий орешек-4» бывший сотрудник государственной службы кибербезопасности, которого никто не слушал (его прототипом один журналист New York Times назвал меня. Вздор!), взламывает национальные системы. В фильме «На крючке» в результате хакерской атаки обрываются линии высокого напряжения и вся жизнь рушится.

309

Третья мировая война: какой она будет?

;

В «Итальянской работе» хакеры просто выводят из строя светофоры, а в «Одиннадцати друзьях Оушена» без электричества остается весь Лас-Вегас. Таких фильмов очень много, и киноманы легко могут представить, к чему приводит кибервойна. Однако высокопоставленные чиновники редко ходят в кинотеатры. Или, наверное, думают, что все это лишь плод воображения. Чтобы заставить их понять, что такие сценарии вполне реальны, нам необходима специальная учебная программа. Генерал Кен Минихэн давно уже продвигает идею проведения военной игры, похожей на «Приемлемого получателя»: «Мы напугаем их до смерти, как напугали президента в 97-м».

Конгресс, на удивление, провел уже немало слушаний по теме кибербезопасности и дал задание Управлению государственной ответственности (УГО) исследовать этот вопрос. В одном из докладов перед УГО был поставлен вопрос, обоснованны ли предостережения о том, что хакеры могут атаковать электросеть. УГО исследовало одну из немногих государственных электросетей, которая находится в ведении независимой государственной корпорации «Управление ресурсами бассейна Теннеси». В ответном докладе УГО от 2008 года сообщалось, что в этих сетях есть множество уязвимых мест, открытых для вторжения. Однако по вопросам кибервойны в целом конгресс сделал очень мало.

Конгресс — это федерация феодалов, объект превратностей бесконечного фандрайзинга и лоббирования тех, кто предоставил фонды. Отсюда вытекает два вредных последствия относительно участия конгресса в контроле над кибервойной. Во-первых, каждый хочет сохранить свою сферу влияния. Конгресс отвергает любые предложения, подобные тому, что внес сенатор Боб Беннэт (республиканец из Юты) о создании отдельного комитета, уполномоченного проводить проверки по кибербезопасности. В итоге данной проблемой занимается около 30 комитетов и под- [[104]](#footnote-105)

Повестка дня

комитетов, и ни один из них не имеет возможности подойти к проблеме целостно. Во-вторых, конгресс «воздерживается от регулирования» и этого не стесняется. Влиятельные доноры из сферы информационных технологий, энергетического и телекоммуникационного бизнеса сделали идею серьезного регламента в области кибербезопасности столь же отдаленной, сколь и идеи общественного финансирования кампаний по выборам в конгресс или значительных ограничений взносов в пользу избирательных кампаний.

Для ведения нужного нам диалога необходимы серьезные академические исследования и обучающие программы, полки новых книг, доскональные журналистские расследования и серьезное рассмотрение в конгрессе.

2. Оборонительная триада

Следующий пункт программы предупреждения кибервойны — это оборонительная триада. Как рассматривалось выше, оборонительная триада блокирует вредоносные программы на участках главных интернет-провайдеров, защищает элементы управления электросетей, укрепляет безопасность сетей Министерства обороны и целостность его оружия. В Министерстве обороны работа в этом направлении началась по решению президента Буша в последний год его пребывания в должности. Оборонительная триада — это не попытка защитить все в отличие от моей Национальной стратегии по кибербезопасности. Однако она должна защитить все необходимое, чтобы заставить другую страну дважды подумать, прежде чем начать кибервойну против нас. Потенциальный нападающий должен знать, что его атака по большей части провалится и что главным ее последствием станет разного рода воздаяние. Без оборонительной триады Соединенным Штатам лучше воздерживаться от любых действий [[105]](#footnote-106)

Третья мировая война: какой она будет?

(не только в киберпространстве), которые могут спровоцировать кибератаку на Америку. Сейчас мы настолько уязвимы перед масштабной кибератакой, что нашим лидерам лучше соблюдать осторожность.

Мы не сумеем построить два из трех зубьев оборонительной триады (обеспечить защиту магистральных интернет-провайдеров и электросетей) без дополнительного регулирования. Раньше, говоря о национальной безопасности в целом, я приводил такое сравнение: обеспечить безопасность без дополнительного регулирования со стороны федерального правительства — это все равно что защищаться с завязанными за спиной руками. Было время, когда федеральное регулирование было чересчур навязчивым и неэффективным, но этого можно избежать, если правительство попросит некоторые отрасли промышленности воздерживаться от определенных вещей и очертит желаемые цели. На конференции Black Hat (о которой уже речь) эксперт по кибербезопасности и автор многих книг Брюс Шнейер сказал то же самое, заявив, что разумное регулирование, которое определяет цель и не диктует средства ее достижения, необходимо для улучшения кибербезопасности.

В программу по кибербезопасности должно входить правило, которое требует от магистральных интернет- провайдеров проводить глубокое инспектирование пакетов на предмет обнаружения вредоносных программ, не нарушая при этом принципа неприкосновенности частной жизни и не допуская оплошностей. Интернет-провайдерам необходимо предоставить правовую защиту, чтобы они не опасались исков — по сути, за то, что блокируют вирусы, «черви», DDoS-атаки, фишинги и прочие формы вредоносного ПО. Напротив, по новым правилам их следует обязать делать это.

Чтобы Министерство национальной безопасностиисполнило свою роль в оборонной триаде, нам нужно создать [[106]](#footnote-107)

Повестка дня

заслуживающий доверия и высокопрофессиональный орган, возможно, Управление по киберобороне. Управление по киберобороне должна контролировать системы глубокого инспектирования пакетов, которыми будут управлять интернет-провайдеры. Кроме того, она должна мониторить состояние Интернета в режиме реального времени; взять на себя ответственность за регулирование кибербезопасности энергетического сектора, которая сейчас возложена на Федеральную комиссию по управлению энергетикой; предоставлять точку фокуса для правоприменительных акций, связанных с киберпреступностью. Но самая важная роль управления должна заключаться в обороне как домена .gov, так и доменов критической инфраструктуры в случае кибератаки. Она может в режиме реального времени предоставлять интернет-провайдерам известные сигнатуры вредоносного ПО и координировать взаимный обмен сигнатурами, которые обнаружили сами интернет-провайдеры. Существующая уже сорок лет национальная система связи, задачей которой было обеспечивать телефонную связь в случае аварий и которая недавно была переименована в Национальный интеграционный центр кибербезопасности и коммуникаций, могла бы предоставлять интернет-провайдерам внеполосную систему связи для передачи сигнатур вредоносного ПО. Управление по киберобороне может использовать экспертные оценки Пентагона и служб разведки, но не следует вверять миссию защиты отечественных компьютерных сетей Агентству национальной безопасности. Специалисты из АНБ обладают огромным опытом, но при этом пользуются недоверием общества, которое особенно обострили незаконные перехваты сообщений по заказу Буша и Чейни.

Помимо регулирования интернет-провайдеров необходимо также ввести регулирование сети электропередач. [[107]](#footnote-108)

Третья мировая война: какой она будет?

I

Единственный способ обезопасить сеть — это получить доступ к кодам команд, которые отдаются устройствам, управляющим системой, аутентификации отправителей, а также ряду абсолютно внеполосных каналов, не связанных с интрасетями компаний и публичным Интернетом. Федеральная регулятивная комиссия этого не запрашивала, хотя в конце концов установила некоторые регламенты в 2008 году, однако до сих пор не начала приводить их в исполнение. И даже если начнет, не ожидайте многого. У комиссии нет ни опыта, ни персонала, чтобы убедиться в том, что электроэнергетические компании отсоединили элементы управления от магистралей, которые может использовать хакер. Задача наблюдения за выполнением этих правил также должна быть возложена на Управление по киберобороне, которое должно предоставлять экспертные оценки и тесные связи которой с промышленностью не станут помехой для безопасности, как это было в случае Федеральной регулятивной комиссии.

Управление по киберобороне должно также взять на себя ответственность за мириады гражданских федеральных ведомств и агентств, которые сейчас пытаются организовать киберобзащиту собственными силами. Кроме того, консолидация в предложенном управлении всего, что сделано в сфере безопасности административно-бюджетным управлением и управлении общими службами, увеличит наши шансы на достижение лучших результатов в управлении безопасностью гражданских (невоенных) государственных сетей.

3. Киберпреступность

Поскольку киберпреступники — это потенциальные наемные кибервоины, мы должны в качестве третьего пунк- [[108]](#footnote-109)

Повестка дня

та нашей программы сократить уровень киберпреступности в Интернете. Киберпреступники начали проникать в сети поставок производителей как аппаратного, так и программного обеспечения для того, чтобы внедрить вредоносный код. Вместо того чтобы просто использовать широко распространенные хакерские инструменты, киберпреступники теперь начинают писать собственный, специально разработанный код для взлома систем безопасности, как было в случае с кражей миллионов номеров кредитных карт из Т. J. Махх в 2003 году. Эта тенденция указывает на растущую изощренность киберпреступников и, пожалуй, свидетельствует о том, что угроза может расшириться до уровня национальной. А это позволяет предположить, что нам нужно прилагать больше усилий к борьбе с киберпреступностью. Сегодня киберпреступления расследует ФБР, Секретная служба (теперь она называется Immigration and Customs Enforcement) и Федеральная комиссия по торговле. И все-таки раздаются жалобы компаний и частных лиц на то, что их заявления о киберпреступлениях остаются без ответа. Девяносто независимых прокуроров Министерства юстиции, работающие по всей стране, чаще игнорируют киберпрестпле- ния, поскольку отдельные хищения превышают сумму в 100 тысяч долларов, необходимый для заведения федерального дела. Адвокаты часто не разбираются в компьютерных вопросах и не хотят расследовать преступления, жертвы которых находятся в другом городе или, еще хуже, в другой стране.

Президент мог бы назначить агентов ФБР и Секретной службы, которые занимаются киберпреступлениями, на определенные должности в предлагаемую Управление по киберобороне, и они вместе с адвокатами подготавливали бы дела для Министерства юстиции. Единый следственный центр в рамках Управления по киберобороне, коор-

Третья мировая война: какой она будет?

динирующий работу региональных подразделений, мог бы проводить экспертизу, расследовать преступления, устанавливать международные связи, необходимые для увеличения возможностей ареста, что до определенной степени сдерживало бы киберпреступников. Сегодняшняя правоприменительная практика в США киберпреступников никак не устрашает. Сейчас киберпреступления действительно выгодны. Чтобы прекратить это, США необходимо существенно больше вкладывать в борьбу федеральных правоприменительных органов с киберпреступностью. Кроме того, нам придется что-то сделать с оплотами кибепреступности.

В конце 1990-х международные преступные картели отмывали сотни миллиардов долларов через банки в разнообразных карликовых государствах, обычно островных, а также в нескольких более крупных странах. Главные финансовые власти объединились, разработали типовой закон, делающий отмывание денег преступлением, и посоветовали странам — оплотам киберпреступности принять его и обеспечить правовой санкцией. В противном случае крупнейшие международные финансовые институты прекратили бы проводить расчеты в местных валютах и финансовые операции с их банками. Я имел удовольствие сообщить об этом премьер-министру Багамских островов, где закон был быстро принят. Практика отмывания денег не исчезла, но теперь это гораздо сложнее, да и подходящих для этого стран стало меньше. Стороны, подписавшие Конвенцию по киберпреступности Европейского совета, должны принять такие же меры по отношению к странам- оплотам киберпреступности. Им нужно обязать Россию, Белоруссию и другие пренебрегающие нормами права государства начать вводить законы против киберпреступлений. В противном случае их должны ждать последствия. Одним из таких последствий может быть ограничение [[109]](#footnote-110)

Повестка дня

и инспектирование всего интернет-трафика, поступающего из этих стран. Это стоит попробовать.

4. Д □ **ГО ВОР** ОКВ

Четвертым пунктом программы должен стать посвященный кибервойне договор, подобный ОСНВ (Договор об ограничении стратегических наступательных вооружений), который мы назовем Договором об ограничении кибервойны, ОКВ. Соединенные Штаты должны обсудить его положения со своими главными союзниками, а затем внести их в ООН. Как ясно из названия, главная цель договора — ограничить кибервойну, а не стремиться к глобальному запрету хакерства или киберразведки. В Договоре об ограничении стратегических наступательных вооружений и последовавшем за ним Договоре о сокращении стратегических наступательных вооружений разведка не только принималась как неизбежность, но и считалась средством обеспечения «помехозащищенности».

Когда контроль над вооружениями наладился, а доверие и опыт возросли, были приняты новые, более широкие соглашения. Договор ОКВ должен начинаться с принятия следующих положений:

0 Учредить Центр по снижению киберугрозы для обмена информацией и обеспечения содействия государствам — участникам договора.

0 Создать такие понятия международного права, как обязательство содействовать и национальная ки- берответственностъ, которые обсуждались ранее.

0 Принять решение о ненападении на гражданские инфраструктуры, которое будет сниматься, если две [[110]](#footnote-111)

Третья мировая война: какой она будет?

страны ведут активные военные действия или одна страна была атакована другой с помощью кибероружия.

О Запретить подготовку поля боя в мирное время, а именно размещение лазеек и логических бомб в гражданской инфраструктуре, включая энергосистему, систему железных дорог и так далее.

G) Наложить запрет на изменение данных или повреждение сетей финансовых институтов в любое время, а также подготовку к подобным действиям посредством размещения логических бомб.

Позже, когда мы заключим Договор об ограничении кибервойны и обретем некоторый опыт в его соблюдении, можно будет подумать о его расширении. Для начала необходима договоренность о ненападении на гражданские объекты, а не полный запрет кибератак, поскольку государства не должны кривить душой, подписывая обязательства. Страны, вовлеченные в вооруженный конфликт или ставшие жертвой кибератаки, наверняка решат использовать кибероружие. Более того, мы не хотим заставлять государства, ставшие жертвами кибератаки, отвечать на нее наспупательной операцией из-за нашего запрета на кибератаки. Договор не будет препятствовать кибератакам на военные объекты. Не будет он и запрещать подготовку поля боя на военных объектах, поскольку для такого запрета необходим ряд компромиссов, к тому же он осложнит применение ОКВ-1. Тем не менее размещение логических бомб в военных сетях другого государства дестабилизирует положение, и нам следует публично заявить, что в случае обнаружения таких действий мы будем расценивать их как демонстрацию враждебных намерений.

Сложно будет проконтролировать тех, кто действует от лица государства, но в договоре ОКБ ответственность

 з 1 в

Повестка дня

за прекращение их деятельности должны нести государства — участники конвенции. Нужно потребовать, чтобы страны тщательно отслеживали и пресекали хакерские атаки, начинающиеся с их территории. Они должны действовать быстро и в том случае, если их об этом уведомят другие страны через Центр по снижению киберугрозы. Этот центр, созданный по условиям договора, обязаны будут спонсировать подписавшиеся стороны, и в нем будут работать специалисты по сетевой и кибербезопасности. Центр может назначать экспертные группы для помощи в расследованиях и наблюдения за тем, насколько активно и старательно страны расследуют конкретные нарушения. Договор должен включать концепцию национальной киберответственности, в соответствии с которой тот факт, что страна после уведомления не пресекает угрозу, будет считаться нарушением договора. Он должен также предусматривать обязательство содействовать центру и другим странам, подписавшим договор.

В договоре придется предусмотреть проблему атрибуции, которая касается не только стран, организующих работу своих гражданских «хактивистов», которых также нужно учесть в договоре. Атрибуция — тоже сложный вопрос, поскольку страны, как правило, проводят кибератаки через другие государства, а иногда и запускают их не со своей территории. Центр мог бы исследовать заявления государств об их непричастности к кибератаке и позволить другим странам судить, нарушило ли конкретное государство условия договора. Если нарушение очевидно, страны — участники договора могут вводить санкции, самые разные, начиная от отказа в предоставлении виз или запрета на въезд определенным лицам и заканчивая ограничением доступа ко Всемирной сети для интернет-провайдера. Самой крайней мерой может быть ограничение потоков трафика из страны. И наконец, страны-участни- [[111]](#footnote-112)

Третья мировая война: какой она будет?

цы могут сообщить о проблеме в ООН и порекомендовать введение более широких экономических и прочих санкций.

Договор должен ограничиваться только проблемами кибервойны. Не нужно, чтобы он становился международным регулятивным органом, координирующим весь Интернет, как некоторые предлагают. Обременение его такими обязательствами гарантирует, что он будет противоречить интересам США и других стран. Сам по себе договор не прекратит кибератаки на гражданские объекты, но попытки их организации будут обходиться дороже. Принятие ОКВ как международной нормы даст знать кибервоинам и их покровителям во властных структурах, что если сосед раздражает вас, не нужно первым делом атаковать его в киберпространстве. После принятия договора ОКВ единственным поводом для вовлечения в оборонительную кибервойну станет атака другого государства. Применение кибероружия против гражданских целей станет нарушением международного закона. Странам, которые подпишут договор ОКВ, придется обеспечивать тщательный внутренний контроль, чтобы помешать своим кибервоинам вести какие-либо действия без должного разрешения.

5. Киберпространство

СРЕДНЕГО ВОЗРАСТА

Пятый элемент борьбы с кибервойной — это более безопасная сетевая архитектура. Интернету уже сорок, он входит в средний возраст, но при этом не слишком изменился со времен своей юности. Конечно, ширина полосы пропускания возросла, появились беспроводная связь и множество мобильных устройств. Но основная архитектура Интернета, при создании которой никто серьезно [[112]](#footnote-113)

Повестка дня

не задумывался о кибербезопасности, осталась неизменной. Хотя считалось, что многие «глюки» и проблемы безопасности исчезнут, когда на смену старым, полным багов операционным системам Microsoft придет Vista, а потом Windows 7, проблемы остаются даже в самых распространенных программах операционных систем.

Когда я спросил руководителя отдела сетевой безопасности телекоммуникационной компании AT&T, чем бы он занялся, если бы на один день стал «киберцарем», он, не задумываясь, ответил, что программным обеспечением. Эд Аморозо за день видит больше проблем безопасности, чем большинство специалистов по компьютерной безопасности за год. «Программное обеспечение — это самая главная проблема. Мы должны найти способ писать более безопасные программы с меньшим количеством ошибок. Пусть правительство спонсирует исследования и разработки именно в этой области». Хакеры проникают в чужие сети чаще всего потому, что получают доступ к «корню», или статус администратора, через обнаруженный ими «глюк» в программном обеспечении. В связи с этим исследовательские усилия в первую очередь должны быть направлены на две цели. Нам нужно продуктивнее выявлять ошибки и уязвимые места существующих программ, то есть всячески их тестировать. И в то же время мы должны иметь возможность писать новые программные приложения и операционные системы с нуля практически без дефектов.

Хотя люди боятся роботов и искусственного интеллекта (забывая о том, что мы уже бок о бок работаем с ними), пожалуй, стоит подумать о том, как использовать искусственный интеллект для написания кода — то есть создать правила для написания безопасного и элегантного кода. Это довольно большой проект, он потребует государственной поддержки, но разработать интеллектуальную программу, которая будет писать софт, вполне реально.

32 1

Третья мировая война: какой она будет?

Искусственный составитель кода сможет конкурировать с известными разработчиками программного обеспечения, как Deep Blue соперничает с настоящими шахматистами. Можно посадить экспертов, предоставив им открытые исходные коды, и даже привлечь всемирно известных светил.

Работа, проделанная изобретателями Интернета 40 лет назад, имеет большую ценность, чем они могли себе представить. Теперь те, кто финансировал создание Интернета, должны финансировать работу по его усовершенствованию. Сегодняшние исследования в сфере кибербезопасности фрагментарны и, согласно данным президентской комиссии, недостаточно финансируются. Нужен свежий взгляд на киберпространство разработчиков, которые способны думать о новых протоколах, способах аутентификации, усовершенствованных подходах к авторизации доступа, равномерной шифровке трафика и неподвижных данных.

В DARPA (Управлении перспективного планирования оборонных научно-исследовательских работ), которое финансировало большую часть работ на этапе создания Интернета, появились некоторые признаки обновления. После долгих лет отказа от исследований Интернета ситуация начала меняться. В октябре 2009 года DARPA решило профинансировать деятельность консорциума, в который вошли военный подрядчик Lockheed и производитель маршрутизаторов Juniper Networks, занимающийся созданием нового основного протокола Интернета. На протяжении десятилетий трафик в Интернете разбивается на отдельные цифровые пакеты с собственным адресным пространством, или заголовком. В заголовке содержится основная информация — куда и откуда. Протокол, или формат, таких пакетов получил название TCP/IP (протокол управления передачей/межсетевой протокол). Для

322

Повестка дня

богов и основателей Интернета протокол TCP/IP так же священен, как Десять заповедей. А сейчас DARPA ищет, чем бы заменить этот протокол. Какой ужас! Новый военный протокол позволил бы устанавливать, кто посылает каждый пакет. Он позволил бы присваивать пакетам приоритеты в зависимости от цели и даже зашифровывать содержимое. Военный протокол сначала будет использоваться в сетях Пентагона, но только представьте, что бы он сделал для всего Интернета — он мог бы пресекать киберпреступления, кибершпионаж и во многом кибервойну. DARPA не говорит ни о сроках готовности нового военного протокола, ни о том, как может пройти процесс перехода с TCP/IP. И тем не менее, возможно, благодаря этому Интернет когда-нибудь станет безопасным пространством.

Мы не должны отказываться от того, что имеем, до тех пор, пока не убедимся в том, что альтернатива действительно лучше, а процесс перехода осуществим. Каким может быть этот новый порядок? Киберпространство помимо Интернета может состоять из множества интрасетей, работающих по разным протоколам. У некоторых интрасетей должны быть «тонкие» клиенты — не тощие парни, которые ищут адвоката, а компьютерные терминалы, использующие серверы и мэйнфреймы, а не огромные жесткие диски на каждом столе. Если централизованные мэйнфреймы (да, именно старые добрые мэйнфреймы) выйдут из строя, их продублируют резервные системы, расположенные в другом месте. Мэйнфреймы могут координировать работу интрасетей, предотвращать нарушения защиты, неправильное управление конфигурацией. Трафик внутренней сети будет идти по отдельным кабелям и направляться маршрутизаторами, не связанными со Всемирной сетью. Можно организовать сканирование данных для обнаружения вредоносных программ и резервное копирование данных на серверы, часть которых будет отсо-

323

Третья мировая воина: какой она будет?

единяться от сети в случае сбоя системы. Новые интрасети могут использовать технологии постоянного сканирования для выявления и предотвращения аномальной активности, вторжений, краж личных идентификаторов, вредоносных программ или несанкционированного экспорта данных. Они могут зашифровывать все данные и требовать, чтобы пользователь проходил аутентификацию двумя или тремя надежными методами, прежде чем предоставить ему доступ в сеть. Если бы новые сети использовали коммутацию пакетов, то процедуру идентификации пользователя можно было бы встроить в каждый пакет.

Многие возненавидят эту идею. Первые приверженцы Интернета искренне считали, что информация должна быть свободной и неотъемлемой частью этой свободы служит право анонимного доступа к информации. Сторонники открытого Интернета уверены: если вы хотите прочитать «Манифест коммунистической партии», исследование по лечению венерических заболеваний, отчет о нарушениях прав человека в Китае или посмотреть порно, доступ к этой информации не будет считаться свободным, если каждый будет знать, что вы читаете.

Но значит ли это, что все должно происходить в одной большой анонимной открытой для каждого сети? Винт Серф и другие рассматривают Интернет именно так и скорее провалятся сквозь землю, чем согласятся это изменить. Когда я работал в Белом доме, я предлагал организовать Govnet — внутреннюю сеть федеральных агентств, в которую был бы запрещен доступ тех, кто не прошел серьезную аутентификацию. Винт Серф считал эту идею ужасной, полагая, что она разрушит весь открытый Интернет, если ее примут во множестве маленьких сетей. Поборники принципа неприкосновенности частной жизни, чьи доводы я обычно поддерживаю, тоже невзлюбили мое предложение. Они сочли, что это заставит каждого

**324**

Повестка дня

сотрудника, который захочет перейти на общедоступную веб-страницу в Интернете, проходить процедуру идентификации. Конечно же, в Govnet не было бы общедоступных страниц. Но они все равно попадали бы в публичный Интернет. Словом, встретив такое противодействие, идея Govnet не реализовалась. Возможно, сейчас пришло время к ней вернуться.

Помимо специальной сети для федерального правительства в каких еще сферах нам нужны такие безопасные сети? Перечислим лишь несколько: управление полетами и контроль над воздушными перевозками, деятельность финансовых институтов, управление космическими полетами и, конечно же (давайте скажем хором), электросети. Во всех этих сферах останутся закрытые внутренние сети и доступ в Интернет. Но между Интернетом и интранетом не будет связи в режиме реального времени. В идеале их протоколы, приложения и операционные системы должны быть несовместимы. Но должен оставаться и общедоступный Интернет, который мы продолжим, как и прежде, использовать для развлечения, получения информации, покупок, переписки, борьбы за права человека, ознакомления с медицинскими исследованиями, просмотра порнографии и совершения киберпреступлений. Но если бы мы работали в банке, налоговой службе, железнодорожной компании или (опять громко!) энергетической компании, в рабочее время мы бы использовали специальную безопасную внутреннюю сеть. Такие сети все равно могут стать мишенью в кибервойне, но их непохожесть, применение отдельных маршрутизаторов и оптоволокна, строго изолированные «внутренности» существенно снизят вероятность того, что кто-нибудь сумеет вывести их из строя. Винт Серф и все те, кто верен идее открытой сети, вряд ли этому обрадуются, но перемены нужны.

325

Третья мировая война: какой она будет?

**В**. **«На проводе президент»**

Эти слова услышал воображаемый чиновник из Белого дома из второй главы. Чаще всего именно их не хочется слышать, когда кто-нибудь протягивает вам телефонную трубку в момент кризиса. Шестым пунктом нашей программы станет участие президента. Я знаю, что все, кто работает над внутриполитическими вопросами, уверены, что хотя бы один день в неделю президент, как Сизиф, обязан уделять именно его «камню». Я так не считаю.

Однако президент должен лично санкционировать размещение логических бомб и создание лазеек в политически чувствительных сетях других стран. Поскольку логические бомбы служат демонстрацией враждебных намерений, именно президент должен решать, готов ли он пойти на риск дестабилизации отношений, связанный с их размещением. Именно президент должен оценивать вероятность вовлечения США в вооруженный конфликт с другой страной, и только если эта вероятность высока, он может разрешить размещение логических бомб. Ключевые фигуры конгресса необходимо информировать о таких решениях президента так же, как им сообщают о других секретных акциях. Кроме того, президенту следовало бы ежегодно проверять положение дел в сфере кибершпионажа, подготовки к кибервойне и программах по киберобороне. В ежегодном отчете по киберобороне президенту должно сообщаться о прогрессе в защите магистралей, об организации защиты сетей Министерства обороны и (давайте скажем все хором) защите сетей электропередач.

В рамках этой же ежегодной проверки президенту необходимо докладывать о результатах работы Киберкомандования: в какие сети было осуществлено проникновение, какие варианты действий будут у него в случае кризиса, требуются ли какие-то изменения в уже приня-

326

Повестка дня

тых инструкциях. Этот доклад будет подобен ежегодному обзору секретных операций и периодическому смахиванию пыли с планов ядерной войны. Зная о ежегодных проверках, все будут пытаться сохранить лицо. Президент помимо наблюдения за реализацией кибервоенной стратегии может ежегодно выслушивать доклад Управления по киберобороне о том, что сделано в области защиты правительственных агентств, магистральных интернет-провайдеров и (все вместе) электросетей.

И наконец, президент должен на высшем дипломатическом уровне поспособствовать сокращению китайского кибершпионажа и дать знать, что подобные действия мы рассматриваем как экономическую войну.

Как я предлагал ранее, президент должен использовать возможность, которая предоставляется ему ежегодно на церемонии вручения дипломов выпускникам военных академий, чтобы перед курсантами и их родителями провозгласить доктрину Обамы о киберэквивалентности, согласно которой кибератака будет приравниваться к наступательным действиям и реагировать на нее мы будет оптимальным для нас способом, в зависимости от характера и масштаба провокации. Я считаю, что ему следует упомянуть и о предлагаемой нами глобальной системе национальной киберответственности, которая возлагает на страны задачу борьбы с киберпреступностью и якобы спонтанной деятельностью гражданских «хактивистов», и об обязательстве содействовать в пресечении и расследовании киберпреступлений. Такая доктрина прямо противоположна доктрине Буша, озвученной в Вест-Пойнт1, провозглашавшей нашу готовность бомбить или вторгаться в любую страну, которая пугает нас до того, как она что- нибудь сделает.

Вест-Пойнт — разговорное название Военной академии. 3 2 V

1

Третья мировая война: какой она будет?

После такой речи перед выпускниками военных академий весной президента ждет осеннее выступление с ежегодным обращением на открытии сессии Генеральной Ассамблеи Организации Объединенных Наций. Глядя с зеленого гранитного подиума на лидеров и представителей 90 стран, он должен произнести примерно следующее.

Технологии компьютерных сетей, которые моя страна подарила миру, стали великой силой — они способствуют развитию международной торговли, обмену медицинскими знаниями, которые уже спасли миллионы жизней, разоблачению нарушений прав человека и благодаря исследованиям ДНК позволяют нам больше узнать, что все мы — потомки одной и той же африканской Евы.

Однако киберпространством злоупотребляют — преступность растет, каждый год оттуда высасываются миллиарды долларов на поддержку незаконной деятельности картелей. Более того, Интернет уже стал полем битвы. Кибероружие легко приводится в действие, а личность атакующего определить очень сложно, поскольку кибероружие способно ударять по тысячам мишеней, совершать крупномасштабные разрушения за секунды и приносить огромный вред, оно служит новым потенциальным источником нестабильности в эпоху обострения и может стать новой угрозой миру.

Будьте уверены, моя страна будет защищать себя и своих союзников в киберпространстве так же, как и везде. Атаку, проведенную на нас в киберпространстве, мы будем считать равнозначной любому другому нападению и отреагируем

32В

Повестка дня

так, как сочтем нужным в зависимости от характера провокации. Но мы также хотим подписать договор и поклясться никогда, в любых конфликтах, не использовать кибероружие первыми для атаки на гражданские цели. Более того, мы хотим способствовать созданию нового международного Центра сокращения киберрисков и принять на себя обязательство помогать другим странам, которые станут жертвой кибератаки.

Кибероружие вовсе не является, как утверждают некоторые, очередным этапом эволюции на пути к бескровной войне. Если его не контролировать, то даже небольшие разногласия могут выйти из-под контроля и разрастись в крупномасштабную войну. А наша цель, цель тех, кто подписал Устав Организации Объединенных Наций в Сан-Франциско более полувека наза, — избавить грядущие поколения от бедствий войны. Я прошу вас присоединиться ко мне и сделать шаг назад от пропасти, которая может стать новым пространством битвы, и принять меры не для ведения войны в киберпространстве, но для борьбы с кибервойной.

Эта была бы прекрасная речь, и она сделала бы мир безопаснее.

**Глоссарий**

BGP — протокол граничного шлюза — программное обеспечение, посредством которого интернет-провайдер сообщает другим провайдерам адреса своих клиентов, чтобы сообщения попадали к нужному провайдеру. Так, к примеру, AT&T может зарегистрировать в своей BGP-таблице австралийского интернет-провайдера. Если пакет был отправлен Verizon, a Verizonне связан с австралийской сетью, маршрутизатор Verizonзайдет в центр коммутации (см. далее) и заглянет в BGP-таблицу, чтобы найти, у кого есть такая связь, и может перенаправить пакет в AT&T, чтобы оттуда он попал в Австралию. BGP-таблицы недостаточно защищены, и их достаточно легко намеренно изменить, что приведет к неправильному выбору путей транспортировки информации.

ззс

Глоссарий

DARPA (ARPA) — агентство по перспективным оборонным научно-исследовательским разработкам США, организация Министерства обороны, которая отвечает за разработки новых технологий для удовлетворения потребностей вооруженных сил США. DARPA финансировало исследования, результатом которых стало создание Интернета. В 1969 году появилась ARPANET — первая сеть с пакетной коммутацией, связавшая четыре университета.

DDoS -атака — распределенная атака типа «отказ в обслуживании» — стандартная технология кибервойны, используемая преступниками. На интернет-сайт, сервер или маршрутизатор обрушивается столько запросов, что он не в состоянии их обработать. В результате сайт отключается. Для проведения таких атак используются ботнеты, с помощью которых атака распределяется с тысяч компьютеров «в унисон».

DNS — служба, которая преобразует текстовый адрес сайта (например, [www.googie.com](http://www.googie.com)) в числовой адрес, используемый для маршрутизации трафика (например, 192.60.521.7294). На нижней ступени иерархии DNS-сервера известна только маршрутная информация внутри компании; компьютеры более высокого уровня могут знать маршрутную информацию на уровне домена, например ряд адресов .net. На самой высокой ступени компьютеры могут обладать маршрутной информацией национального домена, к примеру .de (Германия). DNS-компьютеры уязвимы перед потоком запросов (см. DDoS) и несанкционированными изменениями маршрутной информации, спуфингом, вследствие которого пользователь попадает на поддельную версию веб-страницы.

JWICS — внутренняя сеть Министерства обороны США для передачи секретных данных/специальной закрытой информации (TS/SCI). Секретная информация поступает из систем сбора разведывательных данных, например со спутников (см.NIPRNET и SIPRNET).

NIPRNET — глобальная сеть Министерства обороны США для передачи несекретной информации. NIPRNET связана с Интернетом через несколько порталов. В Министерстве обороны существуют еще две внутренние сети — SIPRNET и JWICS.

331

Глоссарий

SIPRNET — внутренняя сеть Министерства обороны США, предназначенная для передачи конфиденциальной и секретной информации. Министерство обороны классифицирует информацию на пять категорий: несекретная, конфиденциальная, секретная, сверхсекретная и секретные данные/специальная информация. Предполагается, что SIPRNET не соприкасается с несекретной NIPRNET и Интернетом.

SCADA — комплекс программ, управляющий технологическими системами — работой клапанов, насосов, генераторов, трансформаторов и т. д. SCADAсобирает информацию о работе системы и посылает управляющие сигналы на устройства. Команды могут передаваться как через Интернет, так и по радиоканалам. Команды не шифруются, а их выполнение не требует дополнительного подтверждения правильности.

TCP/IP — протокол управления передачей информации, его иногда называют протоколом надежной доставки. Это означает, что вся информация, отправленная по данному протоколу, будет гарантированно доставлена именно тому получателю, которому она отправлялась.

АНБ (Агентство национальной безопасности) — разведывательное агентство, входящее в состав Министерства обороны США. АНБ — основная организация, занимающаяся сбором информации с помощью электронных средств. Штаб-квартира АНБ расположена в Форт-Миде (шатат Мэриленд), часто ее называют просто Форт.

Аутентификация — процедура, задача которой — установить, является ли пользователь сети именно тем, кем себя называет. Простейшая процедура аутентификации — пароль, но существуют специальные программы, которые выведывают чужие пароли. Двухфакторная аутентификация — это использование пароля и чего-то еще, например отпечатка пальца.

Ботнет — сеть компьютеров, которые вынуждены выполнять команды неавторизированного удаленного пользователя, обычно без ведома владельцев. Такие сети компьютеров-«роботов» используются для кибератак на другие системы. В ботнете обычно существует один или несколько управляющих компьютеров, которые используются оператором ботнета для передачи приказов тайно управляемым устройствам. Компьютеры ботнетов

33Z

Глоссарий

часто называют зомби. Ботнеты используются, помимо других целей, для направления потоков сообщений (см. DDoS).

Внеполосное управление — передача управляющей информации отдельно от передачи данных.

Вредоносное ПО (мэлвер) — вредоносные программы, которые заставляют компьютеры или сети делать то, что не хотелось бы их владельцам или пользователям. Примерами мэлвера служат логические бомбы, «черви», вирусы, снифферы пакетов и регистраторы клавиатуры.

Гарантия содействия — подразумевает, что каждая страна в рамках кибервоенного соглашения принимает обязательство помогать другим странам и/или соответствующей международной организации в исследовании и пресечении кибератак, берущих начало на ее территории.

Глубокое инспектирование пакетов — процедура сканирования пакетов данных, из которых состоят электронные письма, веб-страницы и прочий интернет-трафик. Обычно сканируется только заголовок пакета — шапка, где представлена информация куда и откуда. При глубоком инспектировании пакетов происходит поиск определенных шаблонов в содержании пакета. В ходе этой процедуры разыскиваются только цифровые «отпечатки», идентичные или очень похожие на следы известных вредоносных программ или инструментов взлома.

Гражданская инфраструктура — национальные системы, которые обеспечивают функциональность экономики страны: электросети, трубопроводы, железные дороги, авиалинии, телефонные сети и банковская система. В США эти системы состоят из отдельных неправительственных объединений — частных или государственных компаний.

Граничный маршрутизатор — маршрутизатор, расположенный на границе магистральной и локальных сетей, место в Интернете, где локальный трафик вливается в оптоволоконный кабель национального масштаба.

Запаздывание — временной интервал прохождения пакета данных по сети или маршруту. Задержка измеряется в секундах и долях секунды. Скорость передачи данных определяется пропускной способностью сети, которая зависит от характеристик оптоволоконного кабеля, и быстродействием маршрутизаторов.

333

Глоссарий

Запуск по предупреждению — компонент стратегии, согласно которому страна инициирует конфликт (кибервойну), когда данные разведки позволяют предположить, что противник перешел или собирается перейти к враждебным действиям.

Интернет — глобальная компьютерная сеть, дающая доступ к емким специализированным информационным серверам и обеспечивающая электронную почту. Локальные компьютерные сети могут использовать те же программы и протоколы управления, что и в Интернете, но не являться при этом частью Интернета. Такие закрытые сети называются интранет. Между Интернетом и интранетом может существовать связь, как контролируемая, так и несанкционированная.

Кризис нестабильности — в период обострения отношений между странами могут возникать предпосылки или действия, предпринятые одной стороной, которые заставляют другую сторону считать, что в ее интересах перейти к агрессивным действиям. Кризис нестабильности — это состояние, которое может привести к началу военных действий.

Киберпорог — точка принятия решения, когда командующий должен решить, следует ли переходить от действий в киберпространстве к обычным боевым действиям и как это лучше осуществить. Пересечение этой границы — шаг, который может привести к выходу войны из-под контроля.

Логическая бомба — программа или набор команд, которые заставляют систему или сеть осуществлять деструктивные действия, например отключаться и/или стирать данные.

Магистраль — магистральный высокоскоростной кабель, соединяющий сетевые сегменты глобальной сети в единую систему.

Магистральные интернет-провайдеры — пять основных интернет-провайдеров США, которые владеют и управляют крупнейшими национальными оптоволоконными сетями, по которым идет основной кибертрафик.

Национальная ответственность — концепция, согласно которой правительство страны несет ответственность за атаки, начавшиеся с ее территории. Иногда эту концепцию называют «теорией поджигателя» («Если в вашем доме живет человек, который каждую ночь выходит и поджигает дома ваших соседей,

 334

Глоссарий

а вы об этом знаете, нельзя утверждать, что вы не несете за это ответственности».)

Национальный киберпотенциал — общая оценка способности страны вести кибервойну. Она состоит из трех составляющих: наступательные возможности, зависимость страны от компьютерных сетей и способность страны контролировать и защищать свое киберпространство посредством таких мер, как прекращение поступления трафика извне.

Ненападение — установка, в соответствии с которой страна начинает использовать оружие определенного рода только после того, как оно было использовано против нее. Считается, что оружие конкретного вида будет использоваться только в качестве ответной меры против тех, кто уже его применил.

Переполнение буфера — ошибка, которая позволяет неав- торизированному пользователю получить доступ к сети. При отсутствии ограничения на количество вводимых знаков ненадежный пользователь может передавать команды. Например, посетитель веб-сайта может перейти на поле ввода своего адреса и вместо этого ввести команду, которая позволит ему получить такой же доступ к сети, как у администратора.

Провайдер — организация, которая обеспечивает проводную или беспроводную связь домашнего, рабочего или портативного компьютера пользователя с Интернетом. Интернет-провайдерами могут быть телефонные компании или операторы кабельного телевидения.

Преднамеренное обострение конфликта — ситуация, когда одна из сторон конфликта реагирует на атаку или провокацию расширением масштаба или уровня конфликта и при этом заявляет, что, если ее требования (к примеру, прекращение войны) не будут выполнены, она готова пойти еще дальше. Предполагается, что расширение военных действий демонстрирует серьезность намерений и силу потенциала, а также отказ вести затяжной вялотекущий конфликт. Это похоже на игру в покер, когда один из игроков повышает ставки в надежде убедить соперников сдаться.

Сервер — компьютер, к которому обращаются для получения информации, хранимой на нем, будь то веб-страницы или

335

Глоссарий

электронные письма. Как правило, серверы работают без постоянного мониторинга со стороны человека. Компьютеры, которые управляют движением интернет-трафика, также являются серверами.

Хакер — чрезвычайно квалифицированный специалист- компьютерщик, человек, который понимает самые основы работы компьютерных систем. Изначально хакерами называли программистов, которые исправляли ошибки в программном обеспечении. В просторечии так называют тех, кто использует свои навыки для получения доступа к чужим компьютерам или сетям без авторизации.

Шифрование — представление информации в виде, нечитаемом для тех, кто не имеет ключа для расшифровки. Тот, кто перехватит или украдет зашифрованный поток информации (или «данные в состоянии покоя»), не сможет его прочитать.

Шпионаж — разведывательная деятельность, направленная на сбор информации, доступ к которой другая страна (или субъект) пытается запретить. Кибершпионаж — это несанкционированное проникновение государства в сети, компьютеры, базы данных другой страны с целью копирования и эксфильтрации конфиденциальной информации.

Центр коммутации — здание, в котором расположено огромное количество сетевых маршрутизаторов. Здесь происходит коммутация интернет-трафика и прочего кибертрафика, включая голосовую телефонию.

«Черный» ход — фрагмент программы, который умышленно добавляется для обеспечения несанкционированного вмешательства в ее работу или работу сети. После взлома киберпреступник или кибервоин может оставить ловушку, которая даст ему возможность проникнуть в эту же сеть или программу в следующий раз. Иногда такие лазейки называют «троянами», или «троянскими конями», в честь уловки, которую, как считается, применили древние греки, чтобы проникнуть в Трою.

Эквивалентность, киберэквивалентность — установка, в соответствии с которой кибервоенная атака рассматривается как любая другая атака, включая наступательные действия, а способ реагирования на нее выбирает пострадавшая страна в зависимости от масштабов ущерба и прочих существенных факторов.

 3

1. [↑](#footnote-ref-2)
2. Брукингский институт — научно-исследовательская организация, существующая за счет грантов и пожертвований. Основан в 1927 году в результате слияния Института исследования государственного управления, Института экономики и Школы государственного управления при Вашингтонском университете; носит имя одного из основных учредителей Р. Б. Брукингса. — Примеч. ред. [↑](#footnote-ref-3)
3. Концентрические кольца-коридоры в здании Пентагона обозначаются латинскими буквами от А (центральное кольцо) до Е. Считается, что Е-кольцо Пентагона занимает администрация. — Примеч. ред.

В [↑](#footnote-ref-4)
4. Уильям (Билли) Митчелл — американский военный, генерал, считающийся отцом военно-воздушных сил США. [↑](#footnote-ref-5)
5. № 4595 [↑](#footnote-ref-6)
6. Англоязычное название Грузии совпадает с названием штата Джорджия, в котором находится Атланта, хорошо известная читателям по книге и фильму «Унесенные ветром». — Примеч. ред.

35 [↑](#footnote-ref-7)
7. National Mall— национальный парк, комплекс разнообразных памятников и музеев в историческом центре Вашингтона. — Примеч. ред.

4Р [↑](#footnote-ref-8)
8. SCAD А — программное обеспечение, контролирующее работу сетей, в том числе и сетей электропитания.

52 [↑](#footnote-ref-9)
9. № 4595 [↑](#footnote-ref-10)
10. □ [↑](#footnote-ref-11)
11. Недостаток, неизвестный производителям программного обеспечения, для которого не существует патча или способа устранения.

 В 1 [↑](#footnote-ref-12)
12. № 4595 [↑](#footnote-ref-13)
13. S [↑](#footnote-ref-14)
14. □□ [↑](#footnote-ref-15)
15. □ 1 [↑](#footnote-ref-16)
16. 02 [↑](#footnote-ref-17)
17. 03 [↑](#footnote-ref-18)
18. 04 [↑](#footnote-ref-19)
19. □ 6 [↑](#footnote-ref-20)
20. 07

1MCI (Microwave Communications, Inc.) — корпорация, ранее один из ведущих операторов дальней телефонной связи США. [↑](#footnote-ref-21)
21. G S [↑](#footnote-ref-22)
22. 09 [↑](#footnote-ref-23)
23. 1 □ [↑](#footnote-ref-24)
24. 12 [↑](#footnote-ref-25)
25. 1 4 [↑](#footnote-ref-26)
26. 1 5 [↑](#footnote-ref-27)
27. 1 е [↑](#footnote-ref-28)
28. 17 [↑](#footnote-ref-29)
29. 1 в [↑](#footnote-ref-30)
30. 1 9 [↑](#footnote-ref-31)
31. *20* [↑](#footnote-ref-32)
32. 2 1 [↑](#footnote-ref-33)
33. 22 [↑](#footnote-ref-34)
34. 23 [↑](#footnote-ref-35)
35. 24 [↑](#footnote-ref-36)
36. 25 [↑](#footnote-ref-37)
37. 26 [↑](#footnote-ref-38)
38. № 4595 [↑](#footnote-ref-39)
39. за [↑](#footnote-ref-40)
40. з 1 [↑](#footnote-ref-41)
41. 3 2 [↑](#footnote-ref-42)
42. 33 [↑](#footnote-ref-43)
43. 35 [↑](#footnote-ref-44)
44. 36 [↑](#footnote-ref-45)
45. 37 [↑](#footnote-ref-46)
46. АО [↑](#footnote-ref-47)
47. 42 [↑](#footnote-ref-48)
48. 43 [↑](#footnote-ref-49)
49. 45 [↑](#footnote-ref-50)
50. 4S [↑](#footnote-ref-51)
51. 47 [↑](#footnote-ref-52)
52. 48 [↑](#footnote-ref-53)
53. 49 [↑](#footnote-ref-54)
54. 5D [↑](#footnote-ref-55)
55. 5 1 [↑](#footnote-ref-56)
56. 52 [↑](#footnote-ref-57)
57. 53 [↑](#footnote-ref-58)
58. 54 [↑](#footnote-ref-59)
59. 56 [↑](#footnote-ref-60)
60. 57 [↑](#footnote-ref-61)
61. 58

' Компания RSA Labs— разработчик криптографических технологий. [↑](#footnote-ref-62)
62. 60 [↑](#footnote-ref-63)
63. Ns 4595 [↑](#footnote-ref-64)
64. 62 [↑](#footnote-ref-65)
65. 63 [↑](#footnote-ref-66)
66. 64 [↑](#footnote-ref-67)
67. Закон о патриотизме, принятый в 2001 году, расширяет полномочия федерального правительства по расследованию террористической деятельности и преследованию лиц, подозреваемых в такой деятельности. В частности, закон разрешает властям задерживать иностранцев на срок месяц и более без предъявления обвинений и проводить закрытые судебные слушания таких дел.

165 [↑](#footnote-ref-68)
68. 66 [↑](#footnote-ref-69)
69. 67 [↑](#footnote-ref-70)
70. 6S

1 Клуб Капитолийского холма — вашингтонский политический клуб, объединяющий сторонников Республиканской партии. [↑](#footnote-ref-71)
71. 69 [↑](#footnote-ref-72)
72. *70* [↑](#footnote-ref-73)
73. 7 1

1Best Buy («Лучшая покупка») — крупнейшая в Северной Америке сеть магазинов бытовой электроники. [↑](#footnote-ref-74)
74. 72 [↑](#footnote-ref-75)
75. 73 [↑](#footnote-ref-76)
76. 75 [↑](#footnote-ref-77)
77. 76 [↑](#footnote-ref-78)
78. 77 [↑](#footnote-ref-79)
79. 7 В [↑](#footnote-ref-80)
80. SD [↑](#footnote-ref-81)
81. в 1 [↑](#footnote-ref-82)
82. BZ [↑](#footnote-ref-83)
83. 84 [↑](#footnote-ref-84)
84. S5 [↑](#footnote-ref-85)
85. S6 [↑](#footnote-ref-86)
86. BS [↑](#footnote-ref-87)
87. S9 [↑](#footnote-ref-88)
88. 1. RAND— научно-исследовательский центр в Санта-Монике (штат Калифорния), один из крупнейших «мозговых трестов» страны. Изучает проблемы международных отношений и национальной безопасности, научно-технические, экономические и военные вопросы. [↑](#footnote-ref-89)
89. 92 [↑](#footnote-ref-90)
90. № 4595 [↑](#footnote-ref-91)
91. 95 [↑](#footnote-ref-92)
92. 96 [↑](#footnote-ref-93)
93. 97 [↑](#footnote-ref-94)
94. 98 [↑](#footnote-ref-95)
95. 09 [↑](#footnote-ref-96)
96. 1 □ [↑](#footnote-ref-97)
97. «Принцип необходимого знания» — стратегия защиты информации, соответственно которой пользователь получает доступ только к данным, безусловно необходимым ему для выполнения конкретной функции. [↑](#footnote-ref-98)
98. 11 [↑](#footnote-ref-99)
99. 12 [↑](#footnote-ref-100)
100. 1 4 [↑](#footnote-ref-101)
101. 1 V [↑](#footnote-ref-102)
102. Raytheon Company— авиастроительная компания, разрабатывающая и внедряющая различные технологии в оборонной области.

 239 [↑](#footnote-ref-103)
103. В 5 [↑](#footnote-ref-104)
104. 1 □ [↑](#footnote-ref-105)
105. 1 1 [↑](#footnote-ref-106)
106. 12 [↑](#footnote-ref-107)
107. 13 [↑](#footnote-ref-108)
108. 1 4 [↑](#footnote-ref-109)
109. 1 6 [↑](#footnote-ref-110)
110. 1 7 [↑](#footnote-ref-111)
111. 1 э [↑](#footnote-ref-112)
112. 2 □ [↑](#footnote-ref-113)