СОДЕРЖАНИЕ

ОБ ИСТОЧНИКАХ

Я — журналист и на темы информационной безопасности и электронного шпионажа пишу уже более 10 лет. В основу книги легли материалы более тысячи интервью, которые я провел за эти годы с бывшими и действующими правительственными чиновниками, военными, руководителями и сотрудниками корпораций, специалистами, исследователями и активистами. В течение двух лет работы над этим проектом я вновь встречался с людьми, которых считаю своими самыми надежными и доверенными источниками. Были и те, у которых я брал интервью впервые. Особенное внимание при написании этой книги я уделял беседам с действующими правительственными чиновниками и сотрудниками военных ведомств, чья работа непосредственно связана с политикой и деятельностью в области информационной безопасности. Эти люди работают на передовой, а не отсиживаются в тылу. Я крайне признателен им за то, что они нашли время для доверительного обсуждения со мной тем, которые многие представители власти отказываются обсуждать публично, поскольку слишком часто вопросы касаются секретных материалов и операций.

Многие люди, с которыми я разговаривал, дали разрешение на цитирование их слов в печати, и в этом случае я указы-

ваю имена своих собеседников в тексте или в сносках. Некоторые потребовали, чтобы я не упоминал их имен, а иногда и названий агентств и компаний, в которых они работают. Прискорбно, но зачастую журналисты при освещении вопросов, касающихся секретных тем в области национальной безопасности, не могут полностью раскрыть источники информации. Я не верю, что хоть кто-нибудь из моих собеседников, с кем я разговаривал при сборе материала для этой книги, предоставил мне сведения, которые могут подвергнуть риску национальную безопасность или жизни людей. Но я удовлетворил просьбу этих людей об анонимности по двум причинам.

Во-первых, представленная ими информация была важна для повествования и не могла быть получена из других источников либо подтверждала и дополняла данные, полученные от других не анонимных источников или из открытых документов. Как ни удивительно, но достаточно большое количество информации о кибервойне опубликовано в открытых источниках и никогда не засекречивалось. Во-вторых, эти люди, общаясь со мной, подвергали серьезному риску свое профессиональное благополучие и даже, теоретически, личную свободу. Обсуждая методы ведения кибервойны и шпионажа, источнику зачастую сложно определить, раскрывает он секретную информацию или всего лишь близко подходит к границе дозволенного. Если источники, с которыми я обсуждал эти вопросы, будут идентифицированы по их именам, они могут потерять допуск к сверхсекретным материалам, а это значит, что они фактически не смогут найти работу по профессии в сфере обеспечения национальной безопасности.

Кроме того, эти люди рискуют подвергнуться уголовному преследованию из-за разговоров со мной. Администрация Обамы крайне нетерпима к государственным служащим, которые делятся информацией с журналистами. За разглашение секретной информации Министерство юстиции подвергло уголовному преследованию больше специалистов, чем все предыдущие Администрации вместе взятые. Проще говоря, настали опас-

ные времена для общения с журналистами. Для бывших государственных служащих и военных риск еще выше. Несколько отставных руководителей разведки рассказали мне, что в течение последнего года разведслужбы, на которые они продолжают работать в качестве подрядчиков, дали им понять, что стоит прекратить общение с журналистами, если они хотят продолжать получать государственные заказы. В тех случаях, когда я использую информацию анонимных источников, я старюсь объяснить, почему этим людям можно доверять, при этом я выполняю свое обязательство не раскрывать данные, которые могли бы их идентифицировать.

Значительная часть этой книги основана на документах, взятых из открытых источников. К ним относятся правительственные отчеты и презентации, свидетельские показания в конгрессе, записи выступлений высокопоставленных чиновников, а также крайне подробные и непрерывно множащиеся аналитические отчеты частных исследователей по безопасности. Когда я начинал работать над книгой, многие коллеги спрашивали, как я смогу писать работу на столь секретную тему, как кибербезопасность. Однако я был удивлен, когда узнал, что огромное количество достоверной и обличительной несекретной информации существует в открытых источниках. Из нее я извлек значительное количество сведений, которые подрывают заявления многих государственных чиновников о том, что эта тема слишком деликатна и уязвима, чтобы обсуждать ее публично. За последние несколько лет все больше госчиновников и военных руководителей стали говорить о кибервойне и шпионаже более открыто, и меня это обнадеживает. Общество не сможет понять эти проблемы, а власти — принимать обоснованные законы и вести взвешенную политику без непредвзятого и откровенного публичного обсуждения данных вопросов.

ПРОЛОГ

Шпионы появились без предупреждения. Они тихо занимались своим ремеслом, воруя секреты у самой мощной и влиятельной военной организации. Им удалось поработать несколько месяцев, прежде чем их присутствие было замечено. А когда американские власти наконец обнаружили воров, стало понятно, что уже слишком поздно. Был нанесен большой ущерб.

Незваные гости ускользнули с огромным объемом технической и конструкторской информации о самом важном новом оружии Соединенных Штатов — самолете-истребителе последнего поколения, который разрабатывался по программе, получившей название «Единый ударный истребитель» (Joint Strike Fighter, JSF). Предполагалось, что этот истребитель станет самым совершенным боевым самолетом, который будет задействован всеми родами войск и обеспечит господство ВВС США в воздухе на десятилетия. Истребитель, получивший название F-35, был самым технически сложным оружием из когда-либо созданных, а кроме того, при оценочной стоимости проекта в $337 млрд еще и самым дорогим.

Все указывало на то, что преступником, совершившим с конца 2006 г. серию дерзких взломов, является военное ведомство Китая. У этой организации были мотив и возмож-

ности украсть секретные сведения об F-35. Особенно их интересовали подробности о системе, позволяющей истребителю скрываться от вражеских радаров. Десятки лет Китай проводил агрессивную кампанию по шпионажу в вооруженных силах своего самого серьезного противника — США. Начиная с конца 1970-х гг. агенты китайских спецслужб часто посещали и даже работали в американских университетах, государственных исследовательских лабораториях и компаниях, выполнявших оборонные подряды, организуя утечки конструкторской документации по системам вооружения, в том числе по ядерным боеголовкам.

Однако было нечто новое в этой истории. Шпионы не забирали бумажные документы из офисов и не подслушивали разговоры инженеров в комнатах отдыха. Они воровали информацию удаленно с помощью компьютерных сетей. Программу разработки JSF взломали.

Специалисты по информационной криминалистике, задействованные в работе над F-35, начали поиск преступников. Чтобы понять, как хакерам удалось проникнуть в систему, пришлось принять образ мыслей взломщиков, начать думать, как они. Так в команде появился свой хакер. Это был бывший военный офицер и ветеран секретных кибервойн. Он приобрел ценный опыт в первых армейских информационных битвах середины 1990-х гг. — тех, в которых требовалось скорее проникнуть в голову противника, чем в его базы данных. Это были вариации классических пропагандистских войн в компьютерную эпоху; здесь от военных хакеров требовалось знать, как внедриться во вражеские коммуникационные системы и передать сообщения так, чтобы их приняли за сообщения из доверенного источника. Позже основной задачей бывшего офицера стала слежка за повстанцами и террористами на территории боевых действий в Ираке с помощью контроля их мобильных телефонов и интернет-сообщений. И хотя ему было всего сорок с небольшим, по стандартам профессии он был опытным сотрудником.

Вот что было известно специалистам BBC об утечке по программе JSF: данные были украдены не с компьютера военного ведомства. По всей видимости, утечка информации произошла из компании, привлеченной к работам по проектированию и созданию истребителя. Шпионам пришлось сделать обманный маневр, нацелившись на работавшие по договорам с Министерством обороны компании, компьютеры которых содержали огромное количество сверхсекретной информации, в том числе и некоторые чертежи узлов истребителя F-35, такие же, какие можно было обнаружить на компьютерах военного ведомства. Тактика шпионажа была выбрана умно. Подрядные компании необходимы американским военным; без их участия не летают самолеты, не ездят танки и не строятся корабли. Но их компьютеры обычно защищены слабее, чем сверхсекретные военные компьютерные сети, самые важные из которых даже не подключены к Интернету. Хакеры просто нашли другой способ проникновения, нацелившись на фирмы, которым военные поручали так много разных важных задач.

Военные следователи не были уверены, в какой из компаний образовалась брешь в системе защиты информации. Это могла быть и Lockheed Martin, ведущий подрядчик по программе F-35, а может быть, одна из компаний-соисполнителей — Northrop Grumman или BAE Systems, или какая-то другая компания из более тысячи фирм и поставщиков, привлеченных к работе над многочисленными сложными механическими или электронными системами самолета. Программы, помогающие управлять этим самолетом, состоят из более 7,5 млн строк кода — это почти в три раза больше, чем в программах управления самых современных истребителей. А еще 15 млн строк кода управляют логистикой, обучением и другими вспомогательными системами. Для шпиона такая ситуация соответствует, по военной терминологии, «обстановке с многочисленными целями». Куда ни посмотри, можно найти секреты о системах навигации самолета, его бортовых датчиках, системах контроля и вооружении.

Начать расследование было разумно с ведущего подрядчика — компании Lockheed Martin. На компьютерах компании хранилась крайне важная информация о самолете, но что, может быть, было более существенно, компания руководила многими соисполнителями, которым сообщались разные детали по проекту F-35. Однако, когда «хакер» из BBC появился в офисе Lockheed, чтобы начать расследование, его встретили не технические специалисты или военные офицеры, курировавшие проектирование F-35, его поприветствовали юристы компании.

«Хакер» попросил ноутбук. «Зачем он вам?» — спросили юристы. Он объяснил, что ему нужно посмотреть на организацию внутренних компьютерных сетей для начала. Кроме того, он хотел узнать, какими программным обеспечением и приложениями пользуются обычные сотрудники Lockheed. В этих программах могли быть уязвимости или лазейки в системе защиты, позволяющие пользователю (в том числе легальному: например, системному администратору) обойти предусмотренные средства обеспечения безопасности, такие как экран ввода логина и пароля пользователя, и получить доступ к компьютеру. Взломщик мог использовать эти точки доступа, чтобы получить плацдарм внутри информационной инфраструктуры компании. Все, что нужно было шпионам, — это точка входа, место, где устанавливается цифровая «опорная база», из которой можно проводить свои операции.

Адвокаты выдали «хакеру» абсолютно новый ноутбук, прямо из коробки. Его еще ни разу не подключали к корпоративной сети Lockheed. К нему ни разу не прикасался ни один из сотрудников компании, кроме адвоката. «Хакер» возмутился. Фактически его просили выяснить, как в дом проникли взломщики, при этом не позволили осмотреть и изучить место преступления.

Почему компания Lockheed, которая зарабатывала на проекте создания Единого ударного истребителя миллиарды долларов, не сделала все возможное, чтобы помочь найти шпио-

нов? Может быть, потому, что тщательное расследование показало бы, насколько слабо защищены были компьютерные сети компании. Возможно, следователи обнаружили бы и другие утечки информации по другим военным программам. Рассказы о том, что сеть была взломана шпионами, которые никогда не появлялись на объектах, принадлежащих компании, вряд ли могли помочь делу. Lockheed — крупнейший поставщик товаров и услуг для американского правительства. В 2006 г. компания заключила контракты на $33,5 млрд, причем более 80% — с Министерством обороны США. Мало того, эти цифры не учитывают секретную работу в интересах разведывательных агентств, объем которой, несомненно, увеличит общую сумму еще на несколько миллиардов. В Lockheed не могли допустить, чтобы компания выглядела как слабый хранитель ценных государственных тайн, и на самом деле ни один из оборонных подрядчиков не может допустить подобного. Кроме того, акции Lockheed свободно обращаются на открытом рынке ценных бумаг. Скорее всего, акционеры крайне негативно отреагировали бы на новости о том, что компания не может защитить ключевую для своего многомиллиардного бизнеса информацию.

Неудивительно, что «хакер» не нашел ничего ценного на предоставленном ноутбуке. Высокопоставленные военачальники, курировавшие проект JSF, были вне себя из-за обнаружившихся утечек информации. Они потребовали, чтобы и Lockheed, и все остальные вовлеченные в проект подрядчики оказали самую широкую помощь в расследовании. С их точки зрения, эти компании не просто работали на правительство. В действительности они сами были частью правительства, получая деньги налогоплательщиков и выполняя сверхсекретную работу. Военные углубили расследование, и за несколько месяцев «хакер» и его помощники тщательно изучили компьютерные сети компании Lockheed и других подрядчиков, работавших над проектом.

Следователи обнаружили, что случай проникновения не был единичным. Сети Lockheed взламывались неоднократно.

Они не могли сказать точно сколько, но ущерб от проникновения был оценен как значительный, принимая во внимание неконтролируемый доступ взломщиков к сетям и объем украденной информации. В результате всей операции, целью которой были и другие компании, шпионам удалось украсть несколько терабайт данных о внутреннем устройстве истребителя. Такое количество информации в численном выражении составляет примерно 2% от объема собрания Библиотеки Конгресса.

В иные времена внедрение агента в одну из американских корпораций и установка прослушивающего устройства стали бы выдающимся шпионским подвигом. Сейчас же нужно всего лишь заразить компьютер вредоносной программой или через Интернет перехватить канал связи и скачивать передаваемую информацию, находясь на другом конце света.

Чем больше следователи прочесывали логи интернет-соединений и содержимое компьютерных дисков, тем больше жертв взлома они находили. Шпионам удалось проникнуть в сети субподрядчиков в нескольких странах мира. Технические специалисты отследили IP-адреса и методы проникновения, использованные шпионами. Практически не было сомнений, что шпионы были из Китая и, вероятно, принадлежали к той же группе, которая была причастна к другим взломам, нацеленным на американские военные ведомства и крупные компании, работающие преимущественно в области высоких технологий и энергетики. Размах, настойчивость и изощренность китайской киберразведки стали настоящим сюрпризом для руководителей американских военных и разведывательных ведомств. Власти США так и не раскрыли для широкой публики масштаб бедствия, то ли из-за смущения и нежелания стать объектом насмешек, то ли чтобы не дать понять китайцам, что за ними велась слежка.

Шпионы охотились за деталями конструкции истребителя и его способности выдерживать нагрузки, возникающие в полете и во время воздушного боя. Очевидно, что таким обра-

зом они пытались обнаружить слабые места самолета, а кроме того, были заинтересованы в информации, которая поможет создать собственный истребитель. Последствия были ужасающими. Из предположения, что шпионы работали на китайские вооруженные силы, следовало, что однажды американские истребители могут столкнуться в бою со своими копиями. Американским летчикам, возможно, придется иметь дело с неприятелем, который будет осведомлен об уязвимых местах истребителя F-35.

На тот момент информация о системах, которые позволяют самолету обнаруживать противника, и системах управления истребителем, позволяющих выполнять сложные маневры, была в безопасности, поскольку хранилась на компьютерах, не имеющих выхода в Интернет. Но годом позже следователи все еще обнаруживали новые утечки, которые пропустили ранее. Можно было предположить, что кампания по шпионажу продолжается, и целью ее являются даже компьютеры, не подключенные к Интернету. Ведь факт отсутствия выхода в общедоступную сеть, говорит о том, что на этих компьютерах содержится наиболее важная информация.

В конце концов следователи пришли к выводу, что изначально шпионы вовсе не были нацелены на информацию о F-35, их целью был другой секретный проект. Вероятно, принимая во внимание огромный объем незащищенных данных, найденных в компьютерных сетях компании, они решили, что проект F-35 окажется более легкой целью. Изменение планов прямо в процессе ограбления давало понять, насколько нагло и дерзко вели себя шпионы. У некоторых представителей власти вызвало удивление, как мало взломщики прилагали усилий, чтобы скрыть следы проникновения. Казалось, они абсолютно не тревожатся о том, что их обнаружат. Они как будто бросали американцам вызов, предлагая найти их, будучи при этом в полной уверенности, что этого не произойдет.

Шпионы не только получили потенциально полезные разведданные, но еще и существенно задержали разработку истре-

бителя F-35. Власти США позже заявили, что наглое проникновение в компьютеры субподрядчиков привело к тому, что программисты вынуждены были переписать программный код для систем истребителя, задержав таким образом завершение проекта на один год и на 50% повысив его стоимость. Китайцам и не придется столкнуться в бою с этим истребителем, если он так и не взлетит. Кроме того, Китай значительно продвинулся в проектировании собственного самолета. В сентябре 2012 г. во время визита министра обороны США Леона Панетты китайские власти опубликовали фотографии новейшего истребителя, стоящего на аэродроме. Он имел сходство с F-35, но не повторял его конструкцию в точности, что признали и американские власти. При создании китайского истребителя частично была использована информация, украденная шпионами у американских компаний шестью годами ранее.

Руководители компаний не знали точно, зачем их вызвали в Пентагон. Как и то, зачем им временно выдали допуск к государственной тайне. Оглядываясь вокруг, они видели много знакомых лиц: генеральные директора или их представители, работавшие в 12 крупнейших американских корпорациях — подрядчиках Министерства обороны США: Lockheed Martin, Raytheon, General Dynamics, Boeing, Northrop Grumman и др. Эти компании, по праву считающиеся ведущими в своих отраслях, десятилетиями создавали американскую военную машину. Какой бы ни была причина, по которой их собрали в такой спешке в штаб-квартире Министерства обороны тем летним днем 2007 г., вряд ли это были хорошие новости.

Руководители компаний собрались внутри «помещения для работы с конфиденциальной информацией» (SCIF) — специальной комнаты, недосягаемой для подслушивающих устройств. Пригласившие их начали так называемый брифинг об угрозах, и это было обычной практикой, поскольку военные чиновники регулярно обсуждали с руководителями оборонных предприятий существующие угрозы национальной безопасно-

сти. Однако этот брифинг был посвящен угрозам безопасности корпоративной. А если конкретно, то речь шла о тех предприятиях, руководители которых собрались в этой комнате.

Военные специалисты, занимавшиеся расследованием утечек информации по проекту F-35, рассказали о том, что они выяснили. Компьютерные сети каждой из компаний были подвергнуты массированной шпионской атаке. Шпионов интересовала не только информация по проекту F-35; они украли всю секретную военную информацию, какую только смогли найти. Шпионам удалось преодолеть слабые средства электронной защиты и скопировать секретные данные на свои серверы. Они отправляли сотрудникам, работавшим над секретными проектами, безобидные, на первый взгляд, электронные письма, которые выглядели так, как будто пришли из надежных источников внутри компании. Когда адресат открывал такое письмо, на его компьютере устанавливался бэкдор*, позволявший китайцам отслеживать каждое нажатие клавиши на клавиатуре, каждый посещенный сайт, каждый файл, скачанный, созданный или отправленный по электронной почте. Сети адресатов оказывались взломаны, а их компьютеры находились под полным контролем. Говоря языком хакеров, военно-промышленный комплекс Америки поимели.

А тем временем шпионы продолжали проникать в сети этих компаний и добывать секретную информацию и перехватывать сообщения сотрудников. Возможно, они и сейчас просматривали частные электронные письма руководителей компаний. «Многие люди поседели, выйдя из этой комнаты», — рассказал Джеймс Льюис, известный эксперт в области информационной безопасности из Центра стратегических и международных исследований — «мозгового центра» в Вашингтоне, которому известны подробности той встречи.

---

* Бэкдор (от англ. backdoor — «черный ход») — лазейка в коде, которую оставляет разработчик, для удаленного манипулирования разработанным им ПО, обычно в случае неуплаты за работы заказчиком. — *Прим. пер.*

Компании оказались слабым звеном в цепи обеспечения безопасности проекта. Представители Пентагона сообщили руководителям, что ответ на кражу военных секретов является неотложным вопросом национальной безопасности. А для самих компаний — вопросом выживания. Их бизнес зависит от денег, получаемых от продажи самолетов, танков, спутников, кораблей, подводных лодок, компьютерных систем и всех прочих технических и административных услуг, оказываемых федеральным властям. Военные дали ясно понять: если подрядчики хотят продолжить свою работу в этой сфере, им придется потрудиться и обеспечить безопасность в своих компаниях.

Однако заниматься этим они будут не в одиночестве.

После этой встречи Министерство обороны стало предоставлять компаниям информацию о кибершпионах и хакерах, за действиями которых наблюдали американские разведывательные службы. На тот момент в Пентагоне отслеживали около дюжины шпионских операций, проводимых разными группами хакеров. Эти группы можно классифицировать по их интересу к определенным военным технологиям, особенностям проведения военных операций, структуре военных организаций и военным подрядчикам. Эта информация об иностранных шпионах была результатом работы американской разведки и собиралась с помощью отслеживания и изучения попыток проникновения в компьютерные сети военных организаций, а кроме того, путем взлома компьютеров и компьютерных сетей врагов Америки. Разведслужбы США также анализировали огромный объем трафика в глобальных телекоммуникационных сетях в поисках вирусов, сетевых червей* и других вредоносных компьютерных программ. Никогда раньше власти США не делились таким количеством секретной информации с частными лицами. Забота о безопасности

* Вредоносные программы, обладающие способностью к самостоятельному распространению через компьютерные сети. — *Прим. пер.*

нации исторически была прерогативой властей. Однако сейчас правительство и представители индустрии сформировали союз, чтобы противостоять общей опасности. Пентагон передал компаниям информацию об IP-адресах компьютеров и серверов, на которых, предположительно, иностранные агенты хранили украденные данные, а также адреса электронной почты, с которых осуществлялась рассылка писем-ловушек, содержащих вирусы или шпионское программное обеспечение (ПО). Правительственные аналитики сообщали обо всех обнаруженных новейших средствах и методах, которыми пользовались иностранные хакеры для взлома своих целей. Кроме того, они предупреждали компании о тех видах вредоносного ПО, с помощью которого хакеры внедрялись в компьютеры и воровали файлы. Вооруженные этими основными данными — так называемыми идентификаторами угрозы, компании должны были усилить свои средства защиты, сконцентрировать свое внимание на противодействии взломщикам и не допустить, чтобы их компьютерные сети снова подверглись опасности. Идентификаторы угрозы определялись специалистами Агентства национальной безопасности (АНБ) — крупнейшей правительственной разведывательной службой. Ее глобальная сеть наблюдения собирает данные с десятков тысяч компьютеров, которые были взломаны и заражены шпионским ПО специалистами самой АНБ, почти так же, как китайскими шпионами были взломаны компьютеры оборонных компаний. Информация, собранная АНБ, самым полным образом раскрывает возможности, планы и намерения врагов Америки, а потому является сверхсекретной. И вот теперь правительство делится этой информацией с компаниями при условии соблюдения самых строгих правил секретности. Получатели этих сведений не должны были раскрывать, что им переданы идентификаторы угрозы, а кроме того, должны были сообщать Пентагону обо всех попытках проникновения в свои компьютерные сети.

Программу передачи разведданных оборонным предприятиям назвали «Инициативой оборонной промышленности»

(Defense Industrial Base Initiative), и сначала она охватывала всего 12 компаний, руководителей которых собрали на том брифинге в Пентагоне. Однако уже через год число участников увеличилось до 30. Сегодня их около 100. В планах Пентагона приглашать в этот секретный клуб, известный своим участникам как DIB, по 250 новых членов ежегодно.

При этом власти хотят защитить не только военных подрядчиков. Они рассматривают DIB как модель защиты всех отраслей промышленности, начиная с телекоммуникаций и энергетики и заканчивая здравоохранением и банковским сектором, — любого бизнеса, системы или функции, где используются компьютерные сети. В сегодняшних реалиях это практически все сферы деятельности. Инициатива DIB стала началом намного более широкого и все еще развивающегося союза между властью и индустрией.

Руководители разведслужб, высшие армейские чины, и сам президент говорят, что последствия еще одной серьезной террористической атаки на Америку могут померкнуть по сравнению с хаосом и паникой, которые возникнут в результате действий решительной и злонамеренной группы хакеров. Вместо того чтобы украсть информацию, они могут уничтожить сам компьютер, вывести из строя коммуникационные сети или отключить авиадиспетчерские системы, управляющие воздушным движением. Они могут взломать подключенные к Интернету устройства, которые регулируют потоки электроэнергии, и погрузить во тьму целые города. Или провести атаку на саму информацию, уничтожив или повредив данные о финансовых счетах и спровоцировав панику в масштабе страны.

В октябре 2012 г. министр обороны США Леон Панетта выступил с предупреждением, что Соединенным Штатам грозит «электронный Перл-Харбор — атака, которая приведет к физическим разрушениям и смертям, которая парализует и повергнет нацию в шок, создаст абсолютно новое сильное чувство

уязвимости и незащищенности». Пятью месяцами ранее президент Барак Обама в редакционной статье написал, что войны будущего будут вестись в режиме онлайн, когда «неприятель, неспособный совладать с нашей военной мощью на поле сражения, сможет воспользоваться уязвимостями наших компьютерных систем здесь, у нас дома». Обама нарисовал ужасающую и, возможно, гиперболизированную картину. Однако выбранный им риторический прием отражал те беспокойство и озабоченность, которые охватывают высших представителей власти и бизнеса и связаны с тем, что киберпространство, дающее безграничные надежды на улучшение жизни людей, становится еще и наиболее незащищенным местом, в котором присутствуют нечеткие и трудноопределимые угрозы. «Разрушение жизненно важной банковской системы может спровоцировать финансовый кризис, — писал Обама. — Проблемы с питьевой водой или с функционированием больниц могут создать критическую ситуацию в национальном здравоохранении. А, как мы видели во время прошлых аварийных отключений электростанций, перебои электроэнергии могут привести к полной остановке деловой активности в городах и целых регионах страны». Директор ФБР Джеймс Коми заявил, что опасность кибератак и рост киберпреступности, включая шпионаж и финансовые аферы, станут наиболее важными угрозами национальной безопасности в следующем десятилетии. За последние два года возможность разрушительных кибератак возглавила список «глобальных угроз», который составляется при участии всех 17 американских разведывательных служб для отчета перед конгрессом. Защита киберпространства стала главным приоритетом нацбезопасности для властей США, поскольку онлайн-атаки могут иметь разрушительный офлайн-эффект.

И это еще власти не раскрывают всей правды. Чиновники быстры в изображении граждан жертвами, страдающими от беспрерывных происков невидимого врага. Однако военные и разведывательные ведомства США, зачастую в сотрудниче-

стве с американскими корпорациями, сами выступают чуть ли не как самые агрессивные действующие лица в киберпространстве. Соединенные Штаты — одна из немногих стран, государственная политика которых рассматривает киберпространство как поле боя, а потому направлена на полный контроль этой сферы при наличии средств и возможностей на осуществление этого контроля. Более десяти лет кибершпионаж был единственным наиболее эффективным способом сбора информации о противниках страны как за рубежом, так и дома. Агрессивные действия Соединенных Штатов в киберпространстве коренным образом изменяют Интернет, и не всегда в лучшую сторону. В своем рвении защитить киберпространство правительство в сотрудничестве с корпорациями делает его только более уязвимым.

История о том, как Соединенные Штаты осознали важность вопроса безопасности киберпространства, начинается с попыток государства взять эту сферу под свой контроль, использовать ее одновременно и как оружие, и как средство шпионажа. Теперь военные называют киберпространство «пятым театром» боевых действий и считают достижение превосходства на этом театре необходимым для выполнения миссии, точно так же, как и на четырех других: суше, море, воздушном и космическом пространствах. Соединенные Штаты уже включили кибератаки в традиционное понятие военных действий и применяли их для вывода из строя инфраструктуры в других странах — те самые вредоносные действия, которых американские власти опасаются в собственной стране и для предотвращения которых должны приниматься самые экстраординарные меры. Во всем спектре военных действий в киберпространстве США выбрали агрессивную сторону.

Американские армия и разведслужбы выращивают новое поколение кибервоинов, обученных отслеживать компьютерные системы иностранных противников, взламывать их, а при необходимости отключать и выводить из строя. У поня-

тия «кибервойна», как и «киберпространство», нет точного определения. Однако его используют для описания целого ряда наступательных, атакующих действий. Как обычный шпионаж является неотделимой частью традиционной войны, так и кибершпионаж необходим как предварительное условие для атаки на компьютерную систему. В подтверждение этому можно сказать, что США потратили гораздо больше времени и денег на компьютерный шпионаж и похищение информации, чем на вывод из строя ключевых объектов инфраструктуры и уничтожение физического оборудования с помощью компьютерных сетей. Хотя и этим занимались тоже. И подобные атаки будут совершаться все чаще и станут все более эффективными. Действительно, кибервойна — сочетание шпионажа и нападения — стала средством достижения военной победы Америки в Ираке в 2007 г., средством, ни разу до конца не раскрытым и не получившим должной оценки. Военные при содействии американских разведслужб использовали наступательные киберметоды (другими словами, методы компьютерного взлома, хакинг), чтобы выслеживать людей в физическом, невиртуальном мире и затем брать их в плен или уничтожать.

Однако как защита киберпространства не является прерогативой властей, так и ведение войны в нем тоже становится делом частных компаний. Растущая индустрия торговли кибероружием и частные спецслужбы (служб безопасности) предлагают свои товары и услуги как правительственным организациям, так и корпорациям, которые не желают больше терпеть неослабевающий шпионаж и не хотят подвергать себя риску кибератак. Национальные армии неизбежно столкнуться друг с другом на кибернетическом поле боя. Но там же встретятся и корпоративные армии.

Власти действуют в киберпространстве не в одиночку. Защита компьютерных сетей, проведение кибератак в этих сетях требуют участия частного сектора, не всегда добровольного. Подавляющее большинство компьютерных сетей в Соединенных Штатах имеют частных владельцев. Власти

не имеют возможности защитить или наблюдать за всеми сетями. Однако большая часть мировых цифровых коммуникаций проходит через оборудование, расположенное в Соединенных Штатах. Власти обладают привилегированным положением при использовании этих сетей и потому крайне нуждаются в их защите. С этой целью и возник «военно-сетевой» комплекс.

Как и военно-промышленный комплекс ранее, это новое объединение включает производителей танков и самолетов, ракет и спутников. Но, кроме того, в него входят технологические гиганты, финансовые организации и телекоммуникационные компании. Власти Соединенных Штатов заручились поддержкой компаний, убедили их иногда лестью и обманом, а иногда и силой оказывать помощь в предотвращении попыток иностранных или местных недоброжелателей исследовать американские электросети и другие критические объекты инфраструктуры в поисках уязвимых мест. АНБ совместно с выдающимися технологическими компаниями, в том числе с Google, были разработаны секретные мероприятия по мониторингу частных сетей на предмет различных угроз. АНБ передавало секретную информацию ведущим банкам и финансовым организациям для того, чтобы избежать катастрофической кибератаки на Уолл-стрит.

Вместе с тем власти попытались заставить некоторые компании позволить АНБ разместить контрольное оборудование в своих сетях. Технологическим компаниям заплатили за то, чтобы они установили бэкдоры в свои продукты, с помощью которых власти могли бы следить за иностранными разведслужбами и контролировать действия их армий. Кроме того, эти секретные точки доступа позволяют военным проводить кибератаки в иностранных государствах. Без сотрудничества с компаниями Соединенные Штаты не смогли бы сражаться в кибервойнах. В этом смысле новый военно-сетевой комплекс играет ту же роль, которую раньше играл военно-промышленный. Правительства не сражаются в войнах

сами по себе. Они рассчитывают на компании, которые создают оружие, перевозят и кормят войска, строят и ремонтируют самолеты, корабли и спутники. Соединенные Штаты стали самой грозной военной державой в мировой истории благодаря взаимовыгодному сотрудничеству с корпорациями. И теперь власти были нацелены повторить успех в киберпространстве.

США быстро наращивают свои возможности для доминирования в киберпространстве. В 2014 г. правительство потратило более $13 млрд на программы кибербезопасности — в основном для защиты компьютеров и сетей в государственных учреждениях и для обмена с частными компаниями информацией об угрозах, полученной в результате разведывательных операций. Для сравнения стоит упомянуть, что расходы за тот же год на борьбу с изменением климата, которое, по словам президента Обамы, является «современной глобальной угрозой», составили $11,6 млрд. В течение следующих пяти лет одно только Министерство обороны запланировало потратить $26 млрд на технологии кибернетической защиты и нападения. Информация о том, какой именно объем средств Соединенные Штаты планируют потратить на наступательную компоненту, является засекреченной. Однако граница между обороной и нападением в киберпространстве крайне размыта и постоянно сдвигается. Та же инфраструктура, которая была создана для защиты сетей, может быть использована для проведения атак. Официальные лица предпочитают публично говорить об обороне, основываясь на стратегическом и циничном расчете: гораздо проще выбить фонды и политическую поддержку на отражение агрессии противника, чем на создание киберармии для проведения атак и осуществления шпионской деятельности в других странах. И тем не менее именно этим занимаются США, расходуя на свои наступательные операции часть тех миллиардов, которые формально были выделены на «оборону».

В бизнесе в сфере кибербезопасности произошел взрывной рост. Компании и частные лица по всему миру тратят около $67 млрд в год на защиту своих компьютеров и сетей. Многие эксперты, работающие в этой сфере, обучились своему ремеслу в военных или разведывательных организациях. Действительно, Пентагон стал учебной базой для частных киберстражей, которые могут легко удвоить или даже утроить свои доходы, перейдя на работу в частную компанию, работающую в сфере безопасности. Те же самые оборонные подрядчики, которые однажды стали целью для кибершпионов, теперь предоставляют экспертные услуги по защите сетей и ведению войны в них своим клиентам, в том числе энергетическим предприятиям и банкам — тем самым компаниям, защитой которых власти озаботились в первую очередь.

Борьба за контроль над киберпространством определяет американскую национальную безопасность в XXI в. Однако изменения ландшафта киберпространства, обусловленные ответной реакцией на появляющиеся угрозы, могут оказаться намного сильнее, чем изменения, вызванные самими этими угрозами. Решения, которые сегодня принимаются представителями власти и бизнеса, будут иметь серьезные последствия не только для американцев, но и для людей по всему миру, объединенных доверием к широкому, всеобъемлющему и зачастую трудно определимому пространству, не являющемуся ни полностью общедоступным, ни принадлежащим одной корпорации или правительству. Существование угроз в киберпространстве неоспоримо. Ответ на эти угрозы — запутанная и зачастую рискованная задача, и тем не менее все мы кровно заинтересованы в ее решении.

ЧАСТЬ I

1

ПЕРВАЯ КИБЕРНЕТИЧЕСКАЯ ВОЙНА

Боб Стасио не собирался идти в киберсолдаты. После окончания школы Стасио поступил в Буффаловский университет, где проходил обучение по программе службы подготовки офицеров резерва. Он специализировался в области математической физики, изучал головоломную теорию квантовой механики и дифференциальных уравнений в частных производных. Университет, заинтересованный в выпуске студентов, прекрасно разбирающихся в сложных науках, сделал исключение и не стал требовать строго выполнения всей учебной программы, в том числе по английскому языку. Стасио не написал ни одного сочинения за все время обучения в колледже.

В Форт-Льюис (штат Вашингтон) Боб Стасио прибыл в 2004 г., когда ему было 22 года. Штабной офицер разведки только мельком взглянул на резюме младшего лейтенанта, увидел, что он имеет серьезную подготовку по математике и физике, после чего сказал Стасио: «Отправишься в роту радиотехнической разведки (SIGINT)».

Радиотехническая разведка занимается перехватом и анализом сигналов электронных средств связи. Как и другие сферы разведки, эта область представляет собой сплав науки и искусства, но все-таки науки здесь больше. Штабной офицер разведки работал в АНБ и понял, что научная подготовка Стасио в области физики окажется весьма полезной, поскольку большая часть работы в радиотехнической разведке сопряжена с приемом радиосигналов, оптико-волоконной связью и интернет-пакетами.

Военная подготовка Стасио в колледже заключалась в умении использовать винтовку и руководить отрядом. При этом он потратил шесть месяцев на изучение основ сбора и анализа разведданных в школе армейской разведки в Форт-Хуачуке (штат Аризона). По прибытии в Форт-Льюис Стасио был направлен в отряд Stryker — механизированное соединение, легкое на подъем, созданное для быстрого, в течение нескольких дней, развертывания и вступления в бой. Задача Стасио заключалась в определении местоположения противника на поле боля с помощью слежения за его телекоммуникационными сигналами. Также предполагалось, что он будет предугадывать намерения врага путем перехвата приказов командования отрядам или прослушивания запросов командиров отрядов, находящихся в тылу, на выполнение авиаударов. Стасио должен был присоединиться к четвертой бригаде второй стрелковой дивизии под названием Raiders для отправки в Ирак и работать вместе с командой лингвистов, игравшей важную роль, поскольку Стасио не говорил по-арабски. Правда, когда дело дошло до встречи с этими лингвистами, Стасио был сильно расстроен: почти все они говорили только на английском и корейском языках.

Армейская радиотехническая разведка была создана для ведения холодной войны. Тысячи военных все еще продолжают службу на Корейском полуострове. Они по-прежнему проводят учения для ведения сухопутных боев с вооруженными силами Северной Кореи, во время которых радиоразведка —

определение местонахождения танков и подразделений противника — должна играть центральную роль в операции. Однако Raiders были непригодны для борьбы с компьютерными сетями иракских повстанцев, с добровольными джихадистами и террористами. Ведь эти парни не ездили на танках. У них не было единой организации, построенной по правилам военной иерархии. Ну и, конечно, они не говорили по-корейски.

Стасио решил, что его подготовка разведчика окажется практически бесполезной в Ираке, американская оккупация которого постепенно разваливалась. Армейские потери росли в результате подрывов на дорогах, успешно проводимых повстанцами. Солдаты, оставшиеся в живых после этих взрывов, возвращались домой, лишившись конечностей или получив серьезные черепно-мозговые травмы, которые будут мучить их физически и эмоционально до конца дней. Радиотехническая разведка не могла предотвратить эти атаки. На самом деле силы радиотехнической разведки практически не использовались. В октябре 2004 г. один из руководителей службы радиотехнической разведки привел оценки, по которым почти 90% всей информации в Ираке было получено благодаря шпионской сети, состоящей из разведчиков и информаторов, и эта информация не помогла американцам уменьшить интенсивность подрывов и нападений повстанцев.

Стасио читал все, что мог, о повстанческом движении, особенно отмечая способы самоорганизации на основе сетевой модели с многими независимыми группами людей, работающих в командах, автономно от централизованного управления. Эта схема организации была противоположна вертикально устроенной военной бюрократии, когда приказы спускаются сверху вниз через несколько уровней командиров. В принципе, методы разведки, которые Стасио изучал, должны были работать. Предполагалось, что он сможет определить местоположение врага с помощью анализа электронных сигналов и выяснить, каким будет следующий шаг. Однако средства, которые предоставляла армия для этих операций, плохо подходили

для ведения радиоразведки в сложных городских условиях. Raiders использовали систему перехвата сигналов, известную под названием Prophet, — массивный грузовик, снабженный длинной, устанавливаемой на крыше радиоантенной высотой примерно с уличный фонарь. Старшим офицерам бригады нравился Prophet, потому что он говорил им, где находились вражеские силы в пределах ближайшей зоны проведения операции. Это было тактическое устройство, и они направляли его туда, где им требовалось собрать разведданные.

Однако Prophet был создан для перехвата только радиоволн и только на открытой и относительно ровной местности, где велись боевые действия. Стасио знал, что вражеские боевики в Ираке общаются с помощью сотовых телефонов и электронной почты, а также, что они размещали видеозаписи в Интернете. Боевики перемещались небольшими группами в плотной бетонной застройке Багдада и других густонаселенных иракских городов. В таких условиях Prophet был не очень полезен. Действительно, когда Стасио наконец попал в Ирак, он увидел, что отряды армейской разведки, которые прибыли раньше него, использовали Prophet не для перехвата радиосигналов, а для перевозки еды и других припасов.

Была и еще одна причина, по которой ветераны любили Prophet, — он принадлежал им. Они могли направить его туда, куда захотят. Они имели контроль над сбором и анализом разведданных. Стасио подумал, что старшие офицеры обычно не доверяют умникам, прилетевшим из Штатов, чаще из Вашингтона, как не доверяют национальным разведслужбам, таким как ЦРУ и АНБ, которые отсюда, с поля боя, кажутся большими и неуклюжими бюрократическими конторами, битком набитыми программистами и компьютерными чудиками, слишком далекими от приземленных, полевых тактических нужд армии в Ираке.

Однако Стасио знал, что у национальных служб, а в особенности у АНБ, есть кое-что полезное — данные. А именно информация на серверах — результаты перехвата сигналов в электрон-