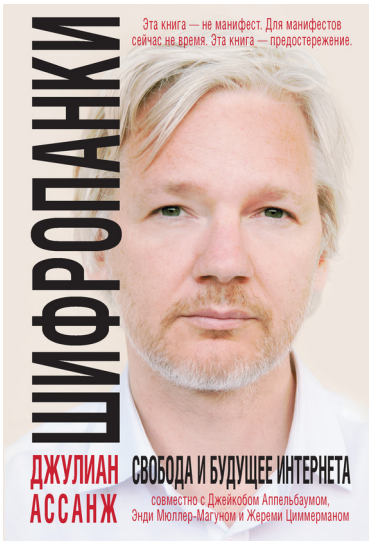
ШИФРОПАНКИ
Эта книга — не манифест. Для манифестов сейчас не время. Эта книга — предостережение.
ДЖУЛИАН АССАНЖ
СВОБОДА И БУДУЩЕЕ ИНТЕРНЕТА
совместно с Джейкобом Аппельбаумом, Энди Мюллер-Магуном и Жереми Циммерманом

Жереми Циммерман
Энди Мюллер-Магун
Джулиан Ассанж
Джейкоб Аппельбаум

Шифропанки: свобода и будущее Интернета

http://www.litres.ru/pages/biblio_book/?art=6700328
Джулиан Ассанж, Джейкоб Аппельбаум, Энди Мюллер-Магун, Жереми Циммерман. Шифропанки: свобода и будущее интернета: Азбука Бизнес, Азбука-Аттикус; Москва; 2014
ISBN 978-5-389-07975-5
Оригинал: JulianAssange, “CYPHERPUNKS FREEDOM AND THE FUTURE OF THE INTERNET”
Перевод:
Николай Караев

Аннотация

Весна интернета позади. Из объединяющего пространства, свободного от цензуры, Сеть превратилась в орудие глобального контроля. Государства все жестче отслеживают поступки своих граждан, подавляя любые нежелательные действия и не только их. Владеет Сетью тот, кто контролирует ее структуры – волоконно-оптические линии связи, спутники, серверы, разбросанные по городам мира. Тотальный характер мощнейшей машины контроля пока очевиден не всем пользователям интернета. Джулиан Ассанж и его соратники по движению шифопанков призывают к борьбе за свободу обмена информацией. Их оружие – криптография. Их знаменитый проект WikiLeaks вступил в конфликт почти со всеми влиятельными державами планеты.

Эта книга – предостережение. Объявлен общий сбор под знамена шифрования.

Содержание

Джулиан Ассанж совместно с Джейкобом Аппельбаумом, Энди Мюллер-Магуном, Жереми Циммерманом Шифропанки: свобода и будущее интернета

Интернет – это угроза всей человеческой цивилизации

Интернет – это угроза всей человеческой цивилизации.
Джулиан Ассанж

Интернет способствовал революциям по всему миру, однако в данный момент полным ходом идет подавление Сети. В эпоху, когда киберпространство осваивают целые сообщества, программы массовой слежки разворачиваются в масштабах планеты. Наша цивилизация стоит на развилке. Одна дорога ведет к будущему, в котором есть «приватность для слабых и прозрачность для сильных»; другая – к интернету, благодаря которому власть перейдет от народов к неподконтрольному никому комплексу спецслужб и их союзников – транснациональных корпораций.

Шифропанки – это активисты, пропагандирующие массовое использование сильной криптографии для защиты наших основных свобод от агрессоров. Джулиан Ассанж, главный редактор и вдохновитель проекта WikiLeaks, стал лидером шифропанковского движения в 1990-х. Сегодня Ассанж сводит вместе мятежных мыслителей и активистов с передового рубежа битвы за виртуальный мир, чтобы обсудить в своевременной и весьма важной новой книге, что именно сделает интернет со всеми нами: освободит или поработит.

Джулиан Ассанж – главный редактор проекта WikiLeaks, обладатель Новой премии СМИ организации «Международная амнистия» (2009), золотой медали Сиднейского фонда мира (2011), премии «Уокли» за журналистику (2011) и премии Марты Геллхорн (2011). Он был участником рассылки Cypherpunk и создал многочисленные программы, проникнутые философией шифропанка, включая криптографическую систему rubberhose и исходный код для WikiLeaks. Вместе со Сьюлетт Дрейфус он написал историю международного хакерского движения – книгу «Компьютерное подполье».

Что такое шифропанк?

Люди, называющие себя шифропанками, пропагандируют использование криптографии и других подобных методов, надеясь с их помощью добиться общественных и политических перемен[1]. Возникшее в начале 1990-х годов, это движение активнейшим образом участвовало в «криптовойнах» того времени и последовавшей «весне интернета» 2011 года.

Термин «шифропанк» (*англ.* cypherpunk) – от слов «(криптографический) шифр» и «панк» – был добавлен в Оксфордский словарь английского языка в 2006 году[2].

[1] Говоря по-простому, криптография (с *греч.* «тайное письмо») – это практика зашифрованной коммуникации.

[2] Oxford English Dictionary Updates Some Entries & Adds New Words; Bada-Bing, Cypherpunk, and Wi-Fi Now in the OED, ResourceShelf, 16 сентября 2006 года: http://web.resourceshelf.com/go/resourceblog/43743 (проверено 24 октября 2012 года).

Введение: призыв к криптографическому оружию

Эта книга – не манифест. Для манифестов сейчас не время. Эта книга – предостережение.

Наш мир не просто катится к транснациональной антиутопии – он мчится к ней на всех парах. Однако в полной мере данный факт осознают лишь круги, связанные с госбезопасностью. Обычные люди из-за секретности, сложности и масштаба идущих процессов этого не видят. Интернет – величайшее изобретение, которое могло даровать нам свободу, – ныне превращен в наиболее опасный проводник тоталитаризма в истории. Интернет – это угроза всей человеческой цивилизации.

Преобразование интернета случилось незаметно – люди, которые понимают, что именно происходит, сами трудятся над установлением глобального контроля и не заинтересованы в том, чтобы эта информация вышла наружу. Если траектория развития общества не изменится, наша цивилизация через два-три года превратится в постмодернистскую антиутопию, где слежка ведется за всеми и каждым в отдельности, и укрыться от нее не может никто, кроме наиболее опытных и информированных людей. Нельзя исключать, что эпоха глобального контроля уже настала.

О том, как интернет меняет нашу цивилизацию, писали многие мыслители, однако все они оказались неправы. Эти авторы ошиблись, потому что у них не было чувства перспективы – оно появляется только с накоплением непосредственного опыта. Они ошиблись, потому что никогда не сталкивались с врагом.

Всякое миропонимание гибнет при первом столкновении с врагом.

Мы увидели своих врагов.

За последние шесть лет проект WikiLeaks вступил в конфликт почти со всеми влиятельными державами планеты. Новая система слежки открылась нам изнутри – и мы сумели проникнуть в ее тайны. Она открылась нам с точки зрения участника сражения – мы должны были защищать своих людей, свои финансы, свои источники информации. Она открылась нам в глобальном разрезе – мы располагаем людьми, имуществом и информацией почти во всех странах. Она открылась нам во временно́м разрезе – мы боролись с данным феноменом много лет и видели, как контроль усиливается и распространяется, снова и снова. Это агрессивный паразит, который высасывает соки из общества, активно работающего с интернетом. Он захватывает всё новые территории, поражая любые страны, а прежде всего – людей.

Что нам нужно сделать?

Давным-давно в некоем месте, расположенном не здесь и не там, мы, создатели и граждане тогда еще молодого интернета, обсуждали будущее нашего нового мира.

Нам казалось, что он еще теснее свяжет человечество – и изменится сама природа государств, определяемых через способ обмена информацией, экономические ценности и военную мощь.

Нам казалось, что слияние существующих государственных структур и интернета создает предпосылки к изменению природы государства.

Для начала давайте вспомним, что государство – это система, через которую протекает принудительная сила: оно словно бы создает поле, размагничивающее источники свободы. Группировки внутри страны могут биться друг с другом за электорат, создавая видимость демократии, но фундамент любого государства – систематическое применение насилия (и противостояние ему). Землевладение, собственность, аренда, дивиденды, налогообложение, судебные штрафы, цензура, авторские права и торговые знаки – все это существует благодаря угрозе применения государственного насилия.

Бóльшую часть времени мы не можем даже вообразить, сколь тонка грань, отделяющая нас от него, – и все мы идем на уступки, чтобы его избежать. Уподобляясь матросам, вдыхающим свежий бриз, мы редко задумываемся о том, что под поверхностью нашего мира кроется тьма, без которой его не было бы.

Что может стать проводником принудительной силы в новом пространстве интернета?

Имеет ли вообще смысл такой вопрос? Как в этом потустороннем пространстве, в царстве вроде бы платоновских идей и информационных потоков может возникнуть само понятие принудительной силы? Силы, способной видоизменять исторические записи, прослушивать телефоны, разделять людей, разрушать сложные структуры и возводить стены – то есть действовать, как армия оккупантов?

Платоновская природа интернета, его идей и информационных потоков окажется иллюзорной, если вспомнить о физической основе всего этого. Фундамент Сети – волоконно-оптические линии связи, проложенные в толще океана, спутники, летающие над нашими головами, компьютерные серверы, размещенные в зданиях различных городов, от Нью-Йорка до Найроби. Как солдат смог зарубить Архимеда простым мечом, так и вооруженные силы способны захватить контроль над главным достижением западной цивилизации и завоевать наше платоновское царство.

Новый мир интернета, отделившийся от старого мира неодушевленных атомов, жаждал независимости. Однако государства и их друзья решили поместить его под колпак, заполучив власть над его физическими носителями. Государство, подобно армии, охраняющей нефтяную скважину, или таможеннику, вымогающему взятки на границе, быстро научилось использовать контроль над физическим пространством для обретения абсолютного контроля над нашим платоновским пространством. Однажды государство разобьет наши мечты о независимости, а затем, усевшись на оптоволоконные кабели и наземные станции систем спутниковой связи, начнет массовый перехват информационных потоков нашего нового мира – самой его сути, успевшей стать основой любых личных, экономических и политических взаимоотношений. Государство вопьется в вены и артерии наших новых сообществ, поглотит любое проявление связей в виде информации или общения, каждый доступный для чтения сайт, любое отправленное письмо, всякую мысль, забитую в Google, после чего сохранит данные – миллиарды перехватов в день, дающих невообразимую власть, – в обширных сверхсекретных информационных хранилищах. Навечно. Государство станет разрабатывать эти копи, эту производную коллективного человеческого разума, используя все более замысловатые алгоритмы поиска и распознавания образов, пополняя свой рудник и все более увеличивая разрыв в правах и возможностях между теми, кто перехватывает информацию, и обществом, которое ее производит. А потом государство воплотит все, чему научилось, в реальном мире: оно станет развязывать войны, нацеливать беспилотные боевые машины, манипулировать комитетами ООН и торговыми соглашениями, а также оказывать услуги обширной сети скованных одной цепью бизнесменов, инсайдеров и коррупционеров.

Но мы нашли средство против государства. Это наша единственная надежда на противодействие тотальной власти. Надежда на то, что храбрость, вдохновение и солидарность помогут нам оказать сопротивление. Мы обнаружили странное свойство физической вселенной, в которой живем.

Вселенная верит в шифрование.

Зашифровать информацию легче, чем расшифровать.

Мы поняли, что сможем использовать это свойство, чтобы создать законы нового мира. Чтобы отделить наше новое платоновское царство от его физических носителей в виде спутников, подводных кабелей – и тех, кому они принадлежат. Укрыть наше пространство за криптографической завесой. Создать новые земли, закрытые для тех, кто контролирует

физическую реальность, – ведь для того, чтобы следить за нами, им понадобятся бесконечные ресурсы.

Таким образом мы провозгласим независимость.

Ученые из Манхэттенского проекта поняли, что вселенная позволяет сконструировать атомную бомбу. Это умозаключение не было очевидным. Создание ядерного оружия вполне могло оказаться нереальным. Однако вселенная верит в атомные бомбы и ядерные реакторы. Она благословляет эти феномены так же, как соль, море или звезды.

А еще вселенная, наша физическая вселенная, обладает свойством, позволяющим индивиду или группе зашифровать информацию – надежно, автоматически, даже не сознавая того, – таким образом, что все ресурсы и вся политическая воля сильнейшей сверхдержавы на Земле не помогут ее расшифровать. Сеть соединяющих нас шифровальных каналов создаст области, свободные от принудительной силы внешнего государства. Свободные от массового перехвата. Свободные от контроля.

Так люди смогут противопоставить воле полностью мобилизованной сверхдержавы собственную волю – и победить. Шифрование – это воплощение физических законов, ему не страшны угрозы государств даже в условиях антиутопии с ее транснациональной слежкой за всеми и каждым.

Мир вовсе не обязан функционировать именно так. Однако по каким-то причинам вселенная благоволит шифрованию.

Криптография – это крайнее выражение ненасильственного прямого действия.

Государство, располагающее ядерным оружием, может подвергнуть неограниченному принуждению миллионы людей, однако даже в этом случае оно окажется не в состоянии сломить волю индивидов, желающих утаить от него свои секреты и использующих сильную криптографию.

Сильная криптография способна противостоять любому насилию. Нет такой формы принуждения, которая могла бы решить математическую задачу.

Но в силах ли мы превратить это странное свойство мира в краеугольный камень в фундаменте освобождения и независимости человечества в платоновском царстве интернета? И может ли случиться так, что по мере слияния социума и интернета эта свобода распространится и на физическую реальность, тем самым трансформировав само понятие государства?

Как мы понимаем, государства – это системы, которые решают, где и как последовательно применять принудительную силу.

На вопрос, может ли принудительная сила просочиться в интернет из физического мира, отвечают криптография и идеалы шифропанков.

По мере слияния государств с интернетом будущее нашей цивилизации становится будущим интернета, так что нам требуется пересмотреть соотношение сил.

Если мы этого не сделаем, глобальность интернета превратит само человечество в гигантскую сеть массовой слежки и контроля.

Мы должны дать сигнал тревоги. Эта книга – крик дозорного в ночи.

20 марта 2012 года, пребывая в Соединенном Королевстве под домашним арестом в ожидании экстрадиции, я встретился с тремя друзьями, такими же, как я, дозорными, в надежде на то, что, если мы заорем в один голос, наши крики пробудят город. Мы обязаны рассказать обо всем, что узнали, – пока у тебя, читатель, еще есть шанс разобраться в происходящем и сделать то, что ты должен сделать.

Пришло время взяться за оружие нашего нового мира, время сражаться за себя и за тех, кого мы любим.

Наша задача – укрепить свободу там, где мы можем это сделать, где не можем – замедлить наступление антиутопии и, наконец, ускорить ее саморазрушение, если нам не останется ничего другого.

Джулиан Ассанж,
Лондон, октябрь 2012 года

Участники обсуждения

ДЖУЛИАН АССАНЖ – главный редактор и вдохновитель WikiLeaks[3]. Джулиан с самого начала был участником рассылки Cypherpunk («Шифропанк») и остается одним из самых видных представителей философии этого движения в мире. Его работа с проектом WikiLeaks наполнила традиционный лозунг шифропанков «приватность для слабых, прозрачность для сильных» политическим содержанием. Хотя Джулиана больше знают как активного борца за свободное волеизъявление, требующего, чтобы власть и ее институты были прозрачны и подотчетны народу, он также остро критикует вторжение государства и корпораций в частную сферу индивидуума. Джулиан – автор многочисленных проектов программного обеспечения с шифропанковской философией, среди которых – первый сканер портов TCP/IP strobe.c, файловая система отрицаемого шифрования rubberhose и оригинальный код для проекта WikiLeaks[4]. В юности Джулиан изучал безопасность ранних компьютерных сетей – в те времена различные виды хакинга еще не были уголовно наказуемым преступлением. В 1990-е Джулиан стал в Австралии общественным активистом и организовал там компанию – провайдер интернета, а также написал в соавторстве со Сьюлетт Дрейфус книгу «Компьютерное подполье» – историю международного хакерского движения. По ее мотивам был снят фильм «Подполье: история Джулиана Ассанжа»[5].

ДЖЕЙКОБ АППЕЛЬБАУМ – основатель Noisebridge, хакспейса[6] в Сан-Франциско, член компьютерного клуба Berlin Chaos и разработчик программного обеспечения[7]. Джейкоб пропагандирует и развивает проект Tor, онлайновую анонимную систему, которая позволяет противостоять слежке и обходить сетевую цензуру[8]. Последние десять лет Джейкоб помогает активистам, защищающим права человека и окружающую среду. В частности, он опубликовал результаты передовых исследований, касающихся безопасности, приватности и анонимности во многих областях – от компьютерной криминалистики до медицинского применения марихуаны. Джейкоб верит в то, что у каждого есть право на чтение без ограничений и право на свободу высказываний без исключений. В 2010 году, когда Джулиан Ассанж не смог произнести речь в Нью-Йорке, Джейкоб сделал это за него. С тех пор он, его друзья и родственники подвергаются агрессии со стороны правительства Соединенных Штатов, в том числе допросам в аэропортах, агрессивным обыскам с угрозами и намеками на неизбежное изнасилование в тюрьме и конфискации оборудования; на слежение за онлайн-сервисами Джейкоба выдаются секретные ордера. Впрочем, он ничуть не запуган этими мерами, он продолжает добиваться победы юридическими способами и остается ярым сторонником свободного волеизъявления, а также видным защитником WikiLeaks.

---

[3] Проект WikiLeaks: http://wikileaks.org.

[4] Подробнее о rubberhose см. «The Idiot Savants' Guide to Rubberhose» Сьюлетт Дрейфус: http://marutukku.org/current/src/doc/maruguide/t1.html (проверено 14 октября 2012 года).

[5] Подробнее о книге «Компьютерное подполье» см.: http://www.underground-book.net.Подробнее о фильме «Подполье: история Джулиана Ассанжа» см. Internet Movie Database: http://www.imdb.com/title/tt2357453/ (проверено 21 октября 2012 года).

[6] Хакспейс, или хакерспейс, – место, где собираются люди с общими интересами к интернету и компьютерным технологиям. – *Прим. пер*.

[7] Noisebridge – хакспейс в Сан-Франциско, обеспечивающий инфраструктуру для техническо-творческих проектов и управляемый совместно всеми членами: https://www.noisebridge.net/wiki/Noisebridge. Компьютерный клуб Chaos Berlin – берлинский филиал компьютерного клуба Chaos (см. ниже): https://berlin.ccc.de/wiki/Chaos_Computer_Club_Berlin.

[8] Проект Tor: https://www.torproject.org.

ЭНДИ МЮЛЛЕР-МАГУН давно состоит в немецком компьютерном клубе Chaos, он бывший член совета директоров и пресс-секретарь клуба[9]. Он является одним из основателей EDRi (European Digital Rights, Европейского движения за цифровые права), общественной организации, отстаивающей права человека в цифровую эпоху[10]. В 2000 году интернет-пользователи ЕС избрали Энди европейским директором ICANN (Internet Corporation for Assigned Names and Numbers, Интернет-корпорация доменных имен и адресов), организации, которая несет ответственность за международную политику в сфере доменных имен и IP-адресов[11]. Как специалист в области инфотехнологической и прочей слежки, Энди проводит журналистские расследования на сайте buggedplanet.info в Project Wiki[12]. Работая с криптографическими технологиями, он вместе с коллегами создал компанию Cryptophone, которая предлагает корпоративным клиентам защищенные от прослушивания системы голосовой коммуникации и проводит стратегические консультации в контексте сетевой архитектуры[13].

ЖЕРЕМИ ЦИММЕРМАН – один из основателей и представитель гражданской правозащитной группы La Quadrature du Net («Квадратура Сети»), наиболее известной европейской организации, отстаивающей права на онлайновую анонимность и распространяющей информацию о попытках регулирования Сети и ущемлении сетевых свобод[14]. Жереми создает инструменты, которые позволяют всем желающим включиться в публичные обсуждения и попытаться изменить порядок вещей. В основном он участвует в войнах за копирайт, спорах по поводу сетевой нейтральности и других проблемах регуляции, от решения которых зависит будущее свободного интернета. Не так давно группа La Quadrature du Net добилась исторического успеха в европейской политике, проведя кампанию против Международного соглашения по борьбе с контрафактной продукцией (ACTA) в Европейском парламенте. Вскоре после участия в обсуждении, которое легло в основу данной книги, Жереми, уезжавший из США, был задержан двумя офицерами ФБР и допрошен на тему WikiLeaks.

[9] Компьютерный клуб Chaos – крупнейшая хакерская ассоциация Европы. Ее деятельность варьируется от технических исследований до кампаний, мероприятий, публикаций и политических консультаций. Сайт компьютерного клуба Chaos: http://www.ccc.de.

[10] EDRi: http://www.edri.org.

[11] ICANN: http://www.icann.org.

[12] buggedplanet: http://buggedplanet.info.

[13] Cryptophone: http://www.cryptophone.de.

[14] La Quadrature du Net: http://www.laquadrature.net.

Примечание редактора

Для того чтобы книга о шифропанках стала более понятной рядовому читателю, каждый участник дискуссии получил возможность существенно расширить и прояснить свои аргументы, а также снабдить их сносками. Отредактированная рукопись в целом отражает динамику изначального разговора.

О попытках преследования проекта WikiLeaks и связанных с ним людей

Участники последующего обсуждения неоднократно ссылаются на недавние события из истории проекта WikiLeaks и его попытки опубликовать те или иные документы. Поскольку эти отсылки могут быть непонятны читателям, не знакомым с историей WikiLeaks, краткая информация о нем приведена ниже.

Миссия проекта WikiLeaks – получать инсайдерскую информацию, размещать ее в открытом доступе и в дальнейшем защищать от неизбежных юридических и политических атак. Влиятельные государства и организации постоянно пытаются запретить деятельность WikiLeaks, однако проект, публикующий то, что никто больше публиковать не станет, изначально обладает защитой от подобных нападений.

В 2010 году WikiLeaks осуществил самую известную на сегодня акцию, разоблачив злоупотребления дипломатической секретностью в армии и правительстве США. Эти публикации известны под названиями «Сопутствующее убийство», «Логи войны» и «Кабельгейт»[15]. В ответ правительство США и его союзники предприняли слаженную и длящуюся по сей день атаку с целью уничтожения WikiLeaks.

[15] «Сопутствующее убийство»: http://www.collateralmurder.com. Логи войны в Ираке: http://wikileaks.org/irq. «Дневник войны в Афганистане»: http://wikileaks.org/afg. «Кабельгейт»: http://wikileaks.org/cablegate.html.

Большое жюри по WikiLeaks

Прямым следствием публикаций этого проекта стало инициированное властями США и начатое сразу несколькими учреждениями уголовное преследование Джулиана Ассанжа и работников WikiLeaks, а также его спонсоров и предполагаемых сообщников. Созванное в Александрии, штат Виргиния, Большое жюри должно было при поддержке ФБР и Министерства юстиции США решить, возможно ли выдвинуть против Джулиана Ассанжа и других ряд обвинений, в том числе и в сговоре согласно закону о шпионаже (Espionage Act) 1917 года. Американские чиновники заявили, что ситуация «не имеет прецедентов по масштабу и по сути». Большое жюри работает без судей и адвокатов. После того как расследование началось, члены Конгресса США предложили использовать закон о шпионаже в качестве средства для запугивания журналистов, «сознательно публикующих ставшую доступной вследствие утечки информацию», и сделать такой подход обычным для юридической системы США[16].

На момент выхода этой книги расследование деятельности WikiLeaks продолжается[17]. Некоторые люди были юридически принуждены к даче показаний. На судебных заседаниях по делу Брэдли Мэннинга, солдата, обвиненного в передаче информации WikiLeaks, выяснилось, что дело, в которое ФБР подшивает данные о расследовании WikiLeaks, насчитывает 42 100 страниц, из них около 8000 посвящены этому человеку. Брэдли Мэннинга держали в заключении без суда более 880 дней. Специальный докладчик ООН по пыткам Хуан Мендес официально заявил, что власти обращаются с Брэдли Мэннингом жестоко и бесчеловечно и подобное обращение может быть приравнено к пыткам[18].

[16] Congressional committee holds hearing on national security leak prevention and punishment, Reporters Committee for Freedom of the Press, 11 июля 2012 года: http://www.rcfp.org/browse-media-law-resources/news/congressional-committee-holds-hearing-national-security-leak-prevent (проверено 21 октября 2012 года).

[17] Подробнее о Большом жюри по WikiLeaks см. хронологию событий, описанную журналистом-фрилансером Алексой О'Брайен: http://www.alexaobrien.com/timeline_us_versus_manning_assange_wikileaks_2012.html (проверено 22 октября 2012 года).

[18] Bradley Manning's treatment was cruel and inhuman, UN torture chief rules, Guardian, 12 марта 2012 года: http://www.guardian.co.uk/world/2012/mar/12/bradley-manning-cruel-inhuman-treatment-un (проверено 24 октября 2012 года).

Призывы к расправе над Джулианом Ассанжем и объявление о создании оперативной группы по WikiLeaks

Расследование Большого жюри – не единственное направление атаки на проект WikiLeaks. В декабре 2010 года после «Кабельгейта» различные американские политики стали призывать к внесудебной расправе над Джулианом Ассанжем, в том числе с помощью удара беспилотного летательного аппарата (дрона). Сенаторы США клеймили WikiLeaks как «террористическую организацию» и называли Ассанжа «хай-тек-террористом» и «агентом противника», участвующим в «кибервойне»[19].

Накануне «Кабельгейта» и публикации материалов, связанных с войной в Ираке, в Пентагоне была создана оперативная группа по WikiLeaks (WikiLeaks Task Force, она же WTF) численностью в 120 человек. Целью ей поставили «проведение операций» против данного проекта. Было публично объявлено о создании в ФБР, ЦРУ и Госдепартаменте США аналогичных оперативных групп – все они работают до сих пор[20].

[19] WikiLeaks: guilty parties “should face death penalty”, Telegraph, 1 декабря 2010 года: http://www.telegraph.co.uk/news/worldnews/wikileaks/8172916/WikiLeaks-guilty-parties-should-face-death-penalty.html (проверено 22 октября 2012 года).

[20] CIA launches task force to assess impact of U.S. cables’ exposure by WikiLeaks, Washington Post, 22 декабря 2010 года: http://www.washingtonpost.com/wp-dyn/content/article/2010/12/21/AR2010122104599.html?hpid=topnews&sid=ST2010122105304 (проверено 22 октября 2012 года).

Прямая цензура

В беспрецедентной попытке подвергнуть СМИ цензуре власти США стали давить на провайдеров, требуя от них отказаться от предоставления услуг сайту WikiLeaks.org. 1 декабря 2010 года Amazon удалил WikiLeaks из своей системы хранения данных, а 2 декабря служба DNS объявила, что домен WikiLeaks.org уничтожен. Однако после этого WikiLeaks не исчез благодаря эффекту «массового зеркалирования»: тысячи сторонников проекта копировали сайт и выкладывали в интернет свои версии, распространяя IP-адреса через социальные сети[21].

Администрация Обамы объявила федеральным служащим, что выложенные в рамках проекта WikiLeaks материалы остаются секретными – даже несмотря на то, что их опубликовали ведущие СМИ планеты, включая газеты New York Times и Guardian. Федеральных служащих известили о том, что чтение этих материалов на WikiLeaks.org или в New York Times будет приравнено к нарушению режима секретности[22]. Правительственные учреждения, такие как Библиотека Конгресса, Министерство торговли и армия США, заблокировали доступ к материалам WikiLeaks в своих сетях. Блокировка распространялась не только на государственный сектор. Чиновники из правительства США известили высшие учебные заведения, что студентам, которые надеются поступить на госслужбу, стоит воздержаться от использования в своих работах опубликованных WikiLeaks материалов и не читать их в интернете.

[21] WikiLeaks fights to stay online after US company withdraws domain name, Guardian, 3 декабря 2012 года: http://www.guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns (проверено 23 октября 2012 года).

[22] Don’t Look, Don’t Read: Government Warns Its Workers Away From WikiLeaks Documents, New York Times, 4 декабря 2010 года: http://www.nytimes.com/2010/12/05/world/05restrict.html?hp&_r=2& (проверено 23 октября 2012 года).

Финансовая цензура: банковская блокада

WikiLeaks существует на пожертвования поддерживающих его людей. В декабре 2010 года ключевые банковские и финансовые учреждения, включая VISA, MasterCard, PayPal и Bank of America, поддались неофициальному давлению США и начали отказывать WikiLeaks в предоставлении финансовых услуг. Они блокировали денежные переводы и пожертвования, сделанные через основные кредитные карты. Все эти учреждения зарегистрированы в Америке, однако их доля на мировом финансовом рынке столь велика, что в возможности переслать деньги WikiLeaks и тем самым поддержать его публикации было отказано как гражданам США, так и людям по всему миру.

«Банковская блокада», как назвали ее СМИ, осуществляется без судебных или административных постановлений и на момент публикации данной книги не прекращена. WikiLeaks подал иски в суды различных стран с целью прорвать блокаду и одержал несколько предварительных побед; судебные процессы продолжаются до сих пор. Вследствие блокады WikiLeaks не получает дохода, между тем расходы проекта возросли, и почти два года он использует резервные фонды.

Происходящее демонстрирует, что у властей есть возможность контролировать финансовые операции третьих лиц. Это прямое покушение на экономическую свободу человека. Более того, блокада, угрожающая существованию проекта WikiLeaks, являет собой пример новой, весьма опасной формы глобальной экономической цензуры[23].

У ряда людей, предположительно связанных с проектом WikiLeaks, возникли загадочные проблемы с банками – от ошибок в реквизитах до полного закрытия счетов.

[23] Banking Blockade, WikiLeaks: http://www.wikileaks.org/Banking-Blockade.html (проверено 22 октября 2012 года).

Притеснение Джейкоба Аппельбаума и Жереми Циммермана

17 июля 2010 года Джулиан Ассанж должен был участвовать в конференции хакеров HOPE в Нью-Йорке. Он отменил выступление, и за него речь произнес Джейкоб Аппельбаум. После этого правоохранительные органы начали травлю Аппельбаума и его близких. Джейкоба часто задерживали, обыскивали, ему не давали связаться с адвокатом и допрашивали при пересечении границы всякий раз, когда он въезжал в Соединенные Штаты или выезжал из них. Его технику изымали, права нарушали, угрожая при этом еще бóльшими проблемами. Аппельбаума задерживали и преследовали больше десятка правоохранительных учреждений США – от иммиграционной и таможенной полиции, подчиняющейся Министерству национальной безопасности, до сухопутных войск. Во время задержаний на Аппельбаума оказывали давление – вплоть до того, что не разрешали пользоваться туалетом. При этом ему не предъявляли никаких обвинений, представители властей так ни разу и не объяснили, по какой причине Джейкоба Аппельбаума подвергают травле[24].

В середине июня 2011 года Жереми Циммерман, собирающийся подняться на борт самолета в вашингтонском аэропорту «Даллес», был задержан двумя людьми, представившимися агентами ФБР. Они начали задавать вопросы, касающиеся WikiLeaks, угрожая при этом арестом и тюремным заключением.

Аппельбаум и Циммерман – лишь двое из длинного списка друзей, помощников и предполагаемых соратников Джулиана Ассанжа, которых травили и за которыми следили американские власти. В этот список также входят и юристы, и выполнявшие свои профессиональные обязанности журналисты.

[24] Советуем прочесть описание самого Джейкоба: «Air Space – a trip through an airport detention center», boingboing, 31 октября 2011 года: http://boingboing.net/2011/10/31/air-space-a-tripthrough-an-ai.html. Рекомендуем также интервью с Джейкобом на сайте Democracy Now. National Security Agency Whistleblower William Binney on Growing State Surveillance, Democracy Now, 20 апреля 2012 года: http://www.democracynow.org/2012/4/20/exclusive_national_security_agency_whistleblower_william (обе ссылки проверены 23 октября 2012 года).

Изъятие электронных записей без ордера и «дело о судебном ордере Twitter»

14 декабря 2010 года компания Twitter получила «ордер административного суда». Министерство юстиции США требовало от компании поделиться сведениями, которые могли иметь отношение к расследованию деятельности WikiLeaks. Бумага из суда представляла собой «ордер 2703 (d)» с отсылкой к закону о сохраненной информации (Stored Communications Act). Согласно ему, правительство США имеет право добиваться раскрытия записей приватных электронных разговоров без выданного судьей ордера на обыск. По сути, американские власти обходят четвертую поправку к конституции, защищающую граждан от несанкционированных обысков и изъятий.

Судебный ордер требовал выдать названия учетных записей, логи сообщений, адреса, телефоны, реквизиты банковских счетов и номера кредитных карт людей, предположительно связанных с WikiLeaks, включая Джейкоба Аппельбаума, исландского парламентария Биргитту Йонсдоттир, голландского бизнесмена и пионера интернета Ропа Гонгрейпа, а также всю информацию по аккаунту собственно WikiLeaks. Ордер запрещал компании сообщать кому-либо о полученных требованиях. Однако Twitter смог успешно оспорить этот запрет в суде и отвоевал право информировать заинтересованных лиц о том, что власти требуют выдачи их данных.

26 января 2011 года, получив от компании Twitter известие о судебном ордере, Аппельбаум, Йонсдоттир и Гонгрейп, чьи интересы представляли адвокатское бюро Keker and Van Nest, Американский союз защиты гражданских свобод и Фонд электронных рубежей, подали через представителей ходатайство об отмене ордера. Дело получило огласку как «дело о судебном ордере Twitter»[25]. Адвокат Аппельбаума предъявил также ходатайство с требованием обнародовать остающиеся засекреченными протоколы судебных заседаний, на которых власти пытались получить конфиденциальные данные Аппельбаума от Twitter и других компаний. 11 марта 2011 года мировой судья отклонил оба ходатайства. Истцы обжаловали это решение.

9 октября 2011 года газета Wall Street Journal сообщила, что калифорнийский провайдер электронной почты Sonic.net также получил ордер с требованием выдать сведения о Джейкобе Аппельбауме. Компания оспорила ордер в суде и проиграла, однако получила разрешение предать огласке тот факт, что ее вынудили раскрыть информацию об Аппельбауме. По сведениям Wall Street Journal, аналогичный ордер получила и компания Google, однако был ли он оспорен в суде, газета не сообщила[26].

10 ноября 2011 года федеральный судья отклонил иски Аппельбаума, Йонсдоттир и Гонгрейпа и обязал Twitter предоставить Министерству юстиции затребованные им сведения[27]. 20 января 2012 года истцы обжаловали решение судьи, оспорив отказ раскрыть информацию об ордерах, которые получили другие компании[28]. На момент выхода этой книги дело еще не было завершено.

---

[25] Официальное название дела – In the Matter of the 2703 (d) Order Relating to Twitter Accounts: Wikileaks Rop_G IOERROR; and BirgittaJ.

[26] Secret orders target email, Wall Street Journal, 9 октября 2011 года: http://online.wsj.com/article/SB10001424052970203476804576613284007315072.html (проверено 22 октября 2012 года).

[27] Twitter Ordered to Yield Data in WikiLeaks Case, New York Times, 10 ноября 2011 года: https://www.nytimes.com/2011/11/11/technology/twitter-ordered-to-yield-data-in-wikileaks-case.html?_r=1 (проверено 22 октября 2012 года).

[28] ACLU & EFF to Appeal Secrecy Ruling in Twitter/WikiLeaks Case, пресс-релиз Фонда электронных рубежей, 20 января 2012 года: https://www.eff.org/press/releases/aclu-eff-appeal-secrecy-ruling-twitterwikileaks-case (проверено 22 октября 2012

года).

Усиление коммуникации против усиления слежки

ДЖУЛИАН: В начале 1990-х, когда запрет криптографии на государственном уровне породил движение шифропанков, многие верили в могущество интернета, который должен был гарантировать всем нам свободную и неподцензурную – по сравнению с обычными СМИ – коммуникацию. Однако шифропанки всегда понимали, что у свободы Сети есть обратная сторона: возможность следить за любым обменом информацией во всей полноте. Сегодня усиленной коммуникации противопоставлена усиленная слежка. Под «усиленной коммуникацией» подразумевается наличие у вас дополнительных степеней свободы по сравнению с теми, кто пытается контролировать чужие идеи; усиление слежки означат обратное.

Сегодня слежка куда более заметна, нежели в те времена, когда поток информации просматривали только американцы, британцы, русские и власти некоторых других стран вроде Швейцарии и Франции. Теперь за Сетью внимательно наблюдают все, практически каждое государство, слежка приобрела массовый характер, она коммерциализируется. Сегодня она становится тотальной: люди рассказывают в интернете обо всех своих политических пристрастиях, о семейных и дружеских связях. Таким образом, усилилась не только слежка за общением людей, существовавшая и ранее, – расширилась сама коммуникация. Причем увеличился как ее объем, так и число типов коммуникации. Новые типы, ранее бывшие приватными, ныне перехватываются в массовом порядке.

Идет битва между силой сведений, собранных информаторами и теневыми структурами, которые постепенно образуются, расширяют связи друг с другом и с частным сектором, и возросшей мощью обычных людей и интернета, ставшего для человечества привычным средством связи.

Я хотел бы поговорить о том, как нам следует рассказывать о наших идеях. Передо мной стоит большая проблема: как человек, не понаслышке знакомый с государственной слежкой и понимающий, как далеко транснациональная индустрия безопасности зашла за последние двадцать лет, я слишком хорошо обо всем этом осведомлен и потому не могу посмотреть на ситуацию глазами обывателя. Однако теперь мой мир – мир всех и каждого: все мы выложили в интернет суть нашей жизни. Мы обязаны как-то рассказывать о том, что нам известно, пока мы можем это делать.

ЭНДИ: Я предлагаю посмотреть на ситуацию не с точки зрения обычного гражданина, а с точки зрения человека, облеченного властью. Не так давно я побывал в Вашингтоне на одной странной конференции и увидел парней с беджами немецкого посольства. Я подошел к ним и сказал: «Ух ты, вы из посольства Германии», – а они сказали: «Ну, не совсем из посольства, мы на деле из-под Мюнхена». Выяснилось, что они представляют внешнюю разведку, и на вечернем фуршете я у них поинтересовался: «Так в чем же суть секретности?» Они ответили так: «Главное – замедлить процессы, чтобы лучше их контролировать». В этом и заключается их агентурная работа: они замедляют процесс, чтобы люди не поняли, что происходит. Объявить что-то секретным – значит ограничить круг тех, кто обладает знаниями и может на это воздействовать.

Если посмотреть на Глобальную сеть с точки зрения власть имущих, последние двадцать лет – страшные годы. Власти воспринимают интернет как болезнь, которая затрудняет их возможность влиять на происходящее и ограничивать знания людей и их способность воздействовать на реальные процессы. Взять хотя бы Саудовскую Аравию, где по какому-то историческому совпадению религиозные вожди и владельцы большей части страны – это одни и те же люди: их заинтересованность в переменах равна нулю. Где-то от нуля до минус пяти, может быть. Они воспринимают интернет как болезнь и спрашивают консультантов:

«Есть у вас лекарство от этой штуки? Если интернетная зараза появится в нашей стране, нам нужен иммунитет». Ответ – тотальная слежка. Консультанты говорят: «Нам нужен полный контроль над этой штукой, нам нужны фильтры, нам необходимо знать обо всем, что делается в Сети». Вот что происходило в последние двадцать лет. Власти вкладывались в слежку как могли – они страшились, что интернет станет им помехой.

ДЖУЛИАН: И все-таки вопреки тотальной слежке миллионы людей благодаря массовой коммуникации могут быстро прийти к согласию. Если у нас получится очень быстро перейти из обычного состояния в новое состояние согласия масс, государству, даже способному наблюдать за процессом, не хватит времени, чтобы дать эффективный ответ.

С другой стороны, вспомним о том, что в 2008 году в Каире прошла акция протеста, организованная через Facebook. Она застала правительство Мубарака врасплох, и в итоге протестующих выследили через тот же Facebook[29]. В 2011 году в «руководстве революционера», одном из важнейших документов тех египетских событий, самая первая страница призывала «не использовать Twitter или Facebook», чтобы распространять это руководство – и на последней странице стояло то же самое предостережение[30]. Тем не менее множество египтян использовали и Twitter, и Facebook. Эти люди выжили лишь потому, что революция получилась успешной. Если бы она провалилась, все они оказались бы в очень, очень тяжелом положении. Не стоит забывать и о том, что президент Мубарак уже на ранней стадии отрезал Египет от Сети. Помогло революции отключение интернета или навредило – это еще вопрос. Некоторые считают, что помогло – люди стали выходить на улицу, чтобы узнать новости, а когда ты на улице – ты на улице. Когда перестают работать мобильник и интернет, поневоле заволнуешься.

Революция должна быть успешной, ей нужна критическая масса участников, она должна случиться стремительно и победить – в противном случае инфраструктуру, позволившую людям быстро прийти к согласию, используют, чтобы выследить и изолировать тех, кто все это организовал.

Так обстояли дела в Египте, а Египет – да, союзник США, но не часть англоязычного разведывательного альянса, куда входят США, Великобритания, Австралия, Новая Зеландия и Канада. Давайте представим себе, что египетская революция начинается в Америке. Что произошло бы с сетями Facebook и Twitter? Государство взяло бы их под контроль. И если бы революция потерпела поражение, ЦРУ и ФБР стали бы извлекать из социальных сетей сведения о главных зачинщиках, как это происходит сейчас.

ЖЕРЕМИ: Слежку трудно отделить от контроля. Нам нужно говорить и про слежку, и про контроль. Это больше моя тема – контроль над интернетом со стороны правительств или корпораций.

---

[29] Речь идет об акции протеста в поддержку подавленной забастовки текстильных рабочих города Махалла-эль-Кубра. Незадолго до забастовки в Facebook сформировалась группа «Молодежное движение 6 апреля» с целью призвать египтян поддержать забастовку в Махалле акциями протеста в Каире и других городах. Группе не удалось добиться желаемого, ее члены, в том числе администраторы Эзраа Абдель Фатта Ахмед Рашид и Ахмед Махер, были арестованы. Махера пытали, требуя выдать пароль от страницы на Facebook. «Молодежное движение 6 апреля» сыграло свою роль в египетской революции 2011 года. См. «Cairo Activists Use Facebook to Rattle Regime», Wired, 20 октября 2008 года: http://www.wired.com/techbiz/startups/magazine/1611/ff_facebookegypt?current-Page=all (проверено 23 октября 2012 года).

[30] Брошюра «Как протестовать по-умному» анонимных авторов распространялась на начальном этапе 18-дневного восстания, которое свергло президента Мубарака. На арабском языке: http://www.itstime.it/Approfondimenti/EgyptianRevolutionManual.pdf. Отрывки переведены на английский и опубликованы, см. «Egyptian Activists' Action Plan: Translated», Atlantic, 27 января 2011 года: http://www.theatlantic.com/international/archive/2011/01/egyptianactivists-action-plan-translated/70388 (обе ссылки проверены 23 октября 2012 года).

ДЖЕЙКОБ: Думаю, не надо объяснять, что цензура – побочный продукт любой слежки вообще, будь то самоцензура или настоящая техническая цензура, и мне кажется, именно это важно донести до обычных людей, не углубляясь в технические дебри. Скажем, если б мы прокладывали дороги так, как строим интернет, на каждой стояли бы камеры слежения и микрофоны, доступ к которым имела бы только полиция – или люди, успешно притворяющиеся полицией.

ДЖУЛИАН: Джейк, в Великобритании дела так и обстоят.

ДЖЕЙКОБ: Когда компания строит дорогу, от нее не требуют оснастить каждый квадратный сантиметр высококлассными приборами слежения, передающими данные некоему тайному обществу. Если обычным людям объяснить, что именно так мы строим дороги в интернете и потом призываем ими пользоваться, люди поймут аналогию и осознают: контролировать дорогу не всегда будут те, кто ее создавал.

ЭНДИ: А кое-кто и дорог-то не строит. Он разбивает в интернете сад и предлагает всем раздеться. Да, я про Facebook! Бизнес, который приносит людям радость, раскрывая сведения о них всем подряд.

ДЖЕЙКОБ: Именно. В ГДР информаторов вознаграждали за то, что они работали на Штази – орган госбезопасности, – и точно так же их теперь вознаграждают за наличие аккаунта в Facebook. Только Facebook платит не деньгами, а социальным кредитом – соцсеть позволяет тебе переспать с соседом. Тут важно говорить именно о человеческом аспекте, потому что дело не в технике как таковой, а в контроле посредством слежки. Местами это совершеннейший паноптикон[31].

ДЖУЛИАН: Меня занимает философия технологии. Под технологией я понимаю не какой-то прибор, а, скажем, согласие большинства в правлении или структуру парламента – то есть системное взаимодействие. Например, я полагаю, что феодальные системы породила мельничная технология. Как только благодаря громадным инвестициям мельницы оказываются централизованы, их чисто физически становится легко контролировать – и естественным образом появляются феодальные отношения. В ходе истории мы, видимо, учились создавать все более сложные технологии. Некоторые из них совместимы с демократией, и доступ к ним может быть обеспечен всем и каждому. Но бóльшая часть технологий из-за своей сложности порождает в итоге весьма сплоченные организации вроде корпорации Intel. Не исключено, что любая технология по своей природе проходит через периоды открытия, централизации и демократизации, когда знание о ней передается следующему, более образованному поколению. Но мне сдается, что основное свойство технологии – это сосредоточение контроля над ней в руках тех, кому принадлежат необходимые данной технологии физические ресурсы.

Показательный пример тут – производство полупроводников. Для него нужен абсолютно чистый воздух, нужен завод, на котором тысячи работников обязаны носить специальные головные уборы, чтобы ни один кусочек кожи, ни один волосок не помешали многошаговому и чрезвычайно сложному процессу. Компания, создающая полупроводники, обладает миллионами часов научных наработок. Если это популярный продукт – а полупроводники

[31] Паноптикон – тюрьма, придуманная в 1878 году философом Иеремией Бентамом. В такой тюрьме один охранник может тайно следить за всеми заключенными сразу. См. Иеремия Бентам (под редакцией Миран Бозовиц) «The Panopticon Writings» (Verso, 1995), доступно в Сети: http://cartome.org/panopticon2.htm (проверено 22 октября 2012 года).

именно таковы, на них держится весь интернет, – значит, освобождение интернета завязано на производство полупроводников. Оно же, в свою очередь, зависит от способности тех, кто физически контролирует завод, находить дешевое сырье.

Следовательно, основа революции высокотехнологичных коммуникаций – и основа свободы, которой мы благодаря этим коммуникациям способны обладать, – неолиберальная, транснациональная, глобализированная рыночная экономика современности. На деле интернет – верхушка айсберга. Высота, которую, если мы говорим о достижениях технологии, современная экономика может взять. Интернет зиждется на очень сложных торговых связях между производителями оптоволоконного кабеля, производителями полупроводников, горнодобывающими компаниями, которые извлекают из-под земли сырье, а также здесь не обойтись без финансовой смазки, которая делает возможной торговлю, без судов, стоящих на страже законов о частной собственности, и т. д. В реальности интернет – это вершина пирамиды всей неолиберальной системы.

ЭНДИ: Что касается технологии, после того как Иоганн Гутенберг изобрел печатный станок, его время от времени запрещали в разных частях Германии, именно потому книгопечатание и распространялось: его запрещали в одной местности, оно перемещалось в другую юрисдикцию[32]. Я не изучал эту историю в деталях, но знаю, что печатников преследовала католическая церковь, поскольку те нарушали ее монополию на изготовление книг, и когда у них появлялись проблемы с законом, они переезжали туда, где книгопечатание было разрешено. Запрет по-своему помогал распространять печатные станки.

С Сетью, думаю, все происходило чуть по-другому. У нас появились машины, которые можно было применять как средство производства, – даже Commodore 64, хотя большинство использовало его для других целей.

ДЖУЛИАН: На каждом маленьком компьютере можно запускать собственное программное обеспечение.

ЭНДИ: Именно. А еще при помощи компьютера можно распространять идеи. Но, с другой стороны – и это философский аргумент, – в начале 1990-х, когда интернет вышел на глобальный уровень, один из основателей базирующегося в США Фонда электронных рубежей Джон Гилмор заметил: «Сеть интерпретирует цензуру как нечто вредное и обходит ее стороной»[33]. Как мы знаем сегодня, это была техническая трактовка пополам с оптимистическим взглядом на перспективы интернета, своего рода попытка принять желаемое за действительное – и одновременно самоисполняющееся пророчество.

ДЖУЛИАН: Но это было верно для Юзнета, который появился около тридцати лет назад и представляет собой, если угодно, множество связанных друг с другом электронных почтовых ящиков. Чтобы понять, что такое Юзнет, вообразите, что нет разницы между людьми и серверами и у каждого есть свой юзнетовский сервер. Вы пишете что-то и передаете файл одному или двум людям. Те (автоматически) проверяют, не получали ли они ваше послание раньше. Если нет, они принимают его и рассылают всем, с кем у них есть связь, и т. д. В результате послание дойдет до каждого, и у всех будет по копии. Если некто начнет

---

[32] Иоганн Гутенберг (1398–1468) – немецкий кузнец, изобретатель механического передвижного печатного станка, положившего начало одному из самых значительных социальных потрясений в истории. Изобретение печатного станка – ближайшая историческая аналогия созданию интернета.

[33] Джон Гилмор – один из первых шифропанков, основатель Фонда электронных рубежей и гражданский активист. Фраза, которую цитирует Энди, впервые появилась в статье «First Nation in Cyberspace», Time Magazine, 6 декабря 1993 года. См. сайт Джона Гилмора: http://www.toad.com/gnu (проверено 22 октября 2012 года).

подвергать файлы цензуре, его попросту проигнорируют, на Юзнет это не повлияет. Послание дойдет до всех, кто не является цензором. Гилмор говорил о Юзнете, а не об интернете. И он не имел в виду сайты.

ЭНДИ: Это технически верное замечание, но интерпретация слов Гилмора и их долгосрочное воздействие породили людей, которые осознавали себя как интернет. Они говорили: «Ладно, цензура есть, но мы ее обойдем», – а политик, не разбиравшийся в технологии, думал: «Черт, эта новая штука ограничивает наш контроль над информационной сферой». Я думаю, Гилмор, один из провидцев шифропанка, сделал великое дело: он вдохновил криптоанархистский взгляд на мир, когда у тебя есть своя версия анонимной коммуникации и ты не боишься, что за тобой будут следить.

ЖЕРЕМИ: По-моему, различные технологии распространяются по-разному – чтобы понять, как работает мельница или печатный станок, надо их увидеть, а сейчас мы все чаще встраиваем систему контроля в саму технологию. Контроль – это часть технологии. В большинстве случаев мы не можем даже открыть современный компьютер, чтобы узнать, из каких компонентов он состоит. И все компоненты спрятаны в маленькие футляры, так что мы не в состоянии понять, что именно они делают.

ЭНДИ: Из-за их сложности?

ЖЕРЕМИ: Из-за сложности и еще потому, что создатели технологии не хотят, чтобы кто-то разобрался в том, как она работает. Ведь речь идет об оригинальной технологии[34]. Кори Доктороу описал это в статье «Будущая гражданская война за компьютеры общего назначения»[35]. Если компьютер универсален, вы можете делать с ним что захотите. Обрабатывать любую информацию на входе, превращать ее во что угодно на выходе. И мы создаем все больше и больше устройств, являющихся компьютерами общего назначения, но работают они только как GPS-навигаторы, или как телефоны, или как MP3-плееры. Мы создаем все больше устройств со встроенной системой контроля, которая запрещает пользователю делать какие-то вещи.

ДЖУЛИАН: Встроенный контроль не позволяет понять, как работает устройство, и переделать его, чтобы оно работало не так, как задумано производителем, а когда устройство подключено к Сети, все становится еще хуже.

ЖЕРЕМИ: Именно, потому что одной из его функций может быть слежка за пользователем и его данными. Вот почему в свободном обществе такое значение имеет свободное ПО.

ЭНДИ: Я абсолютно согласен с тем, что нам нужны машины общего назначения. Но сегодня утром, когда я пытался вылететь сюда из Берлина, лайнер не смог подняться – я столкнулся с таким впервые. Самолет отъехал в сторону, и командир экипажа сказал: «Дамы

---

[34] «Оригинальные технологии – это любые типы систем, инструментов или технических процессов, которые разработаны данной компанией для себя самой… Идеи, которые развили или подали работники компании, обычно считаются интеллектуальной собственностью работодателя, позволяя тому называть технологию оригинальной». Определение взято с сайта wiseGEEK: http://www.wisegeek.com/what-is-proprietary-technology.htm (проверено 22 октября 2012 года).

[35] Кори Доктороу «The coming war on general-purpose computing», boingboing, 10 января 2012 года (на основе доклада, сделанного на компьютерном конгрессе Chaos в декабре 2011 года): http://boingboing.net/2012/01/10/lockdown.html (проверено 15 октября 2012 года).

и господа, наши электрические системы отказали, так что мы решили остановить самолет и перезапустить системы». Я сидел и думал: «Черт, звучит как перезагрузка Windows: клавиши Control + Alt + Delete – вдруг заработает!» И я не слишком огорчился бы, если бы на самолете установили узкоспециальное устройство, которое управляет только самолетом – и делает это очень хорошо. Когда я лечу в самолете, я не хочу, чтобы пилотов отвлек «Тетрис», или вирус Stuxnet, или что-то еще[36].

ЖЕРЕМИ: Самолет сам по себе не обрабатывает твои личные данные, он не контролирует твою жизнь.

ЭНДИ: Ну, когда самолет летит, он очень даже контролирует мою жизнь.

ДЖЕЙКОБ: Довод Кори, я думаю, можно обобщить так: у нас больше нет машин, самолетов, слуховых аппаратов – у нас есть компьютеры на четырех колесах, компьютеры с крыльями и компьютеры, которые усиливают слух. И вопрос не в том, узкоспециальные они или нет, вопрос звучит по-другому: можем ли мы проверить, делают они именно то, что, как утверждается, они должны делать, или нет, и можем ли мы понять, насколько хорошо они функционируют? Люди сплошь и рядом пытаются доказать, что у них есть право упрятать информацию под замок и держать ее в секрете, поэтому они либо усложняют компьютеры, либо ставят юридические препоны, не позволяющие понять, как машины устроены. Тут есть опасность для общества, потому что, как нам известно, люди не всегда действуют в интересах общества, и мы также знаем, что люди ошибаются – не злонамеренно, – так что убирать информацию под замок очень опасно по ряду причин, в том числе и потому, что никто из нас не идеален. Это факт. Возможность получить доступ к чертежам системы, от которой зависит наша жизнь, – одна из причин, из-за чего такое значение имеет свободное ПО, но потому же нас должно волновать и аппаратное обеспечение, «железо». Оно позволяет делать надежные инвестиции, улучшать используемые системы и проверять, работают ли эти системы так, как должны.

Безотносительно свободы: устройство этих систем важно знать еще и потому, что если оно нам не известно, то мы склонны полагаться на власть – на тех, кто либо понимает, как системы работают, либо может их контролировать, даже если незнаком с принципами их функционирования. Вот почему сейчас столько говорят про кибервойну: люди, которые вроде как отвечают за войны, заговорили о технологии так, будто понимают, как она работает. Они часто рассуждают о кибернетической войне, и никто из них – вообще никто – не рассуждает о кибернетическом укреплении мира или о миротворчестве. Они вечно говорят о войне – это их бизнес, и они пытаются взять под контроль технологию и законодательство, чтобы добиться своих целей. Если мы не будем контролировать нашу технологию, эти люди захотят использовать ее в собственных интересах, в частности для ведения войн. Так могут появиться на свет всякие страшные штуки – думаю, именно так был создан червь Stuxnet.

---

[36] Stuxnet – чрезвычайно хитроумный компьютерный червь, разработанный, согласно популярной версии, США и Израилем для нападения на компьютеры Siemens, предположительно использовавшиеся Ираном для обогащения урана. Общую информацию см. в Wikipedia: http://en.wikipedia.org/wiki/Stuxnet. См. также «WikiLeaks: US advised to sabotage Iran nuclear sites by German thinktank», Guardian, 18 января 2011 года: http://www.guardian.co.uk/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear. Проект WikiLeaks обнародовал один из первых отчетов о последствиях аварии на заводе по обогащению урана в Нетензе в результате, как считается сегодня, запуска в систему вируса Stuxnet. См. «Serious nuclear accident may lay behind Iranian nuke chief's mystery resignation», WikiLeaks, 17 июля 2009 года: http://wikileaks.org/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief%27s_mystery_resignation. Данные специализирующейся на международной разведке компании Stratfor, обнародованные WikiLeaks, заставляют предположить участие Израиля. См. Email ID 185945, The Global Intelligence Files: http://wikileaks.org/gifiles/docs/185945_re-alpha-s3-g3-israel-iran-barak-hails-munitions-blast-in.html (все ссылки проверены 16 октября 2012 года).

С другой стороны, пока Америка воюет, разумные люди говорят, что контроль над технологией способен предотвратить войну. Может, это и хороший довод для государства, которое не атакует постоянно другие страны, но вряд ли он применим к стране, вовлеченной одновременно в несколько военных операций.

Милитаризация киберпространства

ДЖУЛИАН: Я наблюдаю сейчас за милитаризацией киберпространства – точнее, за его оккупацией. Когда вы общаетесь с кем-то через интернет или по сотовой связи, которая сегодня срослась с интернетом, вашу коммуникацию перехватывает военная разведка. Это все равно что жить с танком в спальне. Когда вы шлете SMS жене, между вами стоит солдат. Если говорить о коммуникации, мы все живем по законам военного времени, просто танков не видим – но они есть. До такой степени Сеть, которая должна была стать гражданским пространством, превратилась в пространство милитаризованное. Но интернет – это наш космос, все мы используем его для общения друг с другом и с членами наших семей. Коммуникация, составляющая ядро частной жизни, перешла в интернет. Так что на деле наша частная жизнь попала в военную зону. Как если бы солдат притаился под нашей кроватью. Милитаризуется уже сама гражданская жизнь.

ДЖЕЙКОБ: Не так давно мне пришло приглашение из исследовательской лаборатории безопасности и секретности Вашингтонского университета с просьбой потренировать команды этой лаборатории – она хотела принять участие в соревнованиях по киберзащите студентов Тихоокеанского региона. В последний момент меня попросили их консультировать. Мы много тренировались, чтобы поучаствовать в кибервойне, в которой SPAWAR, гражданская организация в составе ВМС США – она проводит пентесты, занимается агрессивным и оборонительным хакингом, – играла роль «красной команды»[37]. Она атакует всех прочих игроков, и задача твоей команды – защитить компьютерную систему, которую тебе дают в начале игры, причем ты заранее ничего об этой системе не знаешь. Ты понятия не имеешь, какую систему тебе придется защищать, вначале не ясно даже, как начисляются очки, и тебе остается только лезть вон из кожи и надеяться на победу.

ДЖУЛИАН: Ты уверен, что вы действительно играли? Может, это была совсем не игра!

ДЖЕЙКОБ: Нет, тебе дают несколько компьютеров – и ты должен их защищать, а «красная команда» ломает твою защиту и перехватывает контроль над системой. Что-то вроде детской версии «Захвата флага» на настоящей хакерской конференции. Очень любопытное соревнование – у этих парней полно «отмычек», и они сами пишут свои программы[38].

ДЖУЛИАН: И какой в этом смысл – с точки зрения ВМС США?

ДЖЕЙКОБ: В данном случае они спонсируют игру, потому что хотят найти потенциальных киберсолдат. Я принес тебе блокнот с логотипом ЦРУ – эта организация занималась на игре вербовкой. Там присутствовал парень по имени Чарли – Чарли из ЦРУ, – он объяснял, что, если ты хочешь устроиться в ЦРУ, это отличная возможность найти работу в реальном мире. Там были представители SPAWAR и Microsoft, они тоже вербовали людей. Идея в том, чтобы натаскать всех игроков, все команды, лучшие из них сразятся на чемпионате страны и «защитят государство» – и в качестве киберсолдат смогут потом иметь дело не только с

[37] Пентест (от *англ.* penetration testing, «тестирование на проникновение») – термин из техники обеспечения безопасности. В ходе теста производится санкционированная атака на компьютерную систему или сеть, позволяющая оценить, насколько последние безопасны. Специалистов, которые проводят пентесты, часто набирают из хакерского сообщества.

[38] «Захват флага» – изначально уличная игра, в которой обычно участвуют две команды: каждая занимает некую территорию и охраняет свой флаг. Цель – заполучить флаг противника и вернуться на свою территорию. На хакерских конференциях принято играть в компьютерную версию этой игры: команды атакуют и защищают компьютеры и сети.

кибероборо́ной, но и с кибератаками. Мы набрали на игре что-то около 4000 баллов, в сумме столько же, сколько второе, третье и четвертое места. На деле мы сыграли лучше их всех, вместе взятых.

ДЖУЛИАН: Ну да, ну да…

ДЖЕЙКОБ: Я тут ни при чем – не думаю, что я такой уж хороший тренер, мой лозунг звучал: «Темнее всего перед тем, как приходит полная тьма», – просто ребята были настоящие гении. Игра получилась любопытная, насквозь военная. Допустим, тебе говорят: «Эй, мы хотим услышать ваш боевой клич!» А ты такой: «Простите, что?..» Нас об этом спросили на обеде, в перерыве между сражениями. На игре только и говорили, что об атакующих системах, о войне, кибервойне, величии военного образа мысли. И вот что интересно: если не считать команду, с которой я работал, в игре участвовало множество людей, что сражались, но не по «Искусству войны», а скорее как на турнире «Кубок сисадмина», обороняя свои системы любыми средствами, и это было омерзительно[39]. Я с ужасом смотрел на людей с военным опытом, которые думали по-военному, но не обучали свои команды стратегии, а громогласно призывали их защищать системы – или же атаковать системы, – и для них это было самое настоящее поле боя, они сочились патриотическим пафосом. Они не пытались развивать творческий подход или поощрить независимый анализ – нет, они требовали от других работать, подобно винтикам, и исполнять приказы во имя народного блага. Я такого никогда раньше не видел. Меня от них тошнило, и почти все мои ребята с трудом переваривали таких людей, они не могли воспринимать их всерьез.

ДЖУЛИАН: Как ты думаешь, может быть, это стандарт для учений ВМС США, который теперь пытаются применить в других областях? Стандарт, установленный решением – международным стратегическим решением – киберкомандования Соединенных Штатов?

ЭНДИ: Похоже на детские тренировочные лагеря нацистов.

ДЖЕЙКОБ: Sie können das sagen weil du bist Deutsche[40]. Нет, не похоже. ВМС участвует в этой игре постольку, поскольку ее финансирует правительство США. Им нужен был тренер, они нашли меня, и я согласился – мне понравилась моя команда, студенты последнего курса. На деле происходит вот что: власти США убеждают людей биться за родину – и пытаются внушить им патриотические чувства. Это была чрезвычайно странная игра: с одной стороны, неплохо знать, как обезопасить систему, и понимать, как работает инфраструктура, от которой зависят наши жизни; с другой – власти не пытались убедить участников во всем этом разобраться, они хотели пробудить в них патриотический пыл, чтобы люди, выполняя подобную работу, были счастливы.

ЭНДИ: Как ни жаль, заинтересованность Соединенных Штатов в безопасности систем очень ограниченна – им нужны уязвимые системы, чтобы можно было захватить над ними контроль. Сегодня криптозащита контролируется не так жестко, как предлагали США около 1998 года, когда отвечавший за международную коммерцию замминистра торговли Дэвид Аарон ездил по миру и ратовал за то, чтобы дать правительству доступ к зашифрованным

[39] Кубок сисадмина (сисадмин, системный администратор – это IT-специалист, поддерживающий работу компьютерной системы или сети) – Джейкоб имеет в виду, что задача наводила его на мысль о турнире системных администраторов.

[40] Ты можешь так говорить, потому что ты немец (*нем.*).

паролям любого пользователя[41]. Однако криптография все равно считается так называемой технологией двойного применения, и во многих странах ее экспорт в качестве продукта для конечного потребителя ограничен законом, а на мировом уровне данный вопрос регулируют Вассенарские соглашения[42]. В контексте объявления каких-то стран и их действий «злом» это, может, и верное решение, но налицо двойные стандарты – скажем, экспорт технологии телекоммуникационной слежки ограничен в куда меньшей степени[43].

ДЖУЛИАН: Энди, ты много лет работал над созданием криптографических телефонов. О каких видах массовой слежки можно говорить применительно к средствам связи? Каков последний технологический тренд в области «оптовой» слежки и правительственной разведывательной индустрии?

ЭНДИ: Массовое накопление информации. Иначе говоря, власти сохраняют всю телекоммуникацию, все голосовые звонки, весь инфопоток сообщений, любые групповые рассылки SMS, а также данные по интернет-соединениям, в ряде ситуаций ограниченные по крайней мере электронными письмами. Если сравнить военный бюджет с расходами на кибервойну, окажется, что обычное вооружение стоит кучу денег, так что киберсолдаты или массовая слежка чрезвычайно дешевы по сравнению, скажем, с одним самолетом. Один-единственный истребитель стоит…

ДЖУЛИАН: Около ста миллионов.

ЭНДИ: А хранение информации дешевеет с каждым днем. Компьютерный клуб Chaos подсчитал, что хранение с приличным качеством звука всех телефонных разговоров по Германии за год обойдется примерно в 30 миллионов евро, включая административные расходы, а само по себе хранение стоит около 8 миллионов[44].

ДЖУЛИАН: Есть еще компании вроде южноафриканской VASTech, продающие подобные услуги за 10 миллионов в год[45]. «Мы перехватим все ваши звонки и сохраним их для вас». За последние два года подход изменился: раньше перехватывался весь инфопоток из одной страны в другую, потом власть выбирала конкретных индивидов, за которыми хотела

---

[41] Aaron says encryption protects privacy, commerce, USIS Washington File, 13 октября 1998 года: http://www.fas.org/irp/news/1998/10/98101306_clt.html (проверено 21 октября 2012 года).

[42] Сайт Вассенарских соглашений: http://www.wassenaar.org (проверено 21 октября 2012 года).

[43] Энди говорит о различных событиях «первых криптовойн» 1990-х годов. Когда активисты шифропанка стали распространять сервисы с сильной криптографией в качестве бесплатного программного обеспечения, правительство США начало препятствовать эффективному использованию последних. Оно приравняло криптографию к вооружениям и запретило ее экспорт; оно попыталось вывести на рынок конкурирующие, заведомо дефектные технологии, позволявшие правоохранительным органам дешифровать любую информацию; оно также попыталось реализовать весьма спорную схему «депонирования ключей». В начале 2000-х годов на протяжении недолгого времени считалось, что попытка бороться с криптографией потерпела фиаско. Однако сейчас разворачивается «вторая криптовойна» – используя и законы, и технологии, власти пытаются обойти или маргинализовать использование криптографии.

[44] Такие же расчеты были проделаны для обнародованных 196,4 миллиарда минут звонков по наземной сети Германии за 2010 год, оцифрованных голосовым кодеком с качеством 8 Кбит/с, в сумме – 11 784 петабайт, округленно с запасом – 15 петабайт. Учитывая, что стоимость хранения одного петабайта составляет около 500 тысяч долларов США, мы получим 7,5 миллиона долларов, или 6 миллионов евро. Добавим расходы на приличное оборудование дата-центра, вычислительные мощности, соединения и фонд заработной платы. Даже если включить в расчет еще 101 миллиард минут звонков по мобильной сети Германии за 2010 год, что составляет еще 50 петабайт и 18,3 миллиона евро, хранение этих данных будет стоить меньше, чем один военный самолет вроде Eurofighter (90 миллионов евро) или F22 (150 миллионов долларов).

[45] Подробнее о VASTech см. на сайте buggedplanet: http://buggedplanet.info/index.php?title=VASTECH (проверено 21 октября 2012 года).

следить, и прослушивала их коммуникацию, а теперь перехватывается и сохраняется вообще все – и навечно.

ЭНДИ: Если говорить в общих чертах, ситуация развивалась следующим образом. Раньше гражданина прослушивали, если он занимал дипломатический пост, работал в какой-то компании, подозревался в чем-то или контактировал с людьми, которые делали что-то не то, – и тогда за человеком начинали следить. Сегодня считается, что эффективнее поступать так: «Мы сначала сохраним всю информацию, а потом ее рассортируем». Власти сохраняют инфопоток на долгосрочную перспективу, и деятельность всей индустрии можно разделить на «тактический» и «стратегический» подходы. Тактический сводится вот к чему: «Прямо сейчас, во время собрания, нужно нашпиговать помещение "жучками", заслать внутрь агента с микрофоном, в начиненной электроникой одежде, развернуть из автомобиля системы слежения GSM (Global System for Mobile communications, Глобальная система мобильной коммуникации), чтобы перехватывать разговоры сразу, не обращаясь к оператору сотовой связи, не получая полицейский ордер на обыск или другие бумажки, без каких-либо юридических процедур». Стратегический подход подразумевает, что мы делаем все то же самое по умолчанию, записываем все подряд и позднее сортируем материалы при помощи аналитических систем.

ДЖУЛИАН: То есть стратегический перехват – это сохранение всего того, что передает спутник связи, и того, что идет по оптоволоконному кабелю.

ЭНДИ: Да, потому что никогда не знаешь, кого и в чем будешь подозревать.

ДЖЕЙКОБ: В Соединенных Штатах рассматривалось дело Агентства национальной безопасности (АНБ) и компании AT&T – второе дело, «Хептинг против AT&T». В Фолсоме, штат Калифорния, Марк Клейн, бывший технический работник телекоммуникационного гиганта AT&T, сообщил, что АНБ сохраняло всю информацию, которую могло получить от AT&T. Они забирали ее оптом – сетевое общение и телефонные звонки, – а значит, всякий раз, когда я звонил по телефону или подключался к Сети в Сан-Франциско в период, о котором говорил Марк Клейн, АНБ получало всю информацию. Оно действовало на территории США против американских граждан[46]. Я более чем уверен в том, что АНБ использовало

[46] Дело о несанкционированной слежке АНБ, рассматривавшееся в суде на территории США, – самый значительный скандал с массовой слежкой в истории Соединенных Штатов. Американский закон о слежке за иностранной разведкой 1978 года (FISA, Foreign Intelligence Surveillance Act 1978, FISA) запрещал госучреждениям шпионить за гражданами США без санкции суда. После событий 11 сентября АНБ стало в массовом порядке нарушать FISA, получив на это секретное распоряжение президента Джорджа Буша. Администрация Буша утверждала, что отдать распоряжение позволило чрезвычайное законодательство, принятое Конгрессом в 2001 году, – разрешение на применение вооруженных сил (The Authorization for the Use of Military Force, AUMF) и патриотический закон. Программа АНБ по несанкционированной слежке на территории США – включая взаимодействие с частными компаниями, в числе которых и AT&T, – оставалась секретной до 2005 года, когда ее разоблачила газета New York Times. См. «Bush Lets U. S. Spy on Callers Without Courts», New York Times, 16 декабря 2005 года, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.Журналисты New York Times узнали о несанкционированной программе слежения АНБ от анонимного информатора. В 2004 году тогдашний ответственный издатель газеты Билл Келлер согласился с требованием администрации Буша не предавать эту информацию огласке в течение года, пока Буш не будет переизбран на новый срок. Однако в 2005 году New York Times поспешила опубликовать материал, когда узнала о том, что власти пытаются получить судебное решение о предварительном запрете на публикацию, как это было в истории с «документами Пентагона».Администрация Буша отрицала тот факт, что программа АНБ незаконна. Министерство юстиции сразу же стало искать источник утечки информации, бросив на дело 25 федеральных агентов и пять прокуроров. Руководство Республиканской партии призвало наказать New York Times по закону о шпионаже.После того как New York Times опубликовала материал, на контакт с прессой вышли другие информаторы, и постепенно стала вырисовываться подробная картина беззакония и бесполезной траты средств вследствие решений, принятых на высшем уровне АНБ. Адвокатские группы вроде Американского союза защиты гражданских свобод (АСЗГС) и Фонда электронных рубежей (ФЭР) подали ряд групповых исков. В одном из этих дел, «АСЗГС против АНБ», суд отказал в удовлетворении иска,

перехваченную информацию в расследованиях, которые власти проводили, чтобы доказать вину тех или иных людей, и здесь есть множество интересных нюансов, связанных с конституционными правами, – ведь хранить эту информацию они собираются вечно.

ЖЕРЕМИ: Еще есть пример системы Eagle, которую французская компания Amesys продала ливийскому диктатору Каддафи, и в коммерческом договоре значилось: «Механизм перехвата информации в масштабах страны». По сути это была большая коробка: устанавливаешь ее где-либо – и прослушиваешь разговоры всех своих подданных[47].

ДЖУЛИАН: Десять лет назад тотальная слежка казалась фантастикой, в нее верили только параноики, но сегодня стоимость массового перехвата снизилась до того, что даже страны вроде Ливии со сравнительно небольшими ресурсами могут позволить себе приобретать французскую технологию. Большинство стран мира уже перехватывают все инфопотоки. Следующий прорыв случится, когда власть научится понимать перехваченную и

поскольку истцы не смогли доказать, что слежка осуществлялась за ними персонально. В другом, «Hepting против AT&T», информатор из AT&T Марк Клейн дал под присягой письменные показания и тем самым разоблачил сотрудничество AT&T с программой слежки. См. раздел «Hepting v. AT&T» на сайте ФЭР: https://www.eff.org/cases/hepting.Марк Клейн проходил по делу «Хептинг против AT&T» свидетелем. В письменных показаниях бывшего работника AT&T из Фолсома, Сан-Франциско, утверждалось, что существует «комната 641A» – объект, на котором корпорация осуществляет стратегический перехват телефонных звонков для АНБ. На объекте имеется доступ к оптоволоконным магистралям, что позволяет отслеживать весь интернет-трафик, проходящий через здание, как иностранный, так и американский. По оценке информатора из АНБ Уильяма Бинни, таких объектов существует по меньшей мере два десятка, и все они размещены в ключевых узлах телекоммуникационной сети Соединенных Штатов.Клейн сообщил важные сведения о характере программы слежки, подтвержденные информаторами из АНБ. Это пример «стратегического перехвата информации» – весь сетевой трафик, проходящий через США, копируется и хранится неограниченное время. Можно с уверенностью сказать, что весь внутриамериканский трафик также перехватывается и хранится, поскольку с технологической точки зрения при таком объеме данных невозможно отфильтровать ту их часть, для которой необходима санкция по FISA. Нынешнее официальное юридическое толкование этого закона гласит, что перехват имеет место, когда сотрудники АНБ получают доступ к сохраненному в базе данных внутриамериканскому трафику – только на этом этапе необходима санкция суда. Граждане США должны сделать вывод, что весь их телекоммуникационный трафик (включая телефонные звонки, SMS, электронные письма и информацию, просматриваемую через браузер) отслеживается и навечно сохраняется в дата-центрах АНБ.В 2008 году в ответ на большое количество исков, поданных по следам скандала с прослушкой, Конгресс США принял поправки к закону FISA 1978 года, немедленно подписанные президентом. Они позволяют тем, кто виновен в нарушении FISA, воспользоваться весьма спорной «неподсудностью, имеющей обратную силу». Сенатор Барак Обама во время своей президентской кампании сделал «прозрачность» частью предвыборной платформы и пообещал информаторам защиту, но после того как в 2009 году Обама возглавил администрацию, Министерство юстиции продолжило политику Буша, в итоге AT&T воспользовалось «имеющей обратную силу неподсудностью» в деле Hepting и других.Министерству юстиции не удалось обнаружить человека, снабдившего информацией газету New York Times, однако оно изобличило информаторов, появившихся после публикации этого материала. Один из них, Томас Дрейк, бывший руководитель высшего ранга из АНБ, много лет жаловался в комитет Конгресса по контролю над разведывательной деятельностью на коррупцию и бесполезную трату средств в программе АНБ «Следопыт». Внутренним жалобам так и не дали хода; все правительственные чиновники, желавшие что-либо сделать, ничего не добились. После статьи в New York Times Дрейк рассказал о программе «Следопыт» газете Baltimore Sun. Большое жюри предало Дрейка суду, назвало его «врагом государства» и обвинило в нарушении закона о шпионаже. См. The Secret Sharer, New Yorker, 23 мая 2011 года: http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer?currentPage=all.В июне 2011 года на дело Томаса Дрейка обратила пристальное внимание общественность, и оно развалилось. После неудачных попыток принудить обвиняемого к сделке и признанию вины Министерство юстиции смирилось с тем, что суд признал Дрейка виновным в части единственного мелкого проступка. Дрейк был осужден на один год условно.Шлейф скандала со слежкой АНБ тянется до сегодняшнего дня. АСЗГС оспаривает конституционность принятых в 2008 году поправок к FISA в деле «Amnesty и другие против Клэппер». См. FISA Amendment Act Challenge, ACLU, 24 сентября 2012 года: http://www.aclu.org/national-security/amnesty-et-al-v-clapper.В деле «Джуэл против АНБ» ФЭР пытался положить конец несанкционированной слежке АНБ. В 2009 году дело было прекращено, после того как администрация Обамы объявила агентство неподсудным в силу сохранения государственной тайны. См. сайт ФЭР о деле «Джуэл против АНБ»: https://www.eff.org/cases/jewel. Тем не менее в декабре 2011 года Девятый окружной апелляционный суд разрешил возобновить дело. Показания по нему дают Томас Дрейк, а также Уильям Бинни и Керк Вибе – информаторы из АНБ. Администрация Обамы, обещавшего сделать государство «прозрачным», обвинила в нарушении закона о шпионаже большее число информаторов, чем предыдущие администрации, вместе взятые. (Все ссылки в этом примечании проверены 23 октября 2012 года.)

[47] См. запись о системе Eagle на сайте buggedplanet: http://buggedplanet.info/index.php?title=AMESYS#Strategic_.28.22Massive.22.29_Appliances (проверено 22 октября 2012 года).

сохраненную информацию и эффективно на нее реагировать. Сегодня во многих странах идет стратегический перехват всего инфопотока внутри государства, а также инфопотока из страны вовне, но что касается последующих действий – автоматической блокировки банковского счета и развертывания полицейской операции, обособления каких-то одних групп и освобождения от ответственности других, – до этого еще не дошло. Siemens продает платформу для разведки с автоматическим реагированием. То есть когда цель А появляется в стольких-то метрах от цели Б – а это можно определить по перехваченным данным сотовых телефонов – и цель А получает электронное письмо с неким ключевым словом, производится такое-то действие. Вот что нас ждет.

Борьба с тотальной слежкой по законам человеческим

ЖЕРЕМИ: Факт, что сегодня технология позволяет полностью отслеживать всяческую коммуникацию. Но у данной монеты есть и другая сторона, а именно – что мы можем сделать с этим. Надо признать, что упомянутая тобой тактическая слежка в ряде случаев применяется вполне законно: следователям, которые занимаются плохими парнями, сообществами плохих парней и т. д., использование таких средств может быть при необходимости разрешено под надзором суда. Вопрос в том, где проходит граница между судебным надзором и контролем граждан над применением подобных технологий. Это политический вопрос. Когда возникают такие вопросы, политиков, которые не понимают, о каких технологиях идет речь, просят всего лишь подписать бумагу. Я думаю, что мы, граждане, должны не просто объяснять – в том числе политикам, – как это вообще функционирует, но и вступать в политические дебаты по вопросам использования таких технологий. Я знаю, что в Германии возникло массовое движение против сохранения обобщенной информации, в результате чего конституционный суд отменил соответствующий закон[48]. В ЕС продолжают спорить о пересмотре Директивы о сохранении информации[49].

ЭНДИ: Ты говоришь о теории демократического государства, которому, конечно, нужно выявлять тут и там плохих парней и прослушивать их телефонные разговоры на основании судебного решения – плюс вести надзор за тем, чтобы прослушка осуществлялась по правилам. Беда в том, что власти должны исполнять законы. Если власти этого не делают, зачем они вообще нужны? Особенно необходимо исполнять законы в части стратегического подхода. А демократические страны Европы оптом закупают аппаратуру, которая позволяет им перехватывать инфопоток, действуя за рамками закона. Судебное решение им не нужно, они просто включают машину и прослушивают тебя – и такую технологию никак не проконтролируешь.

ДЖУЛИАН: Правильно ли будет сказать, что с массовой государственной слежкой можно бороться двумя способами: по законам физики и по человеческим законам? Первый способ – создавать устройства, которые предотвращают перехват. Второй – ввести демократический контроль, то есть принимать законы, запрещающие прослушку без ордера и т. д., и пытаться регулировать слежку на практике. Однако стратегический перехват так просто не одолеешь, его невозможно целенаправленно ограничить законами. Стратегический перехват означает, что вся информация сохраняется вне зависимости от того, виновен человек или нет. Мы должны помнить, что такая слежка ведется именно сильными мира сего. Политики никогда не пойдут на разоблачение государственной слежки. Между тем технология сама по себе столь сложна, а ее использование столь засекречено, что никакой демократический надзор тут не поможет.

---

[48] German court orders stored telecoms data deletion, BBC, 2 марта 2010 года: http://news.bbc.co.uk/1/hi/world/europe/8545772.stm (проверено 15 октября 2012 года).

[49] Директива 2006/24/ЕС Европейского парламента и совета требует от стран Европы сохранять данные телекоммуникации граждан от шести месяцев до двух лет. В Германии применение этой директивы в отношении тамошних законов было признано неконституционным. В мае 2012 года Комиссия ЕС передала дело Германии в Европейский суд за неподчинение директиве (см. пресс-релиз Комиссии: http://europa.eu/rapid/press-release_IP-12–530_en.htm (проверено 15 октября 2012 года)).

ЭНДИ: Еще можно следить за собственным парламентом.

ДЖУЛИАН: При этом всегда можно оправдать слежку – сославшись на мафию, на иностранную разведку, – чтобы народ согласился с созданием такой системы.

ДЖЕЙКОБ: Четыре всадника Инфокалипсиса: детская порнография, терроризм, отмывание денег и война с некоторыми наркотиками.

ДЖУЛИАН: И если такая сложная и секретная на уровне проекта система уже создана, разве возможно контролировать ее политическими средствами? Я думаю, если убрать за скобки очень маленькие страны вроде Исландии, законы и политики не в состоянии взять массовый перехват под контроль – разве что в государстве произойдет революция. Законы тут бессильны. Слишком дешево и просто обойти политиков и следить за людьми без их ведома. В 2008 году шведский парламент принял закон о перехвате информации, так называемый FRA-lagen, по которому шведская разведка, занимающаяся криптоанализом, или FRA, может законно перехватывать любую информацию в любом количестве внутри страны и переправлять ее в Соединенные Штаты – с некоторыми оговорками[50]. Но если уж созданы система перехвата и организация, секретно шпионящая за людьми, о каких оговорках может идти речь? Выполнить требования закона нереально. И действительно, появились судебные дела, доказывающие, что FRA не раз нарушала закон. Многие страны следят за гражданами вообще без всяких законов. И это очень крупное везение, если, как в Швеции, власти решают защитить от преследования самих себя и меняют законодательство. Это, кстати, типичная реакция – когда речь идет о массовой слежке, закон принимается лишь для того, чтобы прикрыть задницу самих следящих.

Что касается технологии, она очень сложна; например, когда в Австралии и Великобритании обсуждался закон, который позволил бы перехватывать все метаданные, большинство не понимало, чем именно они ценны и что вообще значит само это слово[51]. Перехват метаданных подразумевает создание системы, которая физически перехватывает всю информацию и потом отбрасывает все, кроме метаданных. Но такой системе нельзя доверять. Понять, что именно она перехватывает и сохраняет, можно одним способом – привлекая очень опытных инженеров, которые обладают правом войти в систему и посмотреть, что именно она делает, а политики не склонны давать кому-то такое право. Проблема становится все менее разрешимой, потому что сложность и секретность – это гремучая смесь. Система непрозрачна из-за сложности. И непрозрачна из-за секретности. В нее встроена бесконтрольность. Таково свойство системы. Она опасна по определению.

ЖЕРЕМИ: Я не говорю, что политический подход работает. Я говорю о том, как в теории функционирует демократическое государство – и действительно, даже внутри такого теоретического государства имеются спецслужбы, которым позволено то, что запрещено обычным полицейским и следователям. И даже если мы должным образом ограничим зако-

---

[50] См. Sweden approves wiretapping law, BBC, 19 июня 2008 года: http://news.bbc.co.uk/1/hi/world/europe/7463333.stm. Подробнее о FRA-lagen см. Wikipedia: http://en.wikipedia.org/wiki/FRA_law (обе ссылки проверены 10 октября 2012 года).

[51] Метаданные – «данные о данных». В контексте обсуждения термин обозначает информацию, не относящуюся к собственно контенту электронной коммуникации. Это что-то вроде надписи на конверте, а не текст находящегося в нем письма. Отслеживание метаданных затрагивает не содержание электронных сообщений, а всю остальную информацию: кто отправил письмо и кто его получил, IP-адрес (а значит, и физическое место), откуда было послано письмо, время и дата отправки и т. д. Фокус, однако, заключается в том, что технология для перехвата метаданных используется та же самая, что и для перехвата контента. Если вы наделяете кого-то правом следить за вашими метаданными, оборудование будет перехватывать и содержимое коммуникации. Кроме того, большинство людей не понимают, что «метаданные в сумме есть содержание»: если метаданные собрать вместе, они дают фантастически подробную картину чьей-либо коммуникации.

нами обычных следователей, те, кто использует технологии слежки, никуда не исчезнут. На самом деле вопрос заключается вот в чем: должны ли мы, вместо того чтобы контролировать использование технологий, взять под контроль торговлю и владение ими?

ДЖУЛИАН: Речь идет об аппаратуре для массовой слежки, которая перехватывает инфопотоки половины страны или города.

ЖЕРЕМИ: Именно. Это как с ядерным оружием: вы не можете просто взять и продать ракету, и хотя некоторые страны желают создать свое ядерное оружие, у них возникают проблемы. Когда мы говорим о системах вооружения, регулирование идет на уровне технологии, а не ее использования. Я думаю, дискутировать надо о том, должны ли технологии массовой слежки расцениваться как военные.

ДЖЕЙКОБ: Да и нет. Когда это оружие – а в странах вроде Сирии или Ливии оборудование для слежки превращается в оружие, – его применяют специфически, чтобы выявить политических оппонентов. Французская компания Amesys прослушивала британцев, используя технику, применять которую законы Франции запрещают, и успешно продавала свои услуги[52].

ЭНДИ: Во Франции они на такое не пошли бы, да?

ДЖЕЙКОБ: Ну, Amesys поймали за руку, когда The Spy Files опубликовали ее внутренние документы[53]. Рассуждая о данной технологии как об оружии, мы должны помнить, что это не грузовик. Тот, кто продает ее какой-то стране, предоставляет ей грузовик, механика и команду снайперов, которые ездят в кузове, выбирают людей по какому-то признаку и убивают их.

ДЖУЛИАН: Скорее это целая армия грузовиков.

ЭНДИ: Любопытно, как регулируется использование криптографии. Есть Вассенарские соглашения, они применяются на международном уровне – то есть вы не можете экспортировать шифровальные технологии, которые помогают обезопасить покупателя от слежки, в страны, объявленные плохими или – по каким-то причинам – проблемными. Но если вы продаете оборудование для слежки, ограничений нет. Никаких запретов на экспорт. Причина, я полагаю, проста: даже у демократических правительств есть свой интерес, и он состоит в том, чтобы осуществлять контроль. Даже торгуя с плохими странами и поставляя им оборудование для слежки, чтобы они делали ужасные вещи, вы выигрываете, потому что узнаёте, кого именно власти этой страны прослушивают, чего боятся, кто в стране возглавляет оппозицию, кто организует политические мероприятия и т. д. Значит, вы в силах предсказать грядущие события, понять, кого вам следует финансировать, и т. д. Я вижу тут очень грязную игру, которая идет между государствами, и возможна она потому, что продажа технологий для слежки законом никак не регулируется.

---

[52] Amesys входит в концерн Bull, некогда конкурировавший с Dehomag, филиалом IBM, за право поставлять нацистам системы перфокарт. См.: Эдвин Блэк «IBM and the Holocaust» (Crown Books, 2001). Подробнее о том, как Каддафи шпионил за ливийцами в Великобритании, используя оборудование Amesys, см. Exclusive: How Gaddafi Spied on the Fathers of the New Libya, OWNI.eu, 1 декабря 2011 года: http://owni.eu/2011/12/01/exclusive-how-gaddafi-spied-on-the-fathers-of-the-newlibya (проверено 22 октября 2012 года).

[53] Проект WikiLeaks начал выкладывать The Spy Files («Шпионские файлы»), по которым можно судить о масштабах массовой слежки, в декабре 2011 года. Эти документы находятся по адресу http://wikileaks.org/the-spyfiles.html.

ДЖУЛИАН: Я бы остановился на аналогии между массовой слежкой и оружием массового уничтожения. Законы физики позволили создать атомную бомбу, и с ее появлением изменилась геополитика, изменилась жизнь множества людей, хоть и по-разному – кто-то, наверное, стал жить лучше, кто-то ощутил себя на краю полного апокалипсиса. Появились соглашения по контролю, которые пока что – если не считать Японии – спасали нас от ядерных ударов. При этом факт применения и неприменения ядерного оружия очевиден. За последние десять лет массовая слежка очень сильно усложнилась и подешевела: мы живем в эпоху, когда население удваивается каждые двадцать пять лет, между тем мощность слежки удваивается каждые полтора года. Кривая роста слежки круче кривой роста населения. Слежки не избежать. Сегодня за 10 миллионов долларов можно купить аппаратуру, способную непрерывно сохранять перехваченные инфопотоки страны средних размеров. Должна ли наша реакция быть эквивалентной? Демократия и свобода по всему миру оказались под очень серьезной угрозой, на нее нельзя не реагировать, точно так же как нельзя не реагировать на угрозу атомной войны – и нельзя не контролировать ядерное оружие, пока мы способны это делать.

ЭНДИ: В Ливии я видел, как демократически настроенные повстанцы ворвались на станции слежения, забрали записи, доказали, что западные компании помогали режиму Каддафи подавлять политические акции, а потом новое правительство прибрало станции слежения к рукам и теперь снова эксплуатирует их на полную мощность[54]. Я согласен, что контроль над технологией – идея хорошая, но вместе с тем я скептически отношусь к противопоставлению интересов граждан и властей. Я бы даже не говорил о правительствах, потому что властью обладает тот, у кого есть возможность прослушивать все телефонные разговоры. То же самое с ценами на бирже – с чисто экономической точки зрения вы заработаете кучу денег, если знаете, что именно происходит.

[54] Подробнее см. buggedplanet: http://buggedplanet.info/index.php?title=LY.

Конец ознакомительного фрагмента.