МИРОВОЙ БЕСТСЕЛЛЕР

Эрик Шмидт / председатель совета директоров компании Google
Джаред Коэн / директор Google Ideas

НОВЫЙ ЦИФРОВОЙ МИР

Как технологии меняют жизнь людей, модели бизнеса и понятие государств

Eric Schmidt and Jared Cohen

The New Digital Age

RESHAPING the FUTURE of PEOPLE, NATIONS and BUSINESS

ALFRED A. KNOPF
NEW YORK 2013

Эрик Шмидт и Джаред Коэн

Новый цифровой мир

КАК ТЕХНОЛОГИИ МЕНЯЮТ ЖИЗНЬ ЛЮДЕЙ, МОДЕЛИ БИЗНЕСА И ПОНЯТИЕ ГОСУДАРСТВ

Перевод с английского Сергея Филина

Издательство «Манн, Иванов и Фербер»
Москва, 2013

Информация от издательства

Шмидт, Э.
Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств / Эрик Шмидт, Джаред Коэн ; пер. с англ. Сергея Филина. — М. : Манн, Иванов и Фербер, 2013.

ISBN 978-5-91657-824-9

Мир стремительно меняется под влиянием цифровых технологий: личность отдельного человека, социум в целом, политика и экономика практически полностью зависят от них. Личность и государство, информационные войны и терроризм, бизнес и экономика, технологии и коммуникации — оцифровано, кажется, уже все. Выигрывает тот, кто лучше приспособится к этому «дивному новому миру».
Чтобы заглянуть в будущее, понять «тектонические сдвиги» и играть на опережение, прочтите эту книгу. Фактам и прогнозам можно доверять: она написана председателем совета директоров Google Эриком Шмидтом и директором научного центра Google Ideas, по совместительству членом Совета по международным отношениям США Джаредом Коэном. Они как никто другой понимают, куда нас приведут сегодняшние разработки.

Посвящается Ребекке, которой мы признательны за идеи
и поддержку, и Эйдену, которому мы немного завидуем:
он увидит в своей жизни столько новых достижений
высоких технологий!

О будущем стоит думать всем,
ведь в нем мы проведем остаток нашей жизни.

— Чарльз Кеттеринг,
американский изобретатель
и бизнесмен

Введение

Интернет относится к тем изобретениям, которые люди создали, но пока не поняли до конца. То, что вначале было лишь инструментом передачи цифровых данных с одного компьютера размером с комнату на другой, трансформировалось в доступное и многообразное средство самовыражения. Казалось бы, интернет нематериален, но при этом он постоянно мутирует, растет, ежесекундно усложняется. Он несет и блага, и беды, и мы только сейчас начинаем осознавать степень его влияния на наш мир.

Интернет — это крупнейший в истории анархистский эксперимент. Каждое мгновение сотни миллионов людей создают и потребляют в онлайн-пространстве невообразимые объемы информации, и пространство это фактически не имеет границ, в рамках которых действовали бы национальные законы. Благодаря новым возможностям для свободного выражения своего мнения и свободного перемещения информации возник уже хорошо знакомый нам сложный виртуальный ландшафт. Только подумайте, сколько сайтов вы посетили, сколько сообщений электронной почты отправили, сколько историй прочитали в интернете, сколько фактов узнали, со сколькими вымыслами столкнулись! А сколько благодаря этой универсальной платформе завязано отношений, спланировано путешествий, найдено мест работы; сколько раз здесь рождались и воплощались в жизнь мечты! Подумайте и о том, к чему приводит отсутствие контроля сверху: о схемах онлайн-мошенничества, о кампаниях травли, о сайтах, на которых разжигается ненависть к определенным группам людей, о форумах террористов. Все это интернет — крупнейшее в мире самоуправляемое пространство.

По мере расширения этого пространства будут меняться наши представления практически о каждом аспекте жизни — от повседневных мелочей до фундаментальных понятий, касающихся личности, отношений с окружающими и даже собственной безопасности. Под мощным напором новых технологий одна за другой

рушатся традиционные преграды на пути общения людей: расстояния, языки, ограниченный доступ к информации — и начинается подъем новой волны творчества и развития человеческого потенциала. Массовое распространение интернета привело к одной из наиболее поразительных социальных, культурных и политических трансформаций в истории, и сейчас, в отличие от былых времен, мы сталкиваемся с поистине глобальными переменами. Никогда прежде у такого огромного количества людей из разных стран не появлялось столько возможностей. И хотя эта технологическая революция, конечно же, не первая в истории человечества, *впервые* любой из нас может создавать электронную информацию, владеть ею и распространять ее в режиме реального времени, не привлекая посредников.

А ведь все только начинается...

* * *

Коммуникационные технологии распространяются по свету с беспрецедентно высокой скоростью. В первом десятилетии XXI века число людей, имеющих доступ к интернету, во всем мире значительно выросло с первоначальных 350 миллионов, превысив два миллиарда. В то же самое время количество абонентов сотовой связи увеличилось с 750 миллионов до более чем пяти миллиардов (а сейчас их больше шести миллиардов). Эти технологии встретишь в самом отдаленном уголке планеты, во многих регионах мира они развиваются семимильными шагами.

К 2025 году большинство обитателей Земли за время жизни всего лишь одного поколения преодолеют путь от практически полного отсутствия доступа к «нефильтрованной» информации до обладания всей информацией мира, причем с помощью устройства, которое умещается на ладони. Если сохранится нынешний темп развития технологических инноваций, большинство из восьми миллиардов землян к тому моменту станут выходить в сеть.

Интернет будет становиться все доступнее, в том числе и по цене. Повсюду появятся сети Wi-Fi, в разы дешевле существующих. Мы станем еще эффективнее, производительнее и креативнее. В развитых

странах общественные точки беспроводного доступа и высокоскоростные домашние сети, дополняя друг друга, позволят выходить в интернет даже там, где сегодня нет обычной телефонной связи. Эти регионы фактически перескочат через целый технологический этап. В конечном счете технические новинки, которыми мы гордимся сейчас, станут продаваться на блошиных рынках в качестве предметов старины, как их предшественники — дисковые телефоны.

Расти будет не только область применения электронных устройств, но также их скорость и вычислительная мощь. По закону Мура[1], эмпирическому правилу области высоких технологий, скорость микропроцессора — небольшой печатной платы, лежащей в основе любого компьютерного устройства, — удваивается каждые полтора года. Это значит, что в 2025 году компьютер будет считать в 64 раза быстрее, чем в 2013-м. Закон фотоники (это область науки, посвященная передаче информации с помощью модулируемых потоков света) гласит, что объем данных, исходящих из оптоволоконных кабелей, которые обеспечивают наибольшую скорость их передачи, удваивается примерно каждые 9 месяцев. И даже если действие этого закона ограничено естественными причинами, перспектива экспоненциального роста обещает появление таких возможностей в компьютерной графике и виртуальной реальности, которые позволят получать онлайн-впечатления, сравнимые по реалистичности с самой жизнью или даже лучше ее. Представьте, что у вас есть холодек из фильма Star Trek, который создавал для экипажа звездолета виртуальную реальность с полным эффектом присутствия, но такой, который способен как спроецировать перед вашими глазами тропический пляж, так и воссоздать атмосферу концерта Элвиса Пресли. Действительно, за следующим поворотом технологической революции нас ждет превращение многих научно-фантастических сюжетов в научно неоспоримые факты: автомобили без водителя; роботы, управляемые силой мысли; искусственный интеллект; виртуальная реальность с полным эффектом присутствия, позволяющая наложить цифровое изображение на окружающую нас

обстановку. Все эти достижения сольются с физическим миром и дополнят его.

Таково наше будущее, и эти фантастические вещи уже начинают воплощаться в жизнь. Вот почему сегодня так интересно работать в отрасли высоких технологий. И не только потому, что у нас есть возможность создавать удивительные устройства, и не из-за масштаба технологических и интеллектуальных проблем, которые приходится решать, а в силу того, что значат для мира наши открытия.

Коммуникационные технологии позволяют совершить прорыв не только в технической, но и в культурной сфере. Онлайн-вселенная будет продолжать влиять на то, как мы взаимодействуем с другими и какими видим себя. Наша память избирательна, и это позволяет нам быстро приобретать новые привычки и забывать старые. Сегодня трудно представить свою жизнь без мобильных устройств. В эпоху вездесущих смартфонов вы застрахованы от забывчивости, у вас есть доступ к целому миру идей (пусть некоторые государства и стараются его затруднить), да и занять себя всегда есть чем, хотя провести время с пользой по-прежнему трудно, иногда даже труднее, чем раньше. *Смартфон*[2] — действительно удачное название.

Сейчас, когда количество пользователей интернета во всем мире растет беспрецедентно высокими темпами, многим традиционным институтам и иерархическим структурам придется измениться, или они безнадежно устареют, перестав соответствовать требованиям современного общества. О серьезных переменах, ожидающих общество в ближайшем будущем, говорят трудности, с которыми уже столкнулись многие крупные и мелкие компании. Коммуникационные технологии продолжат трансформировать сложившиеся общественные институты и внутренне, и внешне. Нам будет все легче связываться с людьми, живущими очень далеко, чтобы общаться с ними, строить бизнес и налаживать тесные отношения.

Большинство жителей планеты станут все чаще замечать, что живут и работают как бы в двух различных мирах одновременно. В виртуальном мире все мы так или иначе будем иметь доступ к информации, причем быстрый и не зависящий от инструментов и устройств. А в реальном мире по-прежнему будем натыкаться на такие

ограничители, как география, место рождения (некоторые рождаются богатыми в богатых странах, большинство же — бедными в странах бедных), везение, светлые и темные стороны человеческой натуры. В этой книге мы хотим показать, каким образом виртуальный мир может улучшить, ухудшить или изменить мир реальный. Иногда эти миры будут ограничивать друг друга, иногда вступать в противоречия, а порой один из них будет усиливать, ускорять или обострять явления другого.

Наиболее важной ролью коммуникационных технологий станет их участие в изменении степени концентрации власти и ее перераспределении от государств и общественных институтов к гражданам. В истории человечества появление новых информационных технологий часто приводило к усилению людей за счет традиционных влиятельных сил, будь то короли, церковь или политические элиты. Сейчас, как и прежде, доступ к информации и новым каналам связи означает новые возможности для определения направления своего развития, большую вовлеченность в процесс управления своей жизнью и повышение ответственности за нее.

Самым типичным и, наверное, самым ярким примером такого сдвига в распределении власти стало, конечно же, быстрое распространение возможности связываться друг с другом посредством мобильных телефонов с функцией доступа в интернет — хотя бы по причине его масштаба.

Кто-то благодаря недорогому миниатюрному устройству заметит, что его мнение наконец было услышано и учтено, что его наконец начали принимать во внимание, и таким образом получит первый опыт власти в цифровом пространстве. В результате репрессивные государства поймут, что им все труднее контролировать, подавлять и обманывать население, получившее доступ к новым технологиям, а демократическим правительствам придется учитывать все большее количество мнений (частных лиц, организаций и компаний). Конечно, правительства всегда найдут способ воспользоваться таким беспрецедентным проникновением интернета себе во благо, но благодаря нынешней структуре сетевых технологий он приносит пользу в первую очередь людям. Причины этого мы обсудим позже.

Так безопаснее или опаснее все же станет мир в результате усиления властных полномочий граждан? Поживем — увидим. Пока же остается лишь признать реалии мира, объединенного в сеть, — как благоприятные, так и неблагоприятные. Авторы книги изучали этот вопрос с двух точек зрения: один как ученый-компьютерщик, другой как специалист по внешней политике — и хорошо понимают, что однозначного ответа на него пока нет. Будущее зависит от того, как будут выполнять свои новые обязанности государства, граждане, компании и общественные институты.

В прошлом теоретики в области международных отношений частенько обсуждали цели государственного управления. Одни утверждали, что страны проводят такую внешнюю и внутреннюю политику, которая способствует максимизации мощи и безопасности, другие считали, что есть и иные факторы, например задачи торговли и информационного обмена. Цели государств в будущем не изменятся, а вот их представления о способах достижения целей, скорее всего, будут пересмотрены. Появятся две версии внешней и внутренней политики: одна — для физического, «реального» мира, другая — для существующего онлайн мира виртуального. Иногда эти версии будут противоречить друг другу: скажем, правительство принимает жесткие меры против определенного поведения в одной из реальностей и при этом допускает его в другой; ведет войну в киберпространстве и демонстрирует миролюбие в реальном мире... Так или иначе, государства будут пытаться справиться с новыми угрозами своей власти, которые возникают в результате большей соединенности людей.

Для граждан же доступ в интернет означает обладание множественными «личностями» *как* в физическом, *так и* в виртуальном мире. Во многом виртуальные личности окажутся превыше всех остальных: следы, которые люди оставляют, будут запечатлены онлайн навеки. А поскольку то, что мы размещаем в своих постах, пишем в электронной почте и SMS, то, чем делимся в сети, оказывает влияние на виртуальные личности других людей, начнут возникать новые формы коллективной ответственности пользователей.

Рост глобальной соединенности людей означает для организаций, общественных институтов и компаний одновременно как возможности, так и угрозы. Осознавая возросший уровень ответственности перед людьми, эти политические игроки будут вынуждены переосмыслить свою деятельность, изменить планы на будущее, а также скорректировать используемые методы и ведения дел, и информирования о них общественности. Им также придется столкнуться с обострением конкуренции, ведь информационное пространство, а вместе с ним и возможности игроков постоянно расширяются с ростом доступности высоких технологий.

В будущем никто — ни самые могущественные, ни наиболее бесправные — не сможет удержаться в стороне от перемен, которые во многих случаях будут эпохальными.

* * *

Мы познакомились осенью 2009 года в весьма благоприятных для тесного общения обстоятельствах. Это было в Багдаде, где мы обсуждали с иракцами критически важный вопрос: как высокие технологии могут помочь восстановлению страны? Перемещаясь по городу с одной встречи на другую, общаясь с министрами, военными, дипломатами и предпринимателями, мы видели перед собой общество, перспективы которого на возрождение и успех в будущем, казалось, висели на волоске. Приезд Эрика стал первым визитом в Ирак CEO[3] высокотехнологичной компании из списка Fortune 500 и породил много вопросов о том, почему это вдруг Google интересуется Ираком. Поначалу даже мы не понимали до конца, с чем может столкнуться компания в этой стране, каких целей добиться.

Ответ пришел мгновенно. Всюду, куда ни кинешь взгляд, были видны мобильные устройства. Это очень нас удивило. К тому моменту в Ираке больше шести лет шла война, начавшаяся после падения режима Саддама Хусейна, который в своей тоталитарной паранойе запрещал использование мобильных телефонов. В ходе войны была практически полностью уничтожена инфраструктура, большинство жителей столкнулось с перебоями в снабжении продуктами, водой и электричеством. Недоступно дороги были даже базовые товары. В

некоторых районах мусор не убирался *годами*. И главное, никто не чувствовал себя в безопасности — ни высшие государственные чиновники, ни обычные покупатели на базаре. Казалось, что в пугающе длинном списке дел, предстоящих жителям страны, мобильные телефоны должны стоять в самом конце. Однако выяснилось, что, несмотря на все сложные проблемы, приоритет иракцы отдавали именно высоким технологиям.

При этом люди не просто владели высокотехнологичными устройствами и ценили их, но еще и ясно видели их огромный потенциал в деле улучшения своей жизни и участи всей истерзанной войной страны. Мы встречались с инженерами и предпринимателями, подавленными своей неспособностью справиться с задачей самостоятельно. Они уже знали, что для реализации их идей им нужны стабильная подача электроэнергии, приемлемая ширина канала для быстрой передачи данных, доступные цифровые устройства и достаточный объем стартового капитала.

И хотя для Эрика это был первый визит в зону военных действий, а для Джареда — энный, мы оба уезжали из Ирака с чувством, что в мире происходят глубинные сдвиги. Если даже одетые в камуфляж иракцы не только осознают возможности высоких технологий, но и точно понимают, что делать с ними, то сколько же еще миллионов людей знают об интернете и стремятся получить доступ в сеть? Джареда эта поездка убедила в том, что при прогнозировании будущих перемен правительства опасно отстают от жизни (причем страшатся этих перемен), не видя открывающихся возможностей, которые помогут справиться с предстоящими трудностями. А Эрик укрепился в мысли, что компаниям отрасли высоких технологий предстоит решить гораздо больше задач и привлечь намного большее количество клиентов, чем кажется.

В последовавшие за той поездкой месяцы нам стало ясно, что людей, разбирающихся в высоких технологиях, и тех, кто отвечает за решение сложнейших геополитических проблем, разделяет широкая пропасть и никто не пытается перебросить через нее мост. А ведь у сотрудничества участников отрасли высоких технологий, правительства и гражданского общества есть огромный потенциал. Размышляя над распространением сетевых технологий по планете, мы

увлеклись поисками ответа на связанные с этим вопросы: кто будет обладать в будущем большей властью — гражданин или государство? Облегчит или усложнит жизнь террористов развитие технологий? Как связаны тайна частной жизни и безопасность, чем придется пожертвовать ради того, чтобы стать частью новой цифровой эпохи? Как изменятся дипломатия, войны и революции в условиях всеобщей соединенности и как сохранить баланс различных интересов? Когда восстановятся разрушенные страны, что они смогут сделать в области высоких технологий?

Первым опытом нашего сотрудничества стала работа над меморандумом госсекретарю Хиллари Клинтон о полученных в Ираке уроках. Тогда мы и подружились. Мы одинаково смотрим на потенциал высокотехнологичных платформ и на власть, которой они обладают, и это наполняет особым смыслом все, что мы делаем, и не только в компании Google. Мы уверены, что такие современные высокотехнологичные платформы, как Google, Facebook, Amazon и Apple, даже могущественнее, чем считает большинство людей, и будущий мир ждут глубокие изменения в результате их успешного развития и повсеместного распространения. Эти платформы представляют собой настоящую смену парадигмы, подобно изобретению телевидения, и основная их сила заключается в способности расти, то есть в скорости изменения масштабов. Почти ничто не может сравниться со скоростью, эффективностью и агрессивностью распространения этих платформ — разве что биологические вирусы, и это наделяет соответствующей властью тех, кто их строит, контролирует и использует. Никогда прежде столько людей не были связаны сетью, сообщения по которой распространяются мгновенно. Возможности коллективных действий, появившиеся (у потребителей, творческих личностей, разработчиков, активистов и так далее) благодаря этим платформам, способны перевернуть мир. Чтобы получить некоторое представление о том, что нас ожидает, вспомните о хорошо известном влиянии масштаба: как благодаря ему становятся популярными вирусные видеоролики и международные интернет-магазины.

Благодаря эффекту масштаба, обусловленному цифровыми платформами, в новую цифровую эпоху ускорятся все явления, и это

непременно повлияет на общество в целом: на политику, экономику, средства массовой информации, бизнес и общепринятые нормы. Это ускорение и масштаб в сочетании со всеобщей связанностью, которую обеспечивают интернет-технологии, возвещают о наступлении нового этапа глобализации, а именно глобализации товаров *и* идей. Мы как участники сектора высоких технологий просто обязаны досконально и непредвзято изучить влияние, которое наша деятельность оказывала и будет оказывать на жизнь отдельных людей и общества в целом, поскольку в будущем правительствам придется устанавливать правила в условиях тесного сотрудничества как с индивидуумами, так и с корпорациями, которые развиваются невиданными темпами и частенько опережают не успевающих угнаться за ними законодателей. Создаваемые ими цифровые платформы, сети и продукты имеют огромное значение для мира в целом. Поэтому для того, чтобы понять, какое будущее ожидает политику, бизнес, дипломатию и другие важные области, нужно разобраться с тем, какие перемены в этих областях будут определяться развитием технологического сектора.

* * *

В тот момент, когда мы начали обмениваться друг с другом своими мыслями о будущем, события мирового масштаба проиллюстрировали те самые концепции и проблемы, которые мы обсуждали. Китайское правительство инициировало несколько изощренных кибератак на Google; WikiLeaks предала огласке сотни тысяч секретных документов; мощные землетрясения в Гаити и Японии разрушили целые города, но подстегнули развитие инновационных высокотехнологичных продуктов; революции «арабской весны» потрясли мир своей стремительностью, неудержимостью и возможностями мгновенной мобилизации больших масс людей. Открывались новые перспективы будущего, которые необходимо было осмыслить.

Довольно много времени мы обсуждали значения и последствия этих событий, пытаясь сформулировать тенденции и связанные с ними возможные технические решения. Результат этих разговоров — книга, которая находится перед вами.

На ее страницах мы поговорим о будущем, как мы его себе представляем: полном сложных глобальных проблем, связанных с вопросами гражданства, государственного управления, защиты частной жизни и многими другими, причем и трудности, и возможности явятся следствием глобальной связанности. Везде, где это возможно, мы рассказываем, как новые высокотехнологичные инструменты могут помочь людям узнать больше, улучшить и обогатить наш мир. Перемены, в основе которых лежит развитие технологий, неизбежны, но мы способны их контролировать. Что-то покажется вам очевидным, хотя и несколько фантастическим (например, логическое продолжение идеи коммерческих беспилотных аппаратов), а что-то станет полной неожиданностью. Надеемся, что наши прогнозы и рекомендации смогут занять ваше внимание и подтолкнут к размышлениям.

Эта книга не о гаджетах, приложениях для смартфонов и искусственном интеллекте, хотя обо всем этом пойдет речь. Можно сказать, что эта книга о высоких технологиях, но скорее она о людях, об их отношениях к высоким технологиям, о том, как люди на всей планете адаптируют их и применяют в своей жизни сегодня и завтра. А главное, она о ведущей роли человека в новой цифровой эпохе. При всех возможностях, которые несут компьютерные технологии, их использование на благо или во зло зависит исключительно от людей. Забудьте все разговоры о захвате власти машинами. Будущее зависит от нас.

Примечания к введению

ГЛАВА 1

Наше будущее «я»

Скоро все люди на Земле будут связаны друг с другом. Когда пять с лишним миллиардов человек вольются в виртуальный мир и начнут пользоваться всеми преимуществами всеобщего доступа в сеть, это благоприятно скажется на производительности, состоянии здоровья, образовании, качестве жизни и многих других аспектах реального мира, причем каждого человека — от наиболее обеспеченных до тех, кто находится в самом основании экономической пирамиды. Но понятие «иметь доступ в сеть» будет восприниматься людьми очень по-разному, в основном потому, что им придется решать разные задачи. То, что кому-то покажется ничтожным шажком вперед, например смартфон за $20, для некоторых станет столь же серьезным прорывом, как для других — поездки в офис на беспилотном автомобиле. Люди поймут, что в виртуальном мире, где мы пользуемся одними и теми же основными платформами, информацией и онлайн-ресурсами, доступ в сеть делает нас свободнее, хотя в мире реальном разрыв продолжает сохраняться. Всеобщий доступ в сеть не решит проблему неравенства доходов, хотя и облегчит некоторые его наиболее трудноизлечимые следствия вроде отсутствия экономических возможностей и недоступности образования. Именно в таком контексте следует рассматривать инновации и приветствовать их. От всеобщего доступа в сеть выиграют все, хотя и не в равной степени. Так давайте поговорим о том, как эти различия проявят себя в повседневной жизни людей.

Рост эффективности

Благодаря новым возможностям виртуального мира повысится эффективность механизмов мира реального. Когда сеть будет доступна в самых удаленных уголках планеты, новые пользователи смогут с ее

помощью улучшить функционирование различных рынков и институтов как в наиболее, так и в наименее развитых обществах. В результате резко вырастут эффективность и производительность, особенно в развивающихся странах, где экономический рост и технический прогресс многие годы подавлялись технологической изоляцией и ошибочной политикой. Люди смогут добиваться большего меньшими усилиями.

В таких странах главным катализатором станет доступность недорогих электронных устройств, включая смартфоны и планшетные компьютеры. Представим себе, как сегодня влияет на жизнь конголезской рыбачки самый простой мобильный телефон. Когда-то ей приходилось нести весь свой дневной улов на рынок, а затем наблюдать, как рыба медленно портится под солнцем. Теперь же, дожидаясь звонков от покупателей, рыбу можно держать живой в реке. Получив заказ, рыбу вытаскивают из воды и готовят к продаже. Не нужен дорогой холодильник; не нужно нанимать кого-то охранять его ночью; нет риска, что портящийся улов обесценится (или что покупатели отравятся); снижается вероятность перепроизводства. Границы рынка таких рыбачек могут даже раздвинуться за счет координации действий местных рыбаков с помощью того же телефона. В отсутствие традиционной рыночной экономики, на развитие которой могут уйти годы, это неплохой выход и для самих рыбачек, и для сообщества в целом.

Мобильные телефоны меняют методы доступа к информации и ее использованию в развивающемся мире, и область их распространения стремительно растет. В Африке уже 650 млн абонентов сотовой связи, а в Азии — около 3 млрд. Большинство этих людей пользуются лишь базовыми функциями телефонов — голосовыми звонками и текстовыми сообщениями, поскольку в тех странах стоимость передачи данных часто слишком высока, и даже те, кто может позволить себе покупку телефона с функцией выхода в интернет или смартфона, не пользуются всеми их возможностями. Но это изменится, и революция смартфонов принесет им огромную пользу.

Сегодня сотни миллионов людей живут так же, как их предки, в странах, где продолжительность жизни не превышает 60, а в некоторых местах — и 50 лет, и нет никакой гарантии, что

политическая и макроэкономическая ситуация там заметно улучшится в обозримом будущем. То новое, что войдет в их жизнь и их будущее, — это доступ в сеть. Очень важно, что у них есть шанс перескочить этап устаревших технологий вроде телефонных модемов и сразу перейти к высокоскоростным беспроводным соединениям, а это значит, что перемены, которые несет всеобщий доступ в сеть, наступят там быстрее, чем это случилось в развитых странах. Такое распространение мобильных телефонов изменит жизнь в гораздо большей мере, чем могут предполагать наши современники. Подключаясь к сети, люди внезапно получают доступ ко всей информации мира, причем на экране одного устройства и на родном языке. Это касается даже неграмотного пастуха племени масаи из Серенгети (Танзания), родной язык которого, маа, бесписьменный. С помощью голосового запроса он сможет поинтересоваться сегодняшними ценами на рынке или узнать у соседей, нет ли поблизости хищников, получив такой же устный ответ. Мобильные телефоны позволяют жителям прежде изолированных регионов связываться с теми, кто находится очень далеко — и очень сильно отличается — от них. Эти люди смогут использовать попавшие в их распоряжение устройства и с экономической точки зрения: для укрепления своего бизнеса, повышения его эффективности и максимизации прибыли (как конголезские рыбачки с их примитивными мобильниками).

Развитие технологий связи означает не только распространение мобильных телефонов, но и возможность собирать и использовать данные. Сами по себе данные — всего лишь средство, и в тех местах, где рост и развитие тормозятся из-за отсутствия надежных статистических данных о состоянии здравоохранения, образования, экономики и потребностях населения, возможность эффективно собирать статистику может изменить правила игры. От наличия таких данных выигрывает все общество, ведь правительство может более качественно измерять степень успеха своих программ, а средства массовой информации и неправительственные организации — использовать их в своей работе и проверять факты. Так, у компании Amazon есть возможность, опираясь на свои данные по продажам и применяя специальные алгоритмы, разработать и предложить

покупателям банковские займы на индивидуальных условиях, причем часто в тех случаях, когда традиционные банки захлопывают перед ними двери. А растущие рынки и качественные системы показателей могут помочь в создании более здоровой и эффективной экономики.

И развивающийся мир не останется в стороне от достижений в области разработки новых гаджетов и других высокотехнологичных устройств. Даже если цены на сложные смартфоны и домашних роботов (скажем, для уборки пыли) останутся высокими, на нелегальных рынках вроде обширной китайской «шанжай» — сети по распространению поддельной электроники — появятся и станут доступными имитации, способные заполнить эту нишу. Кроме того, технологии, возникшие в развитых странах, в развивающихся странах обретут новые функции. При аддитивном производстве, или 3D-печати, специальные принтеры способны фактически «распечатывать» физические объекты, получая трехмерные данные об этих объектах и воссоздавая их форму путем нанесения одного за другим ультратонких слоев жидкого пластика или иного материала до тех пор, пока не материализуется весь предмет целиком. Таким принтерам под силу большой диапазон задач: они могут производить корпуса мобильных телефонов, детали машин и даже копии мотоциклов в натуральную величину. Влияние этих устройств на развивающийся мир, конечно же, будет значительным. Жители бедных стран при помощи общественных 3D-принтеров и шаблонов с открытым кодом (бесплатно распространяемых программ) смогут распечатывать необходимые им инструменты и предметы вместо того, чтобы полагаться на трудоемкую или ненадежную доставку более дорогих, изготовленных заводским способом изделий.

А в богатых странах процесс 3D-печати станет отличной возможностью еще более усовершенствовать производство. На таких устройствах, управляемых опытным оператором, будут создаваться новые материалы и товары, причем в соответствии со спецификациями, передаваемыми через интернет по запросу клиента. Это не заменит гектары производственных площадей, использующихся сейчас под серийное производство во многих отраслях, но беспрецедентно расширит разнообразие продуктов, доступных жителям развитых стран.

Если говорить о повседневных бытовых заботах состоятельных потребителей, то информационные технологии облегчат многие из них: появятся интегрированные «одежные» машины, которые будут стирать, сушить, гладить, аккуратно складывать и сортировать вещи, а также обеспечивать их хранение и предлагать владельцу подходящий наряд в соответствии с его графиком на определенный день. Стрижка станет автоматизированной и будет выполняться с машинной точностью. Возможность заряжать мобильные телефоны, планшетники и ноутбуки при помощи беспроводной сети сделает зарядные устройства абсолютно ненужными. Данные о многих аспектах нашей жизни окажется возможным сосредоточить в рамках простой в использовании, интуитивно понятной системы управления информацией и принятия решений, которая позволит без усилий взаимодействовать с технологическими устройствами. При наличии соответствующего уровня безопасности, необходимого для защиты личных данных и предотвращения их утраты, такие системы смогут освободить нас от множества мелких забот, в том числе связанных с проверкой списков дел, проектов и мониторингом различных задач, которые сегодня лишь увеличивают стресс и отвлекают в течение дня. Такие информационные системы, специально разработанные для удовлетворения наших потребностей, станут дополнением к ограниченным возможностям человеческой нейробиологии, ведь все мы склонны забывать и ошибаться. В качестве примера можно привести «протезы» для памяти — напоминания в календаре и списки дел — и социальные «протезы», способные мгновенно связать вас со специалистом, имеющим опыт в любой нужной вам области.

Опираясь на такие интегрированные системы, охватывающие и профессиональную, и личную жизнь, мы сможем эффективнее распоряжаться своим временем, что бы это ни означало: больше возможностей серьезно обдумать какую-либо проблему, подольше посидеть над важной презентацией или спокойно отправиться на футбольный матч своего ребенка. Особенно полезными могут стать поисковые системы, предлагающие пользователю альтернативные варианты терминов, которые он ищет. Они будут стимулировать наш мыслительный процесс и в конечном счете усиливать творческие возможности, а не подавлять их. Конечно, мир будет переполнен

всевозможными гаджетами, голограммами, позволяющими вашей виртуальной версии быть где угодно, и бесконечным объемом контента, так что недостатка в способах бездумно потратить время тоже не будет. Однако главное здесь то, что если вы захотите быть продуктивным, то у вас будет для этого больше возможностей.

Прочное место в нашей жизни займут разработки, которые уже ведутся в области роботостроения, искусственного интеллекта и систем распознавания речи. Они упростят взаимодействие с техникой. Вероятно, полностью автоматические человекоподобные роботы с развитым искусственным интеллектом еще какое-то время будут слишком дорогими для большинства людей на планете, но средний американец довольно скоро сможет позволить себе иметь несколько различных многофункциональных роботов. Технология, использованная в пылесосе Roomba компании iRobot — прародителе «домашних» роботов, выпущенном на рынок в 2002 году, — усложнится и станет со временем более многофункциональной. Будущие разновидности таких устройств смогут с легкостью выполнять и другие работы по дому, в том числе частично заменят электрика и даже сантехника.

Не стоит недооценивать влияние, которое на нашу повседневную жизнь окажет развитие программ распознавания речи. Помимо поиска информации онлайн и передачи команд роботам (что возможно уже сегодня) совершенствование распознавания речи будет означать мгновенный перевод в напечатанный текст всего, что вы говорите: сообщений электронной почты, заметок, выступлений, курсовых работ. Большинство людей говорят намного быстрее, чем печатают, так что подобные технологии, несомненно, сэкономят нам много времени, не говоря о том, что помогут избежать кистевого туннельного синдрома[4]. А сдвиг в сторону набора текста на основе распознавания голоса вполне способен полностью изменить весь мир письменных материалов. Сможем мы говорить абзацами, или наши тексты начнут отражать речевые модели?

День, когда начнется рутинное использование технологии распознавания жестов, ближе, чем мы думаем. В 2011 году автоматический сенсор Kinect для видеоприставки Xbox компании

Microsoft, предназначенный для считывания и обработки движений игрока, поставил мировой рекорд по скорости продаж среди электронных устройств: в течение первых шестидесяти дней после вывода его на рынок было продано свыше восьми миллионов штук. Но интерфейс, основанный на распознавании жестов, вскоре найдет свое применение за пределами индустрии развлечений: информационный дисплей, столь правдоподобно изображенный в фильме Minority Report[5], где герой Тома Круза, раскрывающий преступление с помощью компьютера, использует технологию распознавания жестов и голографические изображения, — это лишь начало. На самом деле мы уже вышли за эти пределы: по-настоящему интересным направлением сегодня стала разработка «общительных роботов», способных распознавать человеческие жесты и правильно реагировать на них, как в случае с игрушечной собакой, которая выполняет команду «сидеть» после соответствующего жеста ребенка.

Если же заглянуть еще дальше, то в будущем нам, возможно, даже не придется делать никаких движений для того, чтобы манипулировать такими роботами. В последние несколько лет совершено несколько поразительных прорывов в создании технологии движения, управляемого мыслями, то есть распознавании команд, отданных мысленно. В 2012 году японская команда исследователей одной из лабораторий роботостроения успешно продемонстрировала эксперимент, в ходе которого человека помещали в аппарат МРТ (непрерывно сканировавший мозг и отслеживавший изменения потока крови) и человек управлял роботом, который находился в сотнях миль от него, просто представляя себе движения его различных конечностей. Благодаря камере, закрепленной на «голове» робота, испытуемый смотрел на мир с его точки зрения, и, когда он думал о том, как поднимает «руку» или «ногу» робота, тот выполнял команду практически мгновенно. Возможности технологии движения, управляемого мыслями, в приложении не только к «суррогатам» человека в виде отдельных роботов, но также к изготовлению протезов особенно восхищают, когда осознаешь, что они значат для инвалидов или обездвиженных пациентов с поврежденным позвоночником,

ампутированными конечностями и так далее, которые сегодня не способны передвигаться и общаться с миром.

Больше инноваций — больше возможностей

То, что процесс глобализации продолжится прежними темпами и даже ускорится по мере роста доступности сети, неудивительно. Поражает то, как могут изменить мир даже незначительные успехи в развитии технологий, если при этом возрастают доступ в сеть и взаимозависимость жителей разных стран. Благодаря мгновенному переводу с одного языка на другой, виртуальному общению и коллективному редактированию контента в режиме реального времени (примером могут быть нынешние «вики»-проекты) кардинально изменятся методы взаимодействия компаний с их партнерами, клиентами и сотрудниками. Вероятно, некоторые различия, такие как культурные особенности и часовые пояса, никогда не будут преодолены, но способность общаться с людьми из других стран, практически полностью понимая друг друга и имея возможность использовать платформы с совместным доступом, сильно упрощает такое взаимодействие.

Корпоративная логистика будет все менее интегрированной, и не только на уровне производства, но и в отношении человеческих ресурсов. Благодаря более эффективным трансграничным и межъязыковым коммуникациям возникнет необходимый уровень доверия и появятся новые возможности для трудолюбивых и талантливых людей всего мира. Для французской технологической компании станет привычным, скажем, привлечь команду продавцов из Юго-Восточной Азии, отдел по управлению персоналом держать в Канаде, а инженеров нанимать в Израиле. По мере развития цифровых платформ удастся преодолеть или обойти бюрократические препоны вроде визовых ограничений и правил перевода денежных средств, стоящие сейчас на пути такого рода децентрализации. Вполне возможно, что сотрудники правозащитных организаций, находящиеся в стране, против которой введены жесткие дипломатические санкции, будут получать зарплату посредством мобильных переводов или даже просто электронными деньгами.

По мере того как наше физическое присутствие в офисе будет требоваться все реже, перед талантливыми людьми начнут открываться новые горизонты. Образованная молодежь из Уругвая сможет конкурировать со сверстниками из Калифорнии, претендуя на некоторые должности. Разумеется, как не все виды работ могут быть и будут автоматизированы в будущем, так и не каждый проект удастся выполнять дистанционно, но все же таких работ больше, чем кажется. Для тех же, кто живет всего на несколько долларов в день, появятся неограниченные возможности роста доходов. Уже сейчас можно привести в пример компании, передающие на аутсорсинг мелкие задачи, которые способен выполнить за несколько центов любой человек, имеющий компьютер. В частности, это делается в рамках цифровой платформы распределения задач Amazon Mechanical Turk. По мере повышения качества виртуального взаимодействия диапазон профессий специалистов, доступных клиентам этой платформы, будет постоянно расти: вы сможете привлечь юриста, живущего на одном континенте, а риелтора — на другом. Критики глобализации осудят такое разрушение местных монополий, но это следует только приветствовать: лишь так наше общество сможет двигаться вперед и продолжать развиваться. И действительно, всеобщий доступ в сеть должен *помочь* странам выявить свои конкурентные преимущества: вполне возможно, что лучшие в мире графические дизайнеры живут в Ботсване, а мир пока просто не знает об этом.

Уравнивание правил игры коснется не только талантливых людей — его можно распространить и на мир идей. Инновации все чаще станут появляться не в традиционных центрах роста, а на окраинах, поскольку люди там по мере налаживания новых связей получат возможность смотреть на сложные задачи со своей уникальной точки зрения, тем самым стимулируя перемены. Новый уровень международного сотрудничества и «перекрестное опыление» между разными секторами экономики приведут к тому, что у многих отличных идей и решений появится шанс подняться на поверхность. Их разглядят, осмыслят, изучат, профинансируют, внедрят и признают. Может так случиться, что талантливый программист из России, ныне работающий учителем в школе, придумает новое применение технологии, которая лежит в основе популярной мобильной игры

Angry Birds, и поймет, как с ее помощью усовершенствовать созданные им компьютерные учебные пособия по физике для школьников. Он найдет аналогичное игровое программное обеспечение, но распространяемое свободно, и использует его. Поскольку движение по разработке программ с открытым кодом продолжает набирать силу во всем мире (правительствам и компаниям это позволяет снизить издержки, разработчики же выигрывают благодаря широкому признанию и возможностям заниматься усовершенствованием и поддержкой продукта), в распоряжении нашего учителя-программиста из России окажется огромное количество технических средств для учебы и применения в новых проектах. В эпоху всеобщего доступа к сети у него появится все больше шансов быть замеченным «нужными» людьми, получить предложение о работе или партнерстве, наконец, продать свое творение крупной транснациональной корпорации. Как минимум он сможет начать с ней общаться.

> Инновации могут распространяться снизу вверх, но не все идеи, родившиеся на местном уровне, будут приняты на международной арене, поскольку некоторые предприниматели и изобретатели ориентируются на очень узкую целевую аудиторию и решают весьма специфические задачи. Так бывает и сегодня. Двадцатичетырехлетний кениец Энтони Мутуа представил в 2012 году на научной выставке в Найроби разработанный им ультратонкий кристаллический чип, генерирующий электроэнергию при нажатии на него. Мутуа поместил чип в подошву своего ботинка и продемонстрировал, как с его помощью можно заряжать мобильный телефон во время ходьбы. (Это говорит о том, что отсутствие надежной и доступной электроэнергии и короткий срок службы аккумуляторов (а также нежелание многих правительств восстанавливать электрические сети) является настолько серьезной проблемой для многих, что изобретатели вроде Мутуа вынуждены разрабатывать микросхемы, превращающие людей в мобильные зарядные устройства.) Чип, изобретенный Мутуа, вот-вот начнут производить серийно, и, если ему удастся снизить его стоимость, это будет гениальное устройство. Только вот востребовано оно будет лишь в развивающихся странах — по той простой причине, что только там в нем есть необходимость.

К сожалению, доступность технологий для населения часто определяется внешними факторами. Даже если бесперебойное электроснабжение в конечном счете будет обеспечено (правительством

или самими гражданами), нельзя предугадать, всем ли людям представятся одинаковые возможности иметь современные услуги связи.

* * *

В ближайшие десятилетия преобразится и наиболее важное связующее звено между инновациями и возможностями — образование, ведь доступность интернета видоизменяет привычные методы обучения и предлагает новые возможности для получения знаний. Большинство школьников будут владеть компьютерной «грамотой», ведь школы продолжат внедрять обучение современным компьютерным технологиям в учебные планы, а в некоторых случаях даже заменять традиционные уроки интерактивными семинарами. Образование станет более гибким и адаптированным, учитывающим индивидуальный стиль и темп обучения ребенка. Дети по-прежнему будут ходить в школу для того, чтобы общаться между собой и с учителями. Однако как минимум в половине (а может, и большей части) уроков станут использовать тщательно разработанные учебные инструменты в духе академии Хана (Khan Academy) — некоммерческой организации, которая производит тысячи коротких видеороликов (в основном по математике и естественным наукам) и бесплатно распространяет их в интернете.

> Ролики академии на YouTube набрали уже сотни миллионов просмотров, а преподаватели в США все активнее адаптируют эти материалы и интегрируют в свои программы подход ее основателя, Салмана Хана, заключающийся в модульном обучении, подстроенном под нужды учеников. Некоторые из них даже полностью изменили подход к работе в классе, заменив лекции видеороликами, которые учащиеся смотрят дома вместо традиционных домашних заданий, а задания выполняют в школе, например решая задачи по математике.

По мере повсеместного распространения инструментов «цифрового знания» вроде «Википедии», которые снижают необходимость механического запоминания, во многих школьных системах фокус будет смещаться на развитие способностей критически мыслить и решать проблемы.

Для детей из бедных стран возможность выхода в сеть также означает доступ к образовательным инструментам, хотя и не на таком уровне, который только что был описан. Да, сами школы останутся в ветхих зданиях, учителя будут пренебрегать своими обязанностями, а учебников и канцелярских принадлежностей, как и сейчас, всем не хватит. Но в этом уравнении появится новая переменная — коммуникации, которая даст возможность детям, обладающим мобильными устройствами и доступом в интернет, посещать не только физическую, но и виртуальную школу, пусть последняя и не будет считаться формальным образованием.

В тех странах, где правительство плохо справляется с выполнением даже базовых функций, или в зонах боевых действий простейшие цифровые технологии (например, мобильные телефоны) станут безопасным и недорогим средством дать хоть какое-то образование детям. У тех из них, кто не может ходить в школу из-за ее удаленности, небезопасной обстановки в регионе или невозможности платить за обучение, но имеет доступ к мобильному телефону, все же останется связь с миром знаний. И даже если у ребенка не подключена услуга передачи данных, учиться можно будет при помощи базовых мобильных услуг вроде текстовых сообщений и IVR (интерактивной системы маршрутизации звонков на базе технологии распознавания голоса). Загружая в планшетные компьютеры и мобильные телефоны высококачественные образовательные приложения и развлекательный контент еще до их продажи, можно обеспечить гарантии, что даже «интернет-бедняки», не имеющие надежного доступа в сеть, смогут воспользоваться преимуществами мобильных устройств. А для детей, чьи классы переполнены и испытывают нехватку учителей или чьи национальные стандарты образования недостаточно хороши, связь с миром при помощи мобильных устройств дополнит обучение и поможет раскрыть их потенциал независимо от того, где они родились. Уже сегодня в развивающихся странах запущено множество пилотных проектов, в рамках которых мобильные технологии используются для обучения множеству предметов и привития навыков, в том числе грамоте — как детей, так и взрослых, иностранным языкам и дополнительным университетским курсам. В 2012 году этот подход протестировал в Эфиопии Массачусетский технологический институт:

детям младшего возраста раздавали планшеты с загруженным в них контентом, причем без каких-либо инструкций или объяснений. Результат был поразительным. Через несколько месяцев дети знали алфавит и могли писать целые предложения на английском. Но сегодня, пока доступ в сеть не распространился повсеместно, как это будет в будущем, успех усилий такого рода все же ограничен.

Только вообразите, какие последствия возымеет распространение уже сейчас активно развивающихся образовательных платформ на базе мобильных телефонов или планшетных компьютеров в таких странах, как Афганистан, где уровень грамотности один из самых низких в мире! Такие цифровые платформы как в простом варианте (для мобильных телефонов), так и в более продвинутом онлайн-режиме смогут противостоять ненадежной окружающей среде (политической нестабильности, экономическим спадам, даже плохой погоде) и продолжат выполнять свои функции. Вот почему, несмотря на то что в реальном мире образование для многих останется труднодоступным, значение и надежность виртуального обучения продолжат возрастать. А в странах, где школьная программа очень ограниченна или в значительной степени основана на механическом запоминании, ученики будут иметь доступ к виртуальному миру, поощряющему независимость суждений и критическое мышление.

Повышение качества жизни

Помимо многочисленных «функциональных» улучшений нашей повседневной жизни всеобщий доступ в сеть в будущем обещает нам ослепительный фейерверк «качественных» ее улучшений: укрепится наше здоровье, повысится безопасность, жить станет интереснее. Как и в других случаях, распределение этих благ будет неравномерным, но от этого они не станут менее значимыми.

Все электронные устройства, мониторы и бытовая техника в вашей квартире станут выполнять не только утилитарные функции. Они будут развлекать, отвлекать от забот, обогащать интеллектуально и культурно, расслаблять физически и дарить возможность делиться своими впечатлениями с другими. Главный прогресс будет заключаться в их индивидуализации. Вы сможете подстроить под свои

нужды окружающие вас устройства (все или большую их часть) так, чтобы среда отражала ваши предпочтения. У людей появится более удобный способ вести хронику своей жизни: им не придется больше полагаться на традиционные или онлайн-фотоальбомы, хотя и те и другие по-прежнему будут существовать. Развитие фото- и видеотехники позволит хранить все снятые вами неподвижные или движущиеся изображения в виде трехмерных голограмм. Но еще замечательнее то, что вы сможете сохранить все фотографии, видеоролики и географические координаты в одном устройстве, поставить его на полу в гостиной и мгновенно превратить ее в комнату воспоминаний. Так, молодожены воссоздадут свою свадебную церемонию перед бабушкой и дедушкой, пропустившими ее из-за слабого здоровья.

То, что вы будете смотреть на своих многочисленных мониторах (высококачественных жидкокристаллических дисплеях, голографических проекторах и переносных мобильных устройствах), будет определяться вами, а не программой телепередач. В вашем распоряжении окажется весь мир цифрового контента, постоянно меняющегося, ранжированного и структурированного так, чтобы легко было находить музыку, фильмы, телешоу, книги, журналы, блоги и любые другие произведения искусства на свой вкус. Контроль потребителей над информационными и развлекательными каналами усилится как никогда, поскольку производители контента от ожесточенной защиты своих прав перейдут к более унифицированным и открытым бизнес-моделям, которые смогут обеспечить сохранение своей аудитории. Некое представление о том, как это будет выглядеть, дают современные веб-сервисы вроде Spotify[6], где можно в любое время слушать музыку из огромного каталога с помощью практически любого устройства, бесплатно или за небольшую плату, не нарушая авторские права и обеспечивая доходы правообладателям. Одновременно снижаются традиционные барьеры для создателей контента: уже сегодня YouTube можно назвать местом, где начинается карьера[7] (или обретается мимолетная слава), а завтра еще большее количество платформ будут предлагать художникам, писателям, режиссерам, музыкантам и прочим творческим личностям из любой

страны шанс выйти к широкой аудитории. Для создания качественного контента по-прежнему понадобятся определенные навыки, но станет легче подыскать обладающих такими навыками людей: скажем, мультипликатора из Южной Кореи, актера для озвучивания из Филиппин, сценариста из Мексики, музыканта из Кении — и обеспечить получившемуся произведению такой же потенциальный охват, как у любого голливудского блокбастера.

В будущем индустрия развлечений сможет предложить зрителям более многообразный и персонализированный продукт. По сравнению с интегрированным в него продвижением товаров нынешняя практика скрытой рекламы покажется пассивной и довольно неуклюжей. Если во время просмотра телесериала вам приглянется свитер или понравится блюдо и вы захотите его приготовить, к вашим услугам будет предоставлена любая информация, включая рецепты, подсказки о выборе ингредиентов, а также все остальные факты, связанные с шоу, его сюжетной линией, занятыми в нем актерами и местом действия. Заскучали, хотите взять часовой отпуск? Так почему бы не включить голографическую приставку и не посетить карнавал в Рио? Устали? Отправляйтесь на некоторое время на пляж на Мальдивы. Опасаетесь, что дети становятся слишком избалованными? Пусть погуляют немного по бомбейским трущобам Дхарави. Расстроены тем, что трансляция Олимпиады идет в неудобное время? Купите по умеренной цене голографический абонемент и смотрите, как гимнастки соревнуются прямо перед вами как живые. Благодаря интерфейсам виртуальной реальности и возможностям голографических проекторов вы сможете «включиться» в эти события и чувствовать себя так, как если бы действительно находились там. С реальностью ничто не сравнится, но это будет очень близкое подобие. Во всяком случае гораздо доступнее. Благодаря этим новым технологиям вы сможете получать такие острые ощущения или, наоборот, так расслабляться, как никогда прежде.

Безопасность ваша также вырастет, по крайней мере в пути. До таких потрясающих способов перемещения в пространстве, как сверхзвуковые поезда и суборбитальные космические полеты, далеко, а вот скорое повсеместное распространение автомобилей без водителей уже неизбежно. Несколько беспилотных автомобилей,

разработанных командой инженеров Google и Стэнфордского университета, уже проехали без единой аварии сотни тысяч миль. В недалеком будущем появится множество новых моделей. Ближайший этап — внедрение системы «помощи водителю», то есть возможность включать функцию автоматического вождения, подобную автопилоту авиалайнера. Идею автомобиля без водителя и ее потенциал уже признали власти: в 2012 году в штате Невада стали выдавать лицензии на беспилотные автомобили, позже законность их использования была подтверждена в Калифорнии. Только представьте себе, какие перспективы открываются в секторе дальних грузоперевозок! Вместо того чтобы подвергать испытанию биологические пределы возможностей человека во время тридцатичасовых перегонов, на время отдыха водителя брать на себя основную ответственность за управление и вести автомобиль сможет компьютер.

* * *

Среди всех достижений будущего наиболее значительные успехи ожидаются в здравоохранении и медицине. А благодаря доступу в сеть выиграет большее количество людей, чем когда-либо прежде в истории человечества. Учитывая скорость распространения цифровых технологий и благодаря прорывам в распознавании и лечении болезней, в управлении медицинскими данными и мониторинге личного здоровья миллиарды жителей планеты получат равный доступ к медицинским услугам и информации о здоровье.

> То, что ваш мобильный телефон сумеет поставить диагноз, никого уже не удивит. (*Конечно же*, вы сможете сканировать свои части тела, как сейчас сканируете штрихкоды.) А еще у нас появится возможность провести медицинский осмотр изнутри с помощью специальных устройств (например, микроскопические роботы, находясь в кровеносной системе, будут следить за давлением, фиксировать приближающиеся сердечные приступы и обнаруживать рак на ранней стадии). В искусственный титановый тазобедренный сустав вашего дедушки вставят чип, который будет действовать как шагомер, измерять уровень инсулина в крови и даже вызовет «скорую помощь», если вдруг зафиксирует падение человека. Крошечный имплантат в носу даст вам знать о токсинах в воздухе и начинающейся простуде.

В конечном счете использование этих устройств перестанет вызывать споры, как это случилось с кардиостимуляторами (первый из них был имплантирован в 1950-х годах). Они станут логическим продолжением современных приложений для контроля за персональным здоровьем, позволяющих людям использовать смартфоны для ведения дневника физических упражнений, отслеживания уровня метаболизма и холестерина. И действительно, технология изготовления медицинских устройств для перорального приема уже существует: в 2012 году Управление по контролю за продуктами и лекарствами США одобрило первую электронную таблетку. Она разработана калифорнийской биомедицинской компанией Proteus Digital Health и содержит микроскопический датчик размером один квадратный миллиметр. После проглатывания пациентом и активизации электрической цепи желудочным соком она начинает передавать сигнал на миниатюрный приемник, закрепленный на коже и способный пересылать данные на мобильный телефон. Этот приемник может собирать информацию о реакции пациента на лекарства (проводить мониторинг температуры тела, пульса и других показателей), о регулярности их приема и даже следить за тем, что человек ест. Эта технология значительно облегчит жизнь тем, кто страдает от хронических заболеваний, особенно людям пожилого возраста: она будет автоматически напоминать, что необходимо принять препарат, позволит отслеживать реакцию организма пациента на лекарства и станет персонализированным каналом мгновенной обратной связи с врачом. Возможно, не все захотят скрупулезно отслеживать состояние своего здоровья, не говоря уже о том, чтобы знать в деталях собственное будущее, но, возможно, они согласятся передавать эти данные своему врачу. «Интеллектуальные» таблетки и имплантаты в нос быстро станут доступными и распространенными так же, как витамины и пищевые добавки. В недалеком будущем у нас появится доступ к персональной медицинской системе на базе мобильного устройства, которая автоматически обнаружит «неполадки» в нашем организме при помощи описанных внутренних датчиков, предложит записаться на прием к одному из практикующих в нашем районе врачей, а затем (с нашего согласия) отправит ему всю

необходимую информацию о симптомах заболевания и состоянии здоровья в целом.

Специалисты по тканям смогут выращивать новые органы для того, чтобы заменить состарившиеся или больные, используя синтетические материалы или собственные клетки пациента. Вначале использование этой технологии будет ограничиваться высокой стоимостью. Применяемой сегодня пересадке синтетической кожи придет на смену трансплантация кожи, выращенной из собственных клеток жертв, пострадавших от ожогов. В больницах больше станут полагаться на роботов — хирурги все чаще будут доверять этим умным машинам особенно трудные этапы операций, когда требуется тонкая, утомительная или сложная работа[8].

Провозвестниками эпохи персонализированной медицины станут успехи генетики. Благодаря точечному тестированию и изучению регуляторных последовательностей (и полной расшифровке генома конкретного человека) врачи смогут узнать о пациенте и о том, что ему может помочь, гораздо больше, чем раньше. Ведь, несмотря на заметный научный прогресс, побочные эффекты приема лекарств остаются одними из главных причин госпитализации и смерти людей. Фармацевтические корпорации используют универсальный подход к разработке медикаментов, но постепенно откажутся от него благодаря успехам фармакогенетики. Более качественное генетическое тестирование снизит вероятность возникновения побочных эффектов, повысит шансы пациента на выздоровление и обеспечит врачей и ученых новыми данными для анализа. Появятся лекарства, учитывающие индивидуальную генетическую структуру пациентов, хотя бы (поначалу) и только самых состоятельных. Однако как только стоимость исследования регуляторных последовательностей генома упадет ниже $100 и будет расшифрован почти весь геном, появится возможность выписывать предельно точные рецепты большей части населения планеты.

Жителям развивающихся стран благодаря базовому доступу в сеть и выходу в виртуальный мир удастся значительно повысить качество своей жизни, особенно состояние здоровья. В реальном мире ситуация не изменится: никуда не денутся некачественное медицинское

обслуживание, нехватка вакцин и лекарств, разрушенные системы здравоохранения и прочие внешние факторы, подтачивающие здоровье населения (например, внутренняя миграция, вызванная вооруженными конфликтами). Однако инновационные методы использования мобильных телефонов, особенно частными лицами и неправительственными организациями, выведут систему из состояния стагнации. Это уже происходит. Во всех развивающихся странах идет революция «мобильного здоровья» (сотовые телефоны все чаще используются в качестве средства связи пациентов с врачами, мониторинга системы распределения лекарств и расширения охвата клиник), которая уже улучшила жизнь людей благодаря предпринимателям и некоммерческим организациям, запускающим множество стартапов в области высоких технологий. Сегодня с помощью мобильных телефонов отслеживают поставки медикаментов, проверяют их подлинность, делятся прежде недоступной медицинской информацией, направляют пациентам напоминания о необходимости принять лекарства и прийти на прием к врачу, а также собирают данные о состоянии здоровья населения, что позволяет чиновникам и сотрудникам неправительственных организаций разрабатывать свои программы. Благодаря высоким технологиям удастся хотя бы частично решить главные проблемы здравоохранения в бедных странах (нехватку медицинского персонала, низкое качество обслуживания пациентов в удаленных районах, недостаточное количество лекарств или неэффективное их распределение, низкую информированность населения о вакцинах и профилактике заболеваний).

Пусть мобильные телефоны не могут вылечить болезнь — зато их наличие позволяет людям лучше контролировать свое здоровье. При помощи телефонов мы можем узнать, как снизить риск заболевания или как вести себя на этапе выздоровления. А еще пользоваться их базовыми диагностическими функциями: там нет рентгеновского аппарата, зато есть фотокамера и запись звука. Можно сфотографировать рану или записать кашель и послать эту информацию врачу, после чего пообщаться с ним на расстоянии. Это эффективно, доступно по цене и гарантирует конфиденциальность. Разумеется, такого рода решения на базе цифровых технологий не заменяют нормально функционирующую систему здравоохранения, но

все же помогают организовать контакт со специалистом, на какое-то время обеспечив его данными, и перейти к решению более важных и застарелых проблем.

Верхний сегмент

От доступа в сеть выигрывают все. Те, у кого ничего нет, получат хотя бы что-то, а те, кто имеет многое, будут иметь еще больше. Чтобы продемонстрировать это, перенесемся на несколько десятилетий вперед и предположим, что вы молодой профессионал, живущий в одном из американских городов. Ваше обычное утро будет выглядеть примерно так.

Утреннее пробуждение не будет сопровождаться сигналом будильника, по крайней мере в его традиционном понимании. Вместо него вас разбудит аромат только что сваренного кофе, солнечный свет, ворвавшийся в комнату после того, как раздвинулись автоматические шторы, и нежный массаж спины, который сделает вам ваша высокотехнологичная кровать. Наверняка, проснувшись, вы будете чувствовать себя отдохнувшим, поскольку встроенный в матрас специальный датчик отслеживает ритмы вашего мозга и точно определяет, в какой момент вас можно разбудить, не прервав фазу быстрого сна.

Ваша квартира — настоящий электронный оркестр, которым дирижируете вы. Несколько движений рукой и голосовых команд — и вы отрегулируете температуру и влажность воздуха, включите музыку и свет. Дожидаясь, пока появится вычищенный и выглаженный костюм из автоматического гардероба — судя по электронному календарю, сегодня важная встреча, — вы просматриваете последние новости на полупрозрачных экранах. Затем направляетесь на кухню завтракать, не прекращая смотреть новости, поскольку одно из голографических изображений благодаря датчику движения все время проецируется перед вами, пока вы идете по коридору. Берете чашку кофе, горячую булочку, только что идеально испеченную в вашей печи с функцией контроля влажности, и пробегаете взглядом по новым сообщениям электронной почты на голографическом «планшете», спроецированном прямо перед вами. Центральный компьютер

предлагает вашему вниманию список домашних дел, которыми собираются заняться сегодня роботы, и вы его одобряете. Затем он сообщает, что подходят к концу запасы кофе и что можно совершить удачную покупку — заказать со скидкой большую упаковку, которую он недавно заметил на одной онлайн-распродаже. Возможен другой вариант: попробовать какой-то из сортов кофе, которые нравятся вашим друзьям; их описания также в вашем распоряжении.

Покончив с этим, вы достаете заметки к презентации, которую собираетесь сделать сегодня для важных клиентов из-за рубежа. Все ваши данные, и личные, и рабочие, доступны на всех имеющихся у вас разнообразнейших устройствах, поскольку хранятся в «облаке» — удаленной системе хранения цифровых данных практически безграничной емкости. Вообще у вас несколько взаимозаменяемых компьютеров: один размером с планшетник, второй — примерно как карманные часы, а остальные могут быть гибкими или портативными. И все это очень легкое, невероятно быстро работает и основано на таких процессорах, которые мощнее любых существующих сегодня.

Вы спокойно потягиваете кофе в полной уверенности, что сможете произвести на клиентов нужное впечатление. У вас такое чувство, что вы давно знаете друг друга, хотя никогда не встречались лично, ведь ваши встречи проходят в среде виртуальной реальности. Вы общаетесь с голографическими «аватарами», в точности повторяющими движения и речь клиентов. Их потребности вам совершенно понятны, и не в последнюю очередь благодаря автономным программам-переводчикам, практически мгновенно воспроизводящим сказанное ими на вашем языке. Такого рода виртуальное общение в реальном времени вкупе с возможностью совместно разрабатывать и редактировать документы, а также работать над проектами делает несущественным огромное расстояние, которое вас разделяет.

Перемещаясь по кухне, вы — черт! — пребольно ударяетесь ногой об угол шкафа. Тут же хватаете мобильное устройство и запускаете диагностическое приложение. Внутри устройства есть крошечный микропроцессор, который сканирует ваше тело с помощью субмиллиметровых волн вроде рентгеновских, но с меньшим уровнем радиации. Быстрый анализ показывает, что палец на ноге не сломан,

это просто ушиб. И вы отказываетесь от предложения устройства запросить медицинское заключение у ближайшего доктора.

У вас осталось совсем немного времени до того момента, когда нужно отправляться на работу — естественно, на беспилотном автомобиле. Из вашего календаря ему известно, во сколько вам нужно каждое утро оказаться в офисе, и, учитывая данные о загруженности дорог, за час до выхода из дома он связывается с вами посредством ваших наручных часов и начинает обратный отсчет времени. А сама поездка на работу будет настолько продуктивной или, наоборот, расслабляющей, насколько этого вам захочется.

Перед выходом компьютер напоминает о необходимости купить подарок племяннику — скоро у него день рождения. Вы просматриваете предложенный список идей, автоматически сформированный на основе обезличенных агрегированных данных о пожеланиях других девятилетних мальчиков со схожими интересами, но ни на чем конкретном не останавливаетесь. Затем вспоминаете забавный случай, о котором рассказали вам его родители (забавный для всех, кому за сорок): племянник не понял бытовавшего когда-то оправдания «мою домашнюю работу съела собака», ведь собака не может съесть «облачное» хранилище файлов! Он не застал времена без цифровых учебников и расписаний уроков, размещенных онлайн, и так редко делает задания на бумаге — зато часто пользуется «облачным» хранилищем, — что мысль о возможности «забыть» домашнюю работу и попытаться оправдаться подобным образом кажется ему абсурдной. Вы быстро находите в поисковике собаку-робота и покупаете ее за один клик, добавив пару опций, которые должны понравиться племяннику, например усиленный титановый скелет, чтобы на собаке можно было ездить верхом. Оплачивая покупку, выбираете доставку «точно в срок». Подарок привезут прямо домой к имениннику, причем погрешность времени доставки не превысит пяти минут.

Не выпить ли еще чашечку кофе? Но тактильный будильник («тактильная» технология основана на прикосновениях), встроенный в задник вашего ботинка, уже мягко сжимает вашу ногу — сигнал, что если вы задержитесь, то опоздаете на утреннюю встречу. Возможно, выходя из дома, вы просто захватите яблоко, чтобы съесть его на

заднем сиденье своего беспилотного автомобиля, пока он везет вас на работу.

Если вы относитесь к числу людей с самыми высокими в мире доходами (а это большинство жителей богатых западных стран), то многие из перечисленных технологий окажутся в вашем распоряжении (или в распоряжении ваших знакомых). Вероятно, с какими-то вы уже имели дело. Конечно, кто-то сможет отказаться от автомобилей и летать на работу на беспилотных вертолетах.

* * *

В реальном мире мы по-прежнему будем сталкиваться с трудностями, но экспансия виртуального мира и возможностей, которые он предоставляет нам в онлайне, а также подсоединение к нему дополнительных пяти миллиардов умов означают, что у нас появится больше способов получать информацию и перераспределять ресурсы для их преодоления, пусть решения и не всегда будут идеальными. Между нами сохранятся различия, но широкие возможности для общения помогут сгладить наиболее острые грани.

Успехи телекоммуникаций изменят не только жизнь отдельных людей. То, как сосуществуют друг с другом реальный и виртуальный миры, как они противоборствуют и дополняют друг друга, будет оказывать в ближайшие десятилетия огромное влияние на действия и власти, и общества. И в этом смысле не все новости приятные. В последующих главах мы подробнее рассмотрим, каким образом все: люди, компании, неправительственные организации, правительства — будут справляться с этой новой реальностью существования одновременно в двух мирах и стараться сбалансировать их хорошие и плохие черты. Каждому человеку, каждому государству, каждой организации придется найти собственную формулу, и те, кто сможет лучше ориентироваться в этом многомерном мире, окажутся впереди.

Примечания к главе 1

ГЛАВА 2

Будущее личности, государства и персональных данных

В следующем десятилетии количество виртуальных личностей превысит население Земли. Все мы будем представлены в сети сразу несколькими аккаунтами, а значит, возникнет множество переполняемых энергией сообществ по интересам, которые и отражают, и обогащают реальный мир. В результате образуются огромные массивы информации (уже появился термин «революция данных») и люди получат невиданную раньше власть. И вот здесь необходимо сделать исключительно важное предостережение: в результате этой революции данных мы практически утратим контроль над своей персональной информацией, попадающей в виртуальное пространство, что приведет к серьезным последствиям и в реальном мире. Возможно, это затронет не каждого пользователя, но на макроуровне очень сильно изменит нашу жизнь. Перед нами стоит трудная задача: решить, на что мы готовы пойти для того, чтобы сохранить контроль над личной жизнью и безопасностью.

Сегодня наши виртуальные личности в некоторой степени влияют на наше физическое «я», но пока не доминируют над ним. То, как ведут себя пользователи в социальных сетях, и то, что они пишут, может нравиться или нет, но чаще всего по-настоящему конфиденциальная или личная информация остается скрытой от посторонних глаз. От онлайн-склок и дискредитирующих кампаний страдают в основном заметные общественные фигуры, а не обычные люди. В будущем на нашу личность в реальной жизни все большее влияние станут оказывать наша виртуальная деятельность и контакты в сети. Детально документированное прошлое начнет определять наши перспективы, и мы утратим контроль над тем, как нас воспринимают другие. Одновременно вырастет вероятность несанкционированного

доступа к персональным данным, их кражи или манипулирования ими, в частности благодаря тому, что мы все больше полагаемся на «облачные» хранилища данных. (Говоря упрощенно, «облачные» вычисления проводятся на программном обеспечении, размещенном в интернете, управлять которым пользователь не может. А хранение документов и иного контента «в облаке» означает, что данные находятся на удаленных, а не на локальных серверах или собственном компьютере человека и доступ к ним могут получить разные пользователи и с разных устройств. «Облачные» вычисления ускоряют распространение информации и процесс работы в интернете, поскольку сокращают трафик.) Однако в силу этой уязвимости — и воображаемой, и реальной — технологическим компаниям придется прилагать все больше усилий, чтобы завоевать доверие пользователей в области конфиденциальности и безопасности данных, иначе они столкнутся с оттоком клиентов. Отрасль высоких технологий уже озаботилась поиском новых способов снизить указанные риски, например при помощи двухфакторной идентификации, когда для доступа к своим персональным данным от вас требуется что-то, что вы знаете (предположим, пароль), имеете мобильный телефон или что вам неотъемлемо принадлежит (отпечаток пальца). Не может не радовать то, что над созданием нового поколения таких решений трудятся лучшие в мире инженеры. Как минимум в качестве более надежного, хотя и не идеального выхода будет повсеместно использоваться строгое шифрование. («Шифрованием» называется кодирование информации, при котором декодировать ее может лишь тот, кто прошел верификацию.)

Могут измениться сами основы виртуальной идентификации. Некоторые правительства, решив, что иметь тысячи анонимных, бесконтрольных и непроверенных граждан — «подполье» — слишком рискованно, захотят узнать, кто скрывается за каждым онлайн-аккаунтом, и потребуют верификации на государственном уровне для усиления контроля над виртуальным пространством. В будущем ваша виртуальная личность вряд ли будет ограничена страничкой в Facebook — скорее всего, она станет целым созвездием профилей, созданных вами в интернете, которое будет верифицироваться и даже регулироваться властями. Представьте, что все ваши аккаунты — в

Facebook, Twitter, Skype, Google+, Netflix, подписка на New York Times — привязаны к одному «официальному» профилю. Рейтинг информации, связанной с верифицированными онлайн-профилями, в результатах поиска окажется более высоким по сравнению с контентом без такой верификации, а это, естественно, приведет к тому, что большинство пользователей будут кликать на верхние (верифицированные) результаты. И тогда истинная цена анонимности может стать слишком высокой: даже самый увлекательный контент, созданный владельцем анонимного профиля, просто не будет виден в поисковой выдаче из-за своего чрезвычайно низкого рейтинга.

Переход от ситуации, когда личность формируется офлайн и позднее проецируется в сеть, к созданию онлайн-личности, которая затем воплощается в реальном мире, окажет огромное влияние на граждан, государства и компании. И от того, как удастся решить проблемы конфиденциальности и безопасности личных данных, будут зависеть границы человеческой свободы. На этих страницах мы хотели бы поговорить о том, что всеобщий доступ в сеть будет значить для граждан в будущем, как они им воспользуются и какие последствия это возымеет и для диктатур, и для демократий.

Революция данных

Революция данных принесет жителям планеты колоссальное благо. В частности, они смогут узнать, что думают и как ведут себя другие люди, каких правил придерживаются, почему их нарушают — причем не только соотечественники, но и те, что живут на других континентах. Обретенная способность получать онлайн точную и проверенную информацию по первому требованию на родном языке и в неограниченных количествах будет означать начало эпохи критического мышления в тех сообществах, которые прежде были культурно изолированы от остального мира. В странах с неразвитой инфраструктурой доступ в сеть позволит людям заниматься бизнесом, в том числе онлайн, и взаимодействовать с правительством на совершенно ином уровне.

Это будет означать наступление эры невиданных возможностей. И даже если кто-то попытается сохранить максимум индивидуальности,

дистанцируясь от виртуальной жизни, другие сочтут, что открывающиеся перспективы оправдывают риск, на который приходится идти. Гражданское участие достигнет новых высот: каждый человек, имеющий мобильный телефон и доступ в интернет, сможет внести свой вклад в реализацию идеи подотчетности и прозрачности властей. И лавочник в Аддис-Абебе, и сознательный не по годам подросток в Сан-Сальвадоре станут распространять информацию о случаях вымогательства взяток и коррупции, сообщать о нарушениях избирательного законодательства — в общем, призывать правительство к ответу. А если для того, чтобы полицейские вели себя по закону, недостаточно телефонов с функцией фотосъемки, в полицейских автомобилях можно установить видеокамеры! На самом деле развитие технологий позволит населению контролировать полицию с помощью огромного количества прежде недоступных способов, включая систему мониторинга, предназначенную для формирования рейтинга каждого полицейского в городе, в режиме реального времени. После того как основные общественные институты: системы здравоохранения, образования и судебная система — окончательно вступят в цифровую эру, они станут более эффективными, прозрачными и доступными.

Тем, кто хочет распространять религиозные, культурные и этнические мифы, придется кормить своими выдумками сообщество хорошо информированных слушателей. В распоряжении людей появится больше данных и способов их проверить. И тогда колдун из Малави, занимающийся врачеванием, вдруг столкнется с враждебным отношением к нему со стороны соплеменников, если они найдут в сети информацию, развенчивающую его авторитет, и поверят ей. Или, например, молодые йеменцы, обнаружив, что виртуальное сообщество отрицательно относится к культивируемой в стране традиционной практике женитьбы на маленьких девочках, восстанут против нее, поскольку решат, что она бросает тень на них самих. А последователи индийского «святого» найдут способ проверить его прошлое и отвернутся от него, выяснив, что он их обманывал. Многие опасаются, что в эпоху процветания онлайн-источников у людей может усилиться психологическая склонность искать подтверждение своей позиции (когда, сознательно или нет, они обращают внимание лишь на ту

информацию, которая согласуется с их сложившейся точкой зрения). Однако недавнее исследование ученых из Университета штата Огайо показало, что этот эффект слабее, чем кажется, особенно на американском политическом ландшафте. На самом деле склонность к поиску подтверждений проявляется и когда мы пассивно реагируем на информацию, и когда активно отбираем ее источники. Поэтому, когда миллионы людей выходят в интернет, у нас есть основание с оптимизмом смотреть на будущие социальные изменения.

Властям будет все труднее маневрировать по мере того, как все больше их граждан получают доступ к мобильной связи и интернету. В новую цифровую эру такие репрессивные действия, как уничтожение документов, похищения людей и уничтожение памятников, практически потеряют смысл. Ведь документы можно восстановить и сохранить «в облаке», а давление, которое способно организовать активное глобализированное интернет-сообщество в ответ на беззаконие, заставит власти подумать дважды, прежде чем похищать кого-то или держать в застенках неопределенно долго. Да, некоторые режимы, вроде установленного талибами, по-прежнему смогут уничтожать памятники, как они разрушили бамианские статуи Будды[9]. Но такие памятники можно будет отсканировать с применением самой современной технологии, что позволит сохранить все их углы и закоулки в виртуальной памяти, а затем воссоздать — вручную или при помощи 3D-принтеров — или даже спроецировать в виде голографических изображений. Возможно, Центр всемирного наследия ЮНЕСКО станет использовать такую практику в рамках своей деятельности по реставрации памятников. Старейшую синагогу Сирии, которая сегодня находится в музее Дамаска, можно спроецировать или реконструировать посредством 3D-печати. Активное гражданское общество, которое сегодня имеется в большинстве развитых стран, готовое проверять факты и расследовать действия властей, появится почти везде, причем в значительной степени этому будет способствовать распространение дешевых и мощных мобильных устройств. Как минимум жители всех стран смогут сравнивать себя и свой образ жизни с тем, как живет остальная

часть мира. И в этом контексте варварские или устаревшие обычаи будут выглядеть особенно одиозно.

* * *

В будущем уникальная личность человека окажется его самым ценным активом, и существовать эта личность будет преимущественно в сети. Опыт жизни в режиме онлайн люди станут приобретать с самого рождения, если не ранее. При этом различные периоды человеческой жизни, «замороженные» во времени, будут легкодоступны для всеобщего обозрения. В результате придется создавать новые средства контроля информации, позволив людям самим составлять списки тех, кто может видеть их данные. Используемые нами сегодня технологии связи «инвазивны» по определению: они собирают наши фотографии, комментарии и имена друзей в огромные базы данных, по которым можно проводить поиск и которые в отсутствие внешнего регулирования становятся законной добычей для работодателей, университетских отделов по работе с персоналом и сплетников. Мы то, что мы «твиттим».

В идеале все мы должны сознательно и тщательно управлять своими онлайн-личностями и виртуальными жизнями, отслеживать и корректировать их, чтобы не усложнять свою реальную жизнь, причем с самого раннего возраста. Увы, это невозможно. У детей и подростков желание делиться информацией всегда перевесит смутный отдаленный риск рассказать о себе слишком многое, несмотря на многие примеры негативных последствий. Так что к тому моменту, когда человеку исполнится сорок, в сети сложится повествование о его жизни, очень подробное и включающее все факты и вымыслы, ошибки и победы. И даже слухи будут жить вечно.

В глубоко консервативных обществах, где общественное порицание значит очень многое, мы можем столкнуться со своего рода «виртуальным бесчестием» — сознательными усилиями по дискредитации онлайн-личности человека (путем приписывания ему недостойных поступков и распространения ложной информации или связывания его онлайн-личности с контентом, в котором идет речь о реальном или вымышленном преступлении). Разрушение репутации в

сети может не сопровождаться физическим насилием со стороны злоумышленника, но если, скажем, такого рода обвинения будут предъявлены девушке, ее честь может оказаться запятнанной, причем, к ее несчастью, навсегда — и скрыться в таком случае невозможно. Учитывая публичность позора, все может закончиться ее гибелью от руки одного из родственников.

А что насчет роли родителей? Она нелегка, и это известно всем, у кого есть дети. Появление виртуального мира еще больше усложнило ее, но не стоит считать ситуацию безнадежной. В будущем ответственность родителей не уменьшится, но им придется еще активнее участвовать в жизни своих детей, если они хотят, чтобы те не совершили в сети ошибок, способных навредить их судьбе в реальном мире. А поскольку виртуальное развитие детей значительно опережает их физическое созревание, большинство родителей придут к пониманию того, что самый лучший способ помочь своим отпрыскам — поговорить с ними о необходимости защиты личной информации и соблюдения безопасности в сети даже раньше, чем о вопросах секса. Так что традиционный разговор с детьми по душам не утратит своей роли в их воспитании.

Школьная система тоже изменится и внесет свою лепту в развитие навыков онлайн-осмотрительности. По настоянию родительских ассоциаций наряду с уроками сексуального воспитания в школах появятся уроки защиты личной информации и основ безопасности при работе в интернете. На таких занятиях школьники научатся оптимизировать установки безопасности программ и хорошо усвоят, что можно и чего нельзя делать в виртуальном мире. А учителя будут пугать их историями из реальной жизни о том, что бывает, когда не начинаешь защищать личную информацию и соблюдать безопасность в сети с самого раннего детства.

Конечно же, найдутся родители, которые в попытке обыграть систему начнут действовать еще предприимчивее. Один из примеров — выбор имени будущего ребенка. По мере роста функциональной ценности онлайн-личности роль родителей на начальном этапе жизни детей окажется критически важной. Начинаться все будет с их имен. Стивен Левитт и Стивен Дабнер в книге Freakonomics[10]

проанализировали, насколько популярные в определенных этнических группах имена (в частности, у афроамериканцев) могут предсказывать жизненный успех их владельцев. Дальновидные родители учтут и то, как результаты поисковой выдачи скажутся на будущем их детей. Однако истинно стратегический подход проявится не просто в заблаговременном резервировании аккаунтов социальных сетей и не в покупке соответствующих доменных имен (предположим, www.JohnDavidSmith.com), а в выборе ребенку такого имени, которое облегчит или усложнит процесс его поиска в интернете. Некоторые сознательно выберут уникальные или традиционные, но искаженно написанные имена с тем, чтобы избавить своих детей от прямой конкуренции и облегчить им задачу продвижения в виртуальном мире. Другие, напротив, остановят свой выбор на самых распространенных именах, что обеспечит их детям определенный «щит» от индексации в сети: просто еще одна «Джейн Джонс» среди тысяч подобных записей.

Мы предвидим пышный расцвет отрасли, связанной с защитой персональных данных и репутации. Такой бизнес существует уже сегодня: компании вроде Reputation.com используют различные методы как быстрого реагирования, так и профилактики для того, чтобы удалять из сети нежелательный для их клиентов контент или минимизировать ущерб от его появления[11]. По некоторым сообщениям, в ходе экономического кризиса 2008 года несколько банкиров с Уолл-стрит привлекали компании, специализирующиеся на защите онлайн-репутации, чтобы те минимизировали информацию о них в виртуальном мире. Стоили такие услуги до $10 000 в месяц. В будущем на волне растущего спроса эта отрасль существенно расширится, и услуги репутационных менеджеров станут таким же обычным делом, как брокеров и финансовых консультантов. Нормой для известных и стремящихся к известности людей будет активное управление своим онлайн-имиджем, например, получение от репутационного менеджера ежеквартальных отчетов, фиксирующих его изменение за прошедший период.

Появится новое направление страхования. Вам предложат застраховать свою онлайн-личность от кражи и взлома, ложных обвинений, злоупотреблений и несанкционированного присвоения.

Родители смогут купить страховку от репутационного ущерба, который способны причинить им действия их детей в интернете. А преподаватель, скажем, захочет застраховаться от взлома студентами его профиля в Facebook и размещения на странице оскорбительной и порочащей информации. Страхование от кражи персональных данных уже существует, но в будущем страховые компании смогут предложить своим клиентам защиту и от других злоупотреблений. Такие полисы будут покупать не только те, кому они действительно нужны, но и просто параноидально настроенные люди.

Онлайн-личности возобладают столь высокой ценностью, что их — реальные или придуманные — можно будет купить на черном рынке. В этом будут заинтересованы и обычные люди, и преступники, ведь под чужой маской смогут скрыться как наркоторговцы, так и диссиденты. Такие онлайн-личности, украденные или созданные с нуля, станут продаваться в комплекте со всей необходимой исторической информацией: записями в лог-файлах интернет-провайдеров, фиктивными «френдами» и данными о покупках, то есть всем тем, благодаря чему будут выглядеть правдоподобно. И если полицейский информатор из Мексики захочет избежать мести со стороны наркокартеля, набор таких фальшивых онлайн-личностей наверняка поможет членам его семьи скрыть свое прошлое и начать жизнь с чистого листа.

Естественно, что в цифровую эпоху такой способ побега представляет собой рискованное предприятие: начало новой жизни должно означать полный разрыв всех прежних связей, ведь выдать человека может малейший неверный жест вроде поискового запроса по имени кого-то из родственников. Более того, тому, кто использует фальшивую личность, следует избегать всех мест, где применяется технология распознавания лица, способная связать его со старым аккаунтом человека. Да и сам этот теневой рынок сделок с онлайн-личностями будет неспокойным местом: и покупатель, и продавец остаются анонимными благодаря зашифрованным каналам связи и расчетам в виртуальной валюте, которые очень сложно отследить. Поэтому и посредники, и покупатели столкнутся с теми же рисками, что и сегодняшние участники черного рынка, включая работу правительственных агентов «под прикрытием» и обман в ходе сделок

(вероятность всего этого, скорее всего, даже повысится, учитывая анонимную природу транзакций в виртуальном мире).

* * *

Многие с восторгом отнесутся к отсутствию контроля, что предполагает всеобщий доступ в сеть с неограниченными объемами хранящихся там данных. Люди будут считать, что информация по определению должна быть доступна всем[12] и что еще большая прозрачность сделает мир проще, безопаснее и свободнее. Пока самым заметным евангелистом этой идеи является Джулиан Ассанж[13], но его ценности разделяют, поддерживая созданную им WikiLeaks, люди самых разных убеждений — от правых либертарианцев до крайне левых либералов и аполитичных энтузиастов высоких технологий. И хотя они не всегда согласны друг с другом в вопросах тактики, общей для них является вера в необходимость вечного хранения данных как основы существования общества. По мнению активистов свободного доступа к информации, отсутствие кнопки Delete в конечном счете ускорит движение человечества к полному равенству, производительности и самоопределению, несмотря на некоторые известные негативные последствия такого подхода (угроза индивидуальной безопасности, испорченные репутации и дипломатический хаос). Однако мы убеждены, что это очень опасная модель, особенно если учесть, что всегда найдутся глупцы, готовые по недомыслию поделиться гибельной для многих людей информацией. Вот почему сохранится система государственного регулирования, которая при всем ее несовершенстве по-прежнему будет определять круг лиц, уполномоченных принимать решения о том, какие данные считать секретными, а какие — нет.

Мы встречались с Ассанжем в июне 2011 года, когда он содержался под домашним арестом в Великобритании. Какой бы ни была наша позиция, мы должны учитывать то, к чему могут стремиться активисты, выступающие за полную свободу информации, поэтому мнение Ассанжа является хорошей отправной точкой. Мы не собираемся останавливаться на том, что обсуждается сегодня (этому посвящены многие книги и статьи) и касается в основном западной

реакции на WikiLeaks, содержания обнародованной переписки, степени деструктивности утечек информации и того, какое наказание должны понести причастные к этому люди. Нет, нас интересует будущее и то, что попытаются создать — или разрушить — представители следующего поколения движения за свободу информации, начиная с последователей Ассанжа, но не ограничиваясь ими. В ходе интервью Ассанж поделился с нами двумя своими главными соображениями на эту тему, причем обе посылки связаны друг с другом. Первое: человеческая цивилизация основана на всей совокупности результатов нашей интеллектуальной деятельности, следовательно, правильным является как можно более тщательно фиксировать эти результаты, чтобы обеспечить информацией следующие поколения людей. Второе: поскольку различные лица всегда будут пытаться уничтожить или скрыть часть этой общей истории в своих интересах, цель каждого человека, ценящего истину и стремящегося к ней, — фиксировать как можно больше информации, препятствовать ее уничтожению, а также делать ее максимально доступной для всех жителей планеты.

Ассанж не сражается с секретностью как таковой: по его словам, «есть множество причин, по которым неправительственные организации могут хранить секреты, и, на мой взгляд, это их законное право: они нуждаются в этом, потому что не обладают иной властью». Он борется с секретностью, прикрывающей действия, которые идут вразрез с интересами общества. «Почему правительственные организации стремятся к секретности?» — задает он риторический вопрос. И сам отвечает на него: потому что их планы, стань они известными широкой публике, встретили бы отпор, а секретность помогает им воплотить их. Тот, чьи планы не противоречат интересам общества, не встречает противодействия, и ему нечего скрывать, добавляет он. По словам Ассанжа, в этом противостоянии в конечном счете верх возьмут те, кто обладает реальной поддержкой людей. Так что раскрытие информации «позитивно для организаций, ведущих деятельность, которую поддерживает общество, и негативно для организаций, занятых делами, которые общество не одобряет».

Мы возразили, что в этом случае не желающие огласки организации просто начнут скрывать свою деятельность, но Ассанж выразил

уверенность, что его движение способно этому воспрепятствовать. Он считает, что полная секретность невозможна — серьезные структуры всегда оставляют бумажные следы: «Понимаете, в системную несправедливость обычно вовлечено множество людей». Не у всех из них есть полный доступ ко всем планам, но каждый знает достаточно для того, чтобы выполнять свою работу. «Если перестаешь фиксировать информацию на бумаге, если решишь не оставлять ни электронных, ни бумажных следов, любые институты приходят в упадок, — говорит он. — Вот почему у всех серьезных организаций существует строгая система документирования на бумаге всех решений, в том числе самого высшего руководства». Бумажные следы дают уверенность в том, что команды выполняются должным образом, поэтому, по словам Ассанжа, «если организация настолько “балканизирована” внутри, что утечки невозможны, то это означает резкое снижение ее эффективности». А неэффективность означает слабость.

С другой стороны, Ассанж считает, что открытость может создать проблемы для самих искателей истины: «Открытость затрудняет нам жизнь, поскольку люди начинают скрывать свои плохие поступки, искусственно усложняя систему». В качестве очевидных примеров он привел бюрократическую демагогию и офшорный финансовый сектор. Технически это открытые системы, но по сути своей — непрозрачные: к ним трудно придраться, но еще труднее использовать эффективно. Бороться со сложной, сознательно запутанной, хотя и законной системой, призванной скрывать темные делишки, гораздо труднее, чем с простой цензурой.

К сожалению, такие люди, как Ассанж, и организации вроде WikiLeaks легко смогут воспользоваться возможностями, которые сулят грядущие перемены. И даже тем, кто их поддерживает, не так-то просто дать однозначную оценку применяемых ими методов и последствий прозвучавших разоблачений, особенно если проецировать то, что происходит, в будущее. И здесь одним из самых трудных является вопрос о том, кто будет решать, какую информацию можно обнародовать без купюр, а что нужно хотя бы временно публиковать выборочно? Почему, в частности, именно Джулиан Ассанж определяет, какие материалы представляют собой общественный интерес? И что

будет, если человек, принимающий решения о раскрытии информации, готов смириться с неизбежным вредом, который оно причинит ни в чем не повинным людям? Большинство из нас согласится с тем, что для того, чтобы такие платформы приносили обществу пользу, над ними нужен некоторый контроль, но никто не даст гарантий возможности такого контроля (это подтверждает безжалостность хакеров[14], выкладывающих в сети огромные массивы персональных данных множества людей).

Если решения о раскрытии информации принимаются централизованно, то их должно принимать очень ограниченное количество людей, а людям свойственно иметь предрассудки и отстаивать собственные идеи. И пока этим миром правим мы, представители человеческой расы, а не компьютеры, останется проблема субъективности человеческого суждения независимо от того, насколько прозрачны или технически совершенны используемые нами инструменты.

В будущем на волне все большей доступности интернета можно ожидать всплеск активности платформ, аналогичных WikiLeaks. По мере роста количества пользователей и объемов секретной и конфиденциальной информации появятся десятки более мелких сайтов, стремящихся воспользоваться увеличением спроса и предложения и делающих тайное явным. Мысль убедительная и пугающая, но ошибочная. Рост количества сайтов, публикующих секретные материалы, ограничен естественным образом, в том числе внешними факторами, которые не позволяют успешно сосуществовать множеству аналогичных платформ. Каким бы ни было ваше отношение к WikiLeaks, только подумайте о том, как много факторов способствовали ее превращению в глобальный бренд: несколько крупномасштабных утечек мирового значения, способных привлечь внимание международной общественности; стабильная публикация информации, что доказывает приверженность организации своим идеям, вызывает общественное доверие и стимулирует новых информаторов, показывая им, что WikiLeaks способна их защитить; харизматическая фигура лидера, олицетворяющая организацию и служащая ее «детонатором» (так называет себя Ассанж); постоянное

обнародование новых утечек, часто большими блоками, что позволяет организации оставаться на виду; а также, что немаловажно, распределенная и технически совершенная цифровая платформа для работы с рассекреченными документами, которой пользуются информаторы, сотрудники организации и посетители (при этом оставаясь анонимными) и которая благополучно обходит попытки ее блокировки властями множества стран. Такую сложную и гибкую систему построить непросто и в силу технических проблем, и из-за того, что ценность одних ее компонентов напрямую зависит от остальных (кому нужна продвинутая платформа без мотивированных информаторов или огромный массив секретных данных без системы их непрерывной обработки и распространения?). WikiLeaks потребовались годы на то, чтобы сбалансировать общественный интерес, энтузиазм информаторов и техническую защищенность системы, и поэтому сложно вообразить, что в будущем какие-то вновь созданные, отпочковавшиеся или конкурирующие команды смогут создать аналогичную платформу и выстроить схожий по силе бренд быстрее, чем это удалось сделать Ассанжу, особенно учитывая то, что сейчас все правительства хорошо понимают угрозу, исходящую от таких организаций.

Однако даже если кому-то и удастся запустить конкурирующие сайты, одновременно сможет существовать лишь горстка подобных платформ. На это есть несколько причин. Во-первых, для успеха даже самым «сочным» утечкам требуется последующая «раскрутка» в СМИ. А если сайтов, на которых публикуется рассекреченная информация, станет слишком много, СМИ не смогут уследить за всеми существующими платформами и публикуемыми материалами, да и уровень доверия к ним упадет. Во-вторых, информаторы предпочтут организации, которые, по их мнению, с одной стороны, обеспечат максимальное общественное внимание к их информации, а с другой — максимальную защиту. Новые сайты будут конкурировать за информаторов, обещая им еще большую известность и лучшую защиту, но очевидно, что потенциальный источник информации скорее последует примеру своих успешных предшественников и воспользуется той же платформой. С какой стати ему рисковать представившимся шансом и самой жизнью, полагаясь на

непроверенный сайт? А те организации, которые не смогут стабильно предлагать миру качественные утечки информации, лишатся общественного интереса и финансирования, в результате чего медленно, но верно захиреют. Ассанж считает, что для его организации это вполне благоприятная ситуация и что доверие к WikiLeaks точно позволит ей продолжать свою деятельность. «Информаторы голосуют ногами, — заметил он, — рынок дисциплинировал нас».

Судьба сайтов, специализирующихся на публикации секретных материалов, будет сильно зависеть от того, на какие регионы они ориентированы. На Западе и правительственные структуры, и корпорации в большинстве своем хорошо представляют себе риски, связанные с недостаточной степенью безопасности компьютерных систем. В их системы и так невозможно проникнуть, однако и в государственный, и в частный секторы по-прежнему инвестируются значительные ресурсы для еще более качественной защиты записей, пользовательских данных и инфраструктуры. О большинстве развивающихся стран такого не скажешь, и, поскольку можно ожидать, что в ближайшие десять лет их население получит доступ в интернет, многие государства столкнутся со своей версией WikiLeaks: там появятся информаторы, имеющие доступ к цифровым данным и готовые организовать их утечку в политических целях. Последующие за этим бури, пусть и ограниченные одной страной или регионом, будут иметь для них разрушительные последствия. И даже могут привести к революции. Следует ожидать, что для борьбы с такими сайтами власти станут применять похожие методы (даже если сами организации и их серверы расположены за пределами страны): фильтрация, прямые атаки, финансовая блокада и судебное преследование.

В конце концов технологии, используемые при создании таких платформ, станут настолько совершенными, что блокировать их будет практически невозможно. Когда в 2010 году WikiLeaks в результате DDoS-атак и давления провайдера, предоставлявшего хостинг, утратила контроль над своим основным сайтом WikiLeaks.org, сторонники организации немедленно создали свыше тысячи зеркальных сайтов (копий оригинального сайта, расположенных в разных местах) с такими адресами, как WikiLeaks.fi (в Финляндии),

WikiLeaks.ca (в Канаде) и WikiLeaks.info. В ходе DDoS-атак — атак типа «отказ в обслуживании» — к сайту-мишени обращается одновременно большое количество зараженных компьютеров, засыпая его информационными запросами и приводя к перегрузке системы, в результате чего сайт перестает обслуживать обычных пользователей. WikiLeaks изначально проектировалась как распределенная система: ее деятельность не концентрируется в рамках одного хаба, а распределяется между множеством различных компьютеров, так что отключить такую платформу значительно труднее, чем представляется большинству дилетантов. В будущем организации, специализирующиеся на публикации секретных материалов, наверняка пойдут гораздо дальше создания сайтов-зеркал (простых копий существующих сайтов) и станут использовать новые методы для репликации и сокрытия своих операций, чтобы защититься от действий властей. Одним из инструментов может быть такая система хранения, в рамках которой в различных местах находится множество копий фрагментов файлов. В случае уничтожения какой-то директории с информацией файлы можно будет собрать заново из этих фрагментов. Создатели подобных платформ придумают новые способы сохранения анонимности потенциальных информаторов: WikiLeaks, к слову, постоянно совершенствует методы передачи информации и призывает не пользоваться устаревшими криптографическими инструментами, как только выясняется их уязвимость (допустим, протоколом SSL и скрытыми сервисами Tor), а переходить на Tor-сеть с высоким уровнем шифрования.

А что можно сказать о лидерах этого движения? В будущем появятся новые «ассанжи», но сторонников у них будет по-прежнему не очень много. Наибольшую пользу принесут те, кто последует примеру людей вроде Алексея Навального, блогера и борца с коррупцией из России, пользующегося большой симпатией на Западе.

> Разочаровавшись в российских оппозиционных партиях, этот специализирующийся на недвижимости юрист начал вести собственный блог, посвященный разоблачению коррупции в крупнейших компаниях России. Поначалу он получал материалы, покупая небольшие пакеты акций этих компаний и используя права акционера на получение информации об их деятельности. Позднее он стал применять краудсорсинг и предложил своим

сторонникам использовать те же методы, причем небезуспешно. В конечном счете его блог превратился в полноценную платформу по публикации секретных материалов, посетители которой могут делать пожертвования на ведение ее операционной деятельности посредством PayPal. Известность Навального росла по мере того, как пополнялась коллекция его разоблачений, в частности после обнародования им в 2010 году документов о злоупотреблениях в государственной компании «Транснефть», операторе магистральных нефтепроводов, на сумму $4 млрд. К концу 2011 года благодаря своей популярности Навальный оказался в эпицентре общественных протестов, связанных с выборами, а придуманное им прозвище для возглавляемой Владимиром Путиным партии «Единая Россия» — «Партия жуликов и воров» — мгновенно разнеслось по стране.

Характерно, что при всей своей принципиальности Навальный не использовал в качестве мишени самого Путина, по крайней мере поначалу. Его целью были преимущественно коммерческие организации, хотя, учитывая, что в России частный и государственный сектор разделить непросто, опубликованная информация нередко затрагивала и некоторых чиновников. Более того, несмотря на оказываемое на него давление — Навального задерживали, помещали под арест, устраивали за ним слежку, возбуждали уголовные дела, — он все эти годы остается на свободе. Критики могут называть его лгуном, лицемером или марионеткой ЦРУ, тем не менее Навальный не уезжает из России (в отличие от многих других известных оппонентов Кремля), а блог его продолжает работать.

Некоторые наблюдатели считают, что Навальный не представляет особой угрозы режиму: знают о нем в стране по-прежнему мало, хотя его сторонники объясняют это тем, что невысокие цифры поддержки скорее отражают факт недостаточного распространения интернета и наличие жесткой цензуры в государственных СМИ (Навального запрещено показывать на федеральных телеканалах). Но есть более интересная точка зрения: Навальный, по крайней мере какое-то время, ухитрялся не выходить за рамки борьбы с коррупцией и четко знал, какие — и чьи — секреты раскрывать, а какие — нет. В отличие от других известных критиков Путина, вроде отбывающего тюремный срок миллиардера Михаила Ходорковского и находившегося в добровольном изгнании олигарха Бориса Березовского, Алексей Навальный, похоже, нашел способ бросить вызов Кремлю, борясь с

коррупцией, но не заходя на слишком чувствительную для режима территорию, что могло бы быть для него смертельно опасным. (За исключением плохо смонтированной фотографии, появившейся в прокремлевских СМИ, на которой Навальный, смеясь, беседует с Березовским, нет никаких свидетельств об их связи.) Кажется, что до июля 2012 года власть терпела его, но затем использовала для его дискредитации все возможные средства, предъявив Алексею официальные обвинения в злоупотреблениях, связанных с продажей принадлежавших государственной компании лесоматериалов в бытность его советником губернатора Кировской области. Эти обвинения в преступлении, максимальное наказание за которое — десять лет тюремного заключения, отражают угрозу, которую несут для режима непрекращающиеся антиправительственные протесты. Мир продолжает следить за судьбами таких фигур, как Навальный, чтобы понять, поможет ли его подход обеспечить цифровым активистам защиту от давления властей.

Однако существует опасная возможность появления сайтов, созданных людьми, которые скопируют внешний вид и устройство известных платформ для публикации секретных материалов, но не будут разделять их мотивы. И тогда вместо убежища для информаторов они станут местом хранения и распространения всевозможного ворованного контента: информации о ведущихся военных операциях, взломанных банковских счетах, украденных паролей и домашних адресов, — не связанного никакой особенной идеей, кроме идеи анархии. И такими сайтами будут управлять не идеологические или политические активисты, а агенты хаоса. Пока хакеры и прочие информационные преступники публикуют свою незаконно полученную добычу совершенно бессистемно: например, в 2011 году с одного из торрентов все желающие могли загрузить себе персональные данные 150 тысяч пользователей Sony, украденные хакерской группировкой LulzSec. Однако если появится централизованная платформа, сравнимая по безопасности и известности с WikiLeaks, это может стать настоящей проблемой. Очевидно, что на таких сайтах информация будет размещаться бесконтрольно, никто не станет заниматься ее редактированием и проверкой, а также обеспечением безопасности информаторов, в

отличие от WikiLeaks и его медиапартнеров (Ассанж сказал нам, что на самом деле редактирует материалы лишь для того, чтобы снизить международное давление на организацию, которое ставит ее в трудное финансовое положение, и что предпочел бы вовсе не заниматься этим). Необдуманная публикация некоторых секретных данных вполне может привести к гибели людей. Компьютерные преступники почти наверняка будут организовывать масштабные утечки, чтобы вызвать наибольший ущерб. Выбор и обнародование определенной секретной информации отражает конкретную цель того, кто это делает, а размещение ее без разбора — пренебрежение к чужим секретам в целом.

Большое значение имеет и контекст. Насколько иной была бы реакция, в частности, западных политических лидеров, если бы на сайте WikiLeaks публиковались похищенные секретные материалы таких режимов, как венесуэльский, северокорейский или иранский? А если бы Брэдли Мэннинг (считается, что он предоставил WikiLeaks американские военные и дипломатические документы) был пограничником из Северной Кореи или дезертиром иранского «Корпуса стражей исламской революции», насколько иначе относились бы к нему политики и правоохранительные органы США? Появись сайты, посвященные разоблачению злоупотреблений в *тех* странах, тон властной элиты Запада, конечно же, был бы иным. Принимая во внимание прецедент, установленный президентом Бараком Обамой во время его первого срока — явную «нулевую терпимость» к несанкционированным утечкам секретной информации, допущенным официальными лицами американской администрации, — следует ожидать, что в будущем правительства западных стран придут к двойным стандартам в отношении раскрытия информации в электронных СМИ, поощряя такие действия за рубежом в отношении враждебных стран и яростно борясь с ними у себя дома.

Кризис средств массовой информации

В будущем на нашу жизнь будет сильно влиять то, какими источниками информации мы пользуемся и каким доверяем. Содержание новостей в интернет-эпоху по-прежнему останется

ключевым фактором успеха; кроме того, продолжится борьба за монетизацию и синдикацию контента, которую мы наблюдаем сегодня. Но как изменится привычный медиапейзаж в результате развития технологии, понижающего входные барьеры во всех отраслях экономики?

Абсолютно ясно, что ведущие мировые СМИ будут все чаще уступать в скорости сообщения новостей. Такие организации в эру всеобщего доступа в сеть просто не в состоянии угнаться за интернетом, и неважно, насколько талантливы их журналисты и корреспонденты и сколько у них источников. Основные мировые новости можно будет узнать в первую очередь благодаря таким платформам, как Twitter: открытым сетям, позволяющим распространять информацию мгновенно, глобально и очень просто. Когда у каждого человека на планете появится телефон с функцией передачи данных или доступ к нему — а это не столь отдаленное будущее, — тогда возможность сообщить миру «горячую новость» будет зависеть от везения и случая, что подтверждает пример одного жителя Абботтабада, ставшего известным после своих твитов, в которых он в режиме реального времени сообщил об операции по уничтожению Усамы бен Ладена[15].

В конечном счете этот лаг между событием и моментом, когда о нем узнают традиционные СМИ, приведет к снижению лояльности их аудитории, поскольку читатели и зрители стремятся иметь более оперативные способы получения информации. Каждое следующее поколение землян будет производить и потреблять больше новостей, чем предыдущее, так что люди перестанут пользоваться средствами массовой информации, отстающими от жизни. Такие СМИ смогут удержать свою аудиторию только за счет анализа и прогноза, а также, что еще важнее, доверия к ним. Их аудитория будет доверять полученной информации, точности анализа и умению правильно расставлять приоритеты при отборе новостей. Иными словами, некоторые люди будут, с одной стороны, лояльны к новым платформам за скорость сообщения новостей, а с другой — к традиционным средствам массовой информации за последующую их трактовку.

Новостные СМИ сохранят за собой важную роль во многих аспектах жизни общества, но некоторые из них перестанут существовать в нынешнем виде, а выжившие изменят свои цели, методы и организационную структуру для того, чтобы лучше отвечать требованиям новой глобальной аудитории. По мере исчезновения языковых барьеров и повсеместного строительства вышек сотовой связи появятся новые авторы, потенциальные источники информации, гражданские журналисты и фотографы-любители, готовые внести свой вклад в массмедиа. И это кстати: на фоне сворачивания деятельности множества новостных СМИ, особенно на международной арене, свежие голоса окажутся востребованными. Выиграет и аудитория, которая получит доступ к большему диапазону мнений и точек зрения. Появление огромного количества новых действующих лиц, объединившихся вокруг различных онлайн-платформ в огромную хаотичную медиасистему, приведет к тому, что крупнейшие традиционные СМИ будут не столько сообщать, сколько подтверждать новости.

При этом обязанности сообщать новости будут распределены намного шире, чем сейчас, что означает покрытие большего количества тем, но, возможно, с более низким качеством. Трансформируется роль традиционных: они станут в первую очередь собирать, хранить и проверять информацию, превратившись в своеобразный фильтр доверия, просеивающий все материалы и помечающий то, чему можно верить, а чему — нет, что стоит, а что не стоит читать и обдумывать. Такая проверка, а также способность убедительно анализировать происходящее критически важна представителям элиты — руководителям компаний, политикам и интеллектуалам, полагающимся на устоявшиеся, мощные СМИ. Элита может отдать предпочтение как раз *им* вследствие массового появления в сети низкокачественных новостей и непроверенной информации. В твиттере шансы наткнуться на глубокий анализ не выше, чем у обезьяны набрать на пишущей машинке собрание сочинений Шекспира (хотя они и повышаются в случае обмена твитами двух умных, авторитетных собеседников), но сила открытых, никем не регулируемых платформ для обмена информацией

заключается в их скорости реагирования на события, а не в глубине или проницательности анализа.

Трудной задачей, которую придется решать традиционным СМИ, явится интеграция всех новых голосов из всех уголков планеты. В идеале журналисты должны будут не столько сами находить информацию, сколько сотрудничать с ее источниками: например, в статье о наводнении в Бангкоке нужно не просто процитировать представителя таиландской компании — оператора речных круизов, но и дать ссылку на собственный новостной блог или Twitter этого человека. Естественно, при включении в материалы информации от необученных новичков повышается вероятность ошибок, поэтому многие уважаемые журналисты сегодня считают, что такое поощрение непрофессиональных репортеров гибельно для профессии. И эти опасения не назовешь беспочвенными.

Благодаря глобальному распространению интернета в цепочке формирования контента добавятся новые звенья. Одним из них станет сеть местных специалистов-шифровальщиков, имеющих дело исключительно с ключами для шифрования данных. И хотя они не являются источниками информации и не создают контент, их ценность для журналистов будет заключаться в создании необходимых механизмов конфиденциального общения сторон. Ведь диссиденты в странах с репрессивными режимами, таких как нынешние Беларусь и Зимбабве, всегда с большей готовностью делятся своими историями, если знают, что могут сделать это анонимно и безопасно. Потенциально такую технологию могут предложить многие, но местные независимые специалисты по шифрованию особенно ценятся. Это происходит уже сегодня: мы видим, что на Ближнем Востоке наряду с другими запрещенными товарами большим успехом пользуются услуги операторов виртуальных частных сетей (VPN), которые предлагают защищенный доступ диссидентам и группам бунтарски настроенной молодежи. Средства массовой информации будут полагаться на эти сети и специалистов по шифрованию данных, как полагаются сейчас при подготовке новостных материалов на независимых корреспондентов — стрингеров.

Что касается самих стрингеров, то в будущем появится новый их подвид. Сейчас это, как правило, малоизвестный журналист из другой

страны, часто с нестабильной внутриполитической ситуацией, которому газета платит за репортажи с места событий. Нередко стрингер рискует жизнью, чтобы получить доступ к определенным источникам или оказаться в опасном месте, куда профессиональный журналист иногда не может или не хочет ехать. Может возникнуть отдельная категория стрингеров, имеющих дело исключительно с цифровым контентом и онлайн-источниками информации. Вместо того чтобы подвергать себя опасности в реальном мире, они, пользуясь глобальным распространением интернета, будут получать материалы от источников, с которыми знакомы только заочно. То есть они, как и сегодня, выступят посредниками между журналистами и источниками информации. Однако, учитывая увеличение дистанции и повышение вероятности путаницы, характерных для виртуального мира, СМИ придется уделять еще большее внимание качеству переработки текста, а также проверке сведений и этической стороны репортажей.

> Представьте себе, что известные актеры решают создать собственный новостной онлайн-портал, посвященный некоему взволновавшему их по тем или иным причинам этническому конфликту. Возможно, они считают, что традиционные СМИ недостаточно активно или не вполне объективно освещают его. И вот принято решение избавиться от привычных посредников и начать информировать общество напрямую, организовав, скажем, новостное агентство «Бранжелина Ньюс». Актеры направляют собственных корреспондентов для работы непосредственно в зоне конфликта и ежедневно публикуют посредством онлайн-платформы полученную от них информацию, которую сотрудники редакции облекают в форму новостей. Издержки такого агентства будут низкими — существенно ниже, чем у его традиционных крупных конкурентов: возможно, стрингерам и журналистам даже не понадобится платить — кому-то достаточно шанса получить известность. И вот за короткое время «Бранжелина Ньюс» становится главным источником информации и новостей об этом конфликте: во-первых, благодаря публичности его владельцев, а во-вторых, потому что своей работой заслужило доверие и воспринимается аудиторией вполне серьезно.

В будущем традиционные СМИ столкнутся с такого рода соперничеством, а не только с конкурентами в лице непрофессионалов, пишущих в Twitter и в собственные блоги, и это будет означать заметное усложнение медийной среды. Конечно, как мы уже отметили, многие люди отдадут предпочтение давно существующим агентствам новостей в силу привычки или веры в

устоявшиеся институты, и серьезная работа — журналистские расследования, интервью с высокопоставленными людьми, анализ сложных событий с учетом широкого контекста, — как и раньше, останется уделом традиционных средств массовой информации. Для остальных диверсификация источников информации предоставит возможность выбора между серьезными СМИ и изданиями, созданными «знаменитостями». Учитывая, по всей видимости, непреодолимую любовь жителей многих стран (США, Великобритании, да и других) к таблоидам, многие потребители, скорее всего, предпочтут новости от своих кумиров. То есть причиной популярности таких изданий будет не последовательность позиции и не качество контента, а «звездный» статус их владельцев.

И точно так же, как это уже происходит с благотворительными фондами и бизнес-проектами, известные люди начнут создавать собственные средства массовой информации в качестве логичного «расширения» собственного бренда. (Здесь мы пользуемся термином «известные люди» в максимально широком смысле, имея в виду заметные, публичные фигуры, а сегодня это может быть кто угодно — от звезд телевизионных реалити-шоу до популярных проповедников.) Конечно же, некоторые новые СМИ будут честной попыткой внести свой вклад в общественный дискурс, но многие окажутся скучным и практически лишенным содержания проектом с целью продвижения собственной персоны или получения коммерческой выгоды.

Мы застанем времена, когда новостные порталы известных людей будут привлекать толпы посетителей по причине их новизны или моды. И эту аудиторию не смутит тот факт, что содержание ресурса окажется несравнимо хуже, а профессионализм его авторов — ниже, чем в традиционных СМИ. Критики станут ругать происходящие изменения и оплакивать смерть журналистики. Но не стоит спешить: если меняется аудитория, то должны перераспределяться и источники ее информирования. Люди сами разочаруются в СМИ знаменитостей из-за недостаточного количества новостей или постоянных ошибок журналистов. В случае средств массовой информации лояльность аудитории — вещь непостоянная, и чем сильнее становится конкуренция, тем заметнее это проявляется. А если доверия читателей и зрителей лишится достаточно большое количество подобных новых

СМИ, это приведет к оттоку их аудитории в пользу профессиональных новостных ресурсов, которым, однако, тоже предстоит пережить трансформацию (обеспечить сбор новостей, расширить диапазон тем, сократить время реагирования на события). Не все ушедшие вернутся обратно, да и изначально не все недовольные традиционными СМИ отвергнут их и переключатся на новые модные платформы. В общем, посмотрим, насколько новые средства массовой информации, созданные известными людьми, изменят облик журналистики в долгосрочной перспективе, а вот их появление и участие в привлечении читателей, зрителей и рекламодателей, вне всякого сомнения, вызовет много шума.

* * *

Распространение интернета означает не только новые вызовы существующим СМИ, но и новые возможности прессы в целом, особенно в тех странах, где сейчас ее не назовешь свободной. Одна из причин, по которой коррумпированные чиновники, могущественные представители преступного мира и прочие темные силы могут продолжать преступать закон без страха наказания, заключается в том, что они контролируют местные информационные ресурсы: или непосредственно — в качестве владельца или издателя, или косвенно — посредством давления, подкупа, запугивания или насилия. Это касается и тех стран, где значительная доля СМИ принадлежит государству, как в России, и тех, где власть над огромными территориями удерживают криминальные синдикаты, как в Мексике. В результате недостаточной независимости журналистов растет безнаказанность преступников и снижается вероятность того, что широкая огласка приведет к давлению на политиков и заставит их принять меры к пресечению и расследованию незаконных действий.

Всеобщий доступ в сеть может сдвинуть баланс в пользу общества по многим причинам, и одной из наиболее интересных является возможность цифрового шифрования данных, расширяющего возможности подпольных или нелояльных режиму средств массовой информации. Возьмем международную некоммерческую организацию (НКО), миссия которой заключается в конфиденциальном сборе

информации в местах, труднодоступных или опасных для журналистов. Что сегодня отличает такие организации от других, скажем, от групп наблюдателей или негосударственных медийных ресурсов, так это использование шифрования в их платформах. Принцип работы таких платформ оригинален, но довольно прост. Чтобы сохранить имена журналистов в тайне (а именно они всегда рискуют больше других), каждому репортеру информационного агентства в системе присваивается уникальный код. Код скрывает их имена, номера мобильных телефонов и прочие идентификационные данные, при этом получить доступ к расшифрованным данным могут только ключевые сотрудники в штаб-квартире НКО, которая, что очень важно, располагается за пределами страны. А в самой стране корреспондентов знают только по их уникальному коду, который используется и для отправки репортажей, и при взаимодействии с источниками информации и местными редакторами. Скажем, если кто-то из корреспондентов сообщит о нарушениях на выборах в Венесуэле (а таких сообщений в ходе президентских выборов в октябре 2012 года было много, хотя и не анонимных), подручные президента, ответственные за выполнение «грязной» работы, не смогут его «вычислить», не имея доступа к его персональным данным: даже редакторы не знают, кто он на самом деле. При этом корпункты как таковые в стране также отсутствуют, чтобы не оказаться мишенью. Конечно, изначально СМИ придется проверять своих репортеров, но после того, как журналист получит доступ к системе, его «прикрепляют» к новому редактору (незнакомому с ним), а его персональные данные надежно скрываются во внутренних файлах платформы.

Так что НКО, находящаяся за пределами страны, будет управлять работой своей информационной платформы на безопасном расстоянии, позволяя различным ее пользователям без опаски взаимодействовать под покровом секретности. Сама по себе идея относиться к журналистам так же, как к источникам конфиденциальной информации (защищая их персональные данные и содержание материалов), не нова, но только сегодня становится возможным шифровать то, что позволяет их идентифицировать, и использовать онлайн-платформы для организации анонимного сбора новостей.

Присылаемые журналистами статьи и другие важные материалы лучше хранить на серверах, расположенных в тех странах, где данные находятся под надежной защитой закона: так меньше риска. Вначале НКО может создать бесплатную платформу и предоставлять ее различным новостным ресурсам, которые получают финансирование из независимых источников. А затем объединить все в одну суперплатформу, представляющую «засекреченных» журналистов со всего мира. Мы не являемся сторонниками усилившейся в последнее время тенденции в сторону анонимности, но считаем, что если безопасность под угрозой, а режим репрессивный, то анонимность становится вынужденной мерой, актом отчаяния. Тогда редактор в Нью-Йорке сможет войти в систему под своим логином и паролем, задать поиск по журналистам из Украины и найти кого-то подходящего с длинной историей публикаций и даже рекомендациями от своих коллег, работавших с ним раньше. После чего редактор, даже не зная настоящего имени журналиста и полагаясь исключительно на качество его прежних статей и доверие к платформе в целом, сможет решить, стоит ли начинать сотрудничать с этим человеком. А затем сделать зашифрованный звонок посредством все той же платформы, чтобы познакомиться и пообщаться с ним.

Создать и поддерживать такого рода распределенную, взаимно анонимную систему сбора новостей будет совсем нетрудно, а благодаря шифрованию персональных данных корреспондентов (да и их редакторов) и хранению репортажей на удаленных серверах к ним не дотянутся руки тех, кто выступает против независимой журналистики. Что сделают они с цифровой платформой, особенно в эпоху, когда у любого человека есть доступ к новостям прямо с мобильного устройства? Конечно, пока доступ в сеть там, где сегодня отсутствуют свободные СМИ, затруднен, но по мере изменения ситуации местные журналисты смогут сообщать о происходящих в их странах событиях все более широкой аудитории — по сути, выйти на международный уровень. Таким образом, две эти тенденции — повышение безопасности для тех, кто пишет репортажи, за счет шифрования данных и рост их аудитории за счет повсеместного доступа в сеть — дают уверенность в том, что, даже если судебная система страны слишком коррумпирована или слаба для того, чтобы

должным образом наказать нарушителей закона, их можно публично обвинить в преступлениях в онлайн-СМИ. Возможно, не всех полевых командиров из Восточного Конго удастся предать Международному уголовному суду, но их жизнь осложнится, если каждый их шаг будет фиксироваться независимыми анонимными журналистами, а статьи об их преступлениях станут разлетаться по всему интернету. Как минимум их потенциальных сообщников отпугнет такая «цифровая радиоактивность»: если человек слишком заметен и находится под пристальным наблюдением общественности, он не может считаться надежным партнером по преступному «бизнесу».

Тайна частной жизни: каждый понимает ее по-своему

Обязанности по защите конфиденциальных данных и охране тайны частной жизни лежат на всех: на самих пользователях, на бизнесе и на общественных институтах. Предполагается, что такие компании, как Google, Apple, Amazon и Facebook, будут оберегать данные, защищать свои информационные системы от взлома и обеспечивать пользователей наиболее эффективными средствами для максимально полного контроля над сохранением тайны их частной жизни и личной безопасностью. Но то, как применять эти средства, зависит лишь от самих пользователей. Желая упростить себе жизнь, мы подвергаемся риску утечки конфиденциальной информации, а ведь ее объемы растут ежедневно. И не стоит полагаться на клавишу Delete! Возможность «удалить» данные — не более чем иллюзия: удаленные файлы, сообщения электронной почты и текстовые сообщения легко восстанавливаются. Очень редко данные стираются из физической памяти компьютера: как правило, операционная система лишь удаляет файл из списка во внутренней директории, сохраняя при этом его содержимое до тех пор, пока эта область памяти не понадобится для других нужд. (И даже после того, как на это место записывается новая информация, фрагменты содержимого старого файла все же иногда можно восстановить в силу специфических свойств магнитного носителя. Специалисты-компьютерщики называют это «сохранностью данных вследствие остаточной намагниченности».) «Облачные» вычисления лишь усугубляют проблему невозможности удаления

данных, поскольку это еще один уровень хранения информации пользователей.

Такие механизмы сохранения данных были разработаны для того, чтобы уберечь нас от нашей собственной беспечности при работе на компьютере. В дальнейшем люди будут все больше доверять «облачным» хранилищам информации (примерно как банкоматам) по сравнению с физическими устройствами, полагаясь на специализированные компании в деле хранения самых важных и конфиденциальных данных, ведь это позволяет избежать риска поломки жестких дисков, кражи компьютера или случайного уничтожения документов. Благодаря многоуровневой системе резервирования работа с информацией онлайн станет эффективнее и производительнее, не говоря уже о меньшей эмоциональной нагрузке на пользователей.

Практически вечное хранение данных окажет огромное влияние на поведение людей в виртуальном мире. Все, что мы делаем и с кем общаемся в сети, так или иначе регистрируется, а вся информация остается в ней навечно. Следовательно, всегда есть вероятность того, что чья-то персональная информация станет общедоступной — или по ошибке, или в результате преступления. Ответственность за свое виртуальное общение и в прошлом, и в настоящем люди будут нести сами, а это означает больший риск практически для каждого, ведь сеть онлайн-контактов, как правило, шире и разнообразнее, чем связи в реальном мире. И хорошие, и плохие поступки наших знакомых как-то влияют на нашу жизнь — или позитивно, или негативно. (И не надейтесь, что достаточно изменить настройки безопасности в социальных сетях.)

Следующее поколение людей будет первым, которое оставит «несмываемые» следы. Коллеги Ричарда Никсона вполне могли бы стереть восемнадцать с половиной минут магнитофонной записи, касающейся Уотергейта[16], и скрыться от возмездия. А вот сегодня в соответствии с законом «О переписке президента» президент США имеет дело с постоянной фиксацией даже всех отправленных с его BlackBerry сообщений электронной почты, которые затем становятся достоянием общественности.

Поскольку любая информация «рвется на свободу», не стоит писать того, что, как говорится, вы не хотите услышать из уст прокурора в суде или увидеть на первых полосах газет. В будущем сфера применения этого совета значительно расширится: речь пойдет не только о том, что вы говорите и пишете, но и о сайтах, которые посещаете, о том, кого включаете в свои круги в соцсетях, какими материалами делитесь, а также о том, что делают, говорят и чем делятся те, с кем вы связаны.

Люди будут озабочены проблемой сохранности их персональных данных. Появится множество компаний и стартапов, предлагающих свои услуги: от приложений вроде Snapchat, которое автоматически удаляет фотографию или сообщение через десять секунд после их просмотра, до более продвинутых решений, предполагающих также шифрование и короткий обратный отсчет. Однако такие приложения в лучшем случае лишь снизят риск, что частная информация станет общедоступной. Отчасти это связано с наличием контрприложений, способных автоматически делать мгновенный снимок экрана каждого отправленного сообщения или фотографии, причем быстрее, чем вы дадите мысленную команду своим пальцам, управляющим устройством. Говоря научным языком, попытки сохранить частную информацию в тайне всегда будут неудачными вследствие «аналоговой уязвимости»: в конечном счете кто-то должен увидеть информацию, если она предназначена для того, чтобы быть увиденной. И пока это так, остается риск, что этот «кто-то» сделает скриншот или скопирует контент.

Если мы выходим в интернет, то оказываемся в публичном пространстве и готовы стать публичными фигурами. Вопрос лишь в том, внимание скольких людей мы привлечем и почему. У людей сохранится определенная свобода в том, чем они будут делиться с другими при помощи своих устройств, но проконтролировать то, что сохраняют и чем делятся другие, не будет никакой возможности.

В феврале 2012 года молодой журналист из Саудовской Аравии по имени Хамза Кашгари разместил в твиттере воображаемый диалог с пророком Мухаммедом, в частности, написав: «Некоторые ваши качества я люблю, другие — ненавижу, а многие просто не могу понять». Эти твиты вызвали мгновенный всплеск ярости (нашлись люди, которые посчитали их богохульством или отступничеством; и то

и другое — страшный грех с точки зрения консервативного ислама). Через шесть часов после публикации Кашгари удалил твиты, но к тому моменту успел получить тысячи злобных откликов, угроз убийством и даже узнать о создании группы в Facebook под названием «Народ Саудовской Аравии требует казни Хамзы Кашгари». Он бежал в Малайзию, но спустя три дня был депортирован в Саудовскую Аравию, где его ждало обвинение в богохульстве (уголовном преступлении, наказуемом смертной казнью). Несмотря на то что он извинился сразу, а потом еще раз в августе 2012 года, власти отказываются освободить его.

В будущем окажется не важно, как долго были доступны для публики подобные сообщения — шесть часов или шесть секунд. Они сохранятся с того самого момента, как электронные «чернила» коснутся электронной «бумаги». Случай Кашгари лишь один из многочисленных печальных и тревожных примеров такого рода.

Как уже упоминалось, сохранность данных вследствие остаточной намагниченности останется непреодолимой проблемой везде и для всех, но как именно это отразится на людях, во многом зависит от типа политической системы и степени государственного контроля. Чтобы лучше представить себе возможные различия, рассмотрим открытое демократическое общество, репрессивный автократический режим и несостоятельное государство со слабым или неэффективным правительством.

В открытом демократическом обществе, где естественное человеческое желание делиться информацией поощряется свободой выражения своего мнения и ответственным правительством, люди будут все в большей степени становиться друг для друга и судьями, и присяжными. Доступность данных только усилит складывающуюся уже сейчас тенденцию: в обширном виртуальном ландшафте найдется место каждому мнению, обновление данных в режиме реального времени породит гиперактивное социальное общение, а вездесущие социальные сети позволят всем выступать в роли знаменитости, папарацци и зрителя одновременно. Каждый человек станет создавать гигантские объемы информации о своем прошлом и настоящем, о своих предпочтениях и решениях, о своих стремлениях и привычках. Как и сегодня, большая часть контента будет распространяться по модели opt-in: пользователь сознательно делает выбор в пользу его распространения — по некоторой причине, коммерческой или какой-то

иной; но не все сто процентов. Как и сегодня, многие онлайн-платформы продолжат передавать третьим лицам данные о действиях своих пользователей без их явного на то согласия. Так что люди будут делиться большим объемом информации, чем им кажется. Это станет настоящим подарком для властей и корпораций, ведь обильные потоки статистики позволят им быстрее реагировать на запросы своих граждан и потребителей, точнее «попадать» в интересующую их целевую аудиторию, а также — это касается новой области упреждающего анализа — прогнозировать будущее[17].

Мы уже говорили, что никогда прежде не было такого количества данных, доступных столь многим людям. Мы можем делать выводы друг о друге, пользуясь источниками как точными, так и не очень, как актуальными, например профилем LinkedIn, так и не совсем, вроде давно забытых необдуманных комментариев в YouTube. И восхождение не одного подающего надежды политика будет прервано обнародованием сохранившихся в сети свидетельств его недостойного поведения в далеком прошлом. Конечно, со временем возобладает уже сложившаяся тенденция смягчения общественной реакции на проступки политических лидеров — супружескую неверность или употребление наркотиков в молодости (помните знаменитую фразу президента Билла Клинтона: «А я не затягивался»?). Возможно, избиратели не обратят внимания на скандальный пост или фотографию, опубликованные до того, как их кандидату исполнилось восемнадцать. Терпимость общества к совершенным в юности неосмотрительным поступкам, зафиксированным онлайн, наверняка возрастет, но на это потребуется время и адаптация может оказаться довольно болезненной. В каком-то смысле это логично для нынешнего века, для которого характерно развенчание героев. В новую цифровую эпоху получит продолжение процесс, начало которому было положено ростом влияния СМИ и Уотергейтским скандалом, когда для внимательного изучения окажутся доступными еще больше данных о том или ином индивидууме, причем практически обо всех периодах его жизни. И потерять статус мифического героя будет проще простого: все не без греха, а подтверждения будут копиться в сети на протяжении всей жизни человека.

Всякий, кто желает стать профессионалом и добиться успеха в каком-либо деле, особенно предполагающем доверие со стороны клиентов, не должен опасаться за свое прошлое. Ведь вам небезразлично, что ваш семейный врач по выходным строчит длинные посты против иммигрантов или что тренер по регби вашего сына в молодости работал гидом в бангкокском квартале «красных фонарей»? Знание некоторых деталей прошлого людей, с которыми мы связаны, в том числе политических лидеров, может иметь самые неожиданные последствия. И работа, и личная жизнь будут зависеть от давних событий, зафиксированных в интернете, и многие люди всю свою жизнь могут бояться, что какие-то особенно уязвимые для критики случаи однажды выплывут на поверхность.

В век всеобщей связанности членов общества в демократических странах гораздо труднее скрыть факты коррупции, преступления и скандалы в личной жизни. Ведь в распоряжении бесконечно подозрительных граждан окажется огромное количество информации: налоговые декларации, маршруты авиаперелетов, данные геолокационных сайтов (собирающих сведения о местонахождении абонента при помощи его мобильного телефона) и так далее. Информации, в том числе полученной хакерами незаконным путем, будет более чем достаточно для начала боевых действий. Рука об руку станут работать политические активисты, инициативные группы по контролю за деятельностью властей, просто сознательные члены общества, всегда готовые призвать своих политических лидеров к ответу. При этом в их распоряжении окажется достаточно инструментов для того, чтобы определить, насколько чиновники правительства правдивы. Поначалу уровень доверия к властям может даже снизиться, но со временем он начнет расти, ведь появится следующее поколение лидеров, которые будут учитывать все эти обстоятельства.

Когда общество полностью осознает масштаб описанных изменений, его подавляющая часть потребует от властей действий по защите тайны частной жизни, причем гораздо громче, чем сейчас. С хранением информации в течение бесконечного времени невозможно бороться при помощи законов, однако правила, регулирующие обработку конфиденциальных сведений, хотя бы немного успокоят

стремящихся к приватности пользователей. Сегодняшние власти в странах, за редким исключением, не понимают, что такое интернет: ни его архитектуру, ни многочисленные способы его использования. Но через десять лет все больше политиков будут знать, как работают телекоммуникационные технологии, а также какой властью они наделяют граждан и неправительственные организации. В результате в органах власти появится больше тех, кто сможет со знанием дела обсуждать вопросы охраны тайны частной жизни, безопасности данных и защиты пользователей.

В развивающихся демократических странах, где относительно недавно появились и институты демократии, и высокие технологии, усилия правительств по регулированию этой сферы будут менее последовательными. Чаще всего появление в национальной повестке дня вопроса о необходимости защиты данных совпадает с каким-то инцидентом, формирующим запрос общества на такую государственную услугу, как это было в свое время в США. Там в 1994 году приняли федеральный закон, запрещающий департаментам, которые занимаются регистрацией транспортных средств, делиться с кем-либо этой информацией. Произошло это после целой серии громких скандалов с ее утечкой, в результате которой, в частности, была убита известная актриса. В 1988 году, после обнародования сведений о том, какие видеофильмы брал в прокате покойный судья Роберт Борк, что совпало по времени с выдвижением кандидатов в члены Верховного суда, Конгресс принял закон «О защите данных пользователей видеопроката», в соответствии с которым вводилась уголовная ответственность за раскрытие информации об истории просмотра видеофильмов без согласия потребителя[18].

Хотя весь этот цифровой хаос и станет досадной помехой на пути развития демократических обществ, саму демократическую систему он разрушить не в состоянии. Возможно, некоторые общественные институты или правовые нормы и пострадают, но не исчезнут. А когда в таких странах будут приняты необходимые законы, направленные на регулирование и контроль новых тенденций, ситуация может даже улучшиться в результате возникновения более надежного социального контракта, повышения эффективности и усиления прозрачности

общества. Но произойдет это нескоро, ведь нормы так быстро не поменяешь и всем демократическим странам на это потребуется разное время.

* * *

Больший доступ к информации о жизни людей, который является следствием революции данных, обеспечит репрессивные автократические режимы опасными преимуществами в борьбе с собственными гражданами.

Это, безусловно, очень досадный побочный эффект, и, хочется надеяться, его удастся смягчить. В нашей книге об этом пойдет речь. Однако необходимо признать, что гражданам автократических государств предстоит еще более ожесточенная борьба за свою безопасность и сохранность тайны частной жизни. Будьте уверены, что спрос на специальные инструменты и программное обеспечение для защиты людей от «цифровых» репрессий приведет к бурному росту соответствующего сектора экономики. В этом и состоит сила новой информационной революции: за каждым негативным шагом последует реакция, которая поведет к позитивным переменам. И даже в самых репрессивных государствах за сохранение тайны частной жизни и личную безопасность будет бороться большее число людей, чем против них.

Однако авторитарные режимы все же развяжут свою порочную войну. Они постараются использовать невозможность удаления данных вследствие остаточной намагниченности и свой контроль над мобильными и интернет-провайдерами для создания атмосферы, в которой население будет чувствовать себя особенно уязвимым. Уйдет в прошлое даже то подобие тайны частной жизни, которое существовало прежде: мало того что свои телефоны люди постоянно носят с собой, так они еще и превратятся в «жучки» для подслушивания, которые репрессивные власти мечтают внедрить в каждом помещении. И специальные технические решения могут защитить лишь продвинутое в технологическом плане меньшинство, да и то до поры до времени.

Власти будут «взламывать» устройства еще до их продажи, заранее обеспечивая себе доступ ко всему, что их будущий владелец скажет,

напишет и отправит как публично, так и частным образом. А людям свойственно забывать, насколько уязвимыми могут быть их секреты. И вот они уже случайно выдают спецслужбам полезную для тех информацию о самих себе, особенно если ведут активную социальную жизнь в сети, которую власти, зная, кто они и за что выступают, используют в качестве изобличающих их свидетельств. Благодаря шпионскому программному обеспечению и человеческим ошибкам репрессивные режимы смогут собирать о своих гражданах больше сведений, чем до наступления цифровой эпохи. Целые сети информаторов, поощряемых государством, будут доносить на своих знакомых. Уже существует технология, позволяющая властям управлять видеокамерами ноутбуков, виртуально вторгаясь в дома диссидентов без их ведома и получая возможность видеть и слышать все, что там происходит.

Репрессивные режимы смогут «вычислять» тех, кто установил на своих устройствах приложения для обхода цензуры, так что, даже если человек вовсе не диссидент, а просто хочет нелегально загрузить пару серий «Клана Сопрано», он окажется под колпаком. Представители государства станут проводить эпизодические случайные проверки и обыски компьютеров на предмет наличия программ для шифрования и прокси-приложений, владение которыми будет караться штрафами, тюремным заключением или означать включение в специальные списки правонарушителей. А после у каждого, кто скачал и установил средства для обхода цензуры, вдруг внезапно усложнится жизнь: он не сможет получить кредит в банке, арендовать автомобиль или заплатить через интернет, не столкнувшись с теми или иными проблемами. Агенты спецслужб будут ходить по учебным аудиториям школ и университетов страны и добиваться исключения всех, кого система слежения за онлайн-активностью уличила в загрузке на их мобильные телефоны запрещенного программного обеспечения. При этом репрессии могут распространиться на знакомых и родственников этих студентов, чтобы отбить охоту к такому поведению у как можно большего числа людей.

А в государствах с чуть менее жестким тоталитарным режимом, где власти еще не сделали обязательным использование «официальных» профилей в соцсетях, они, конечно же, попытаются контролировать

уже имеющиеся онлайн-личности, приняв соответствующие законы и внедрив средства мониторинга. Например, может стать обязательным требование включать в профиль в социальной сети определенные личные данные, такие как домашний адрес и номер мобильного телефона, чтобы за пользователем было легче следить. Вполне реально разработать специальные алгоритмы, которые позволят властям «прочесывать» публичные профили граждан с целью обнаружить нарушения требований о раскрытии обязательной информации или нежелательный, с их точки зрения, контент.

В некоторых странах эта практика уже используется, пусть пока и негласно.

> В начале 2013 года многие участники сирийской оппозиции и сотрудники международных неправительственных организаций стали сообщать о том, что их ноутбуки инфицированы компьютерными вирусами (причем это выяснялось только тогда, когда переставали действовать пароли для работы в сети). Иностранные специалисты-компьютерщики проверили жесткие диски и подтвердили наличие на них вредоносного программного обеспечения, в данном случае трояны различных типов (программы, которые внешне выглядели безобидно, но на самом деле несли угрозу), которые похищали данные и пароли, записывали введенные тексты, делали мгновенные снимки экранов, загружали новые программы, удаленно включали веб-камеры и микрофоны, а затем передавали всю эту информацию по IP-адресам, которые, как показал анализ, принадлежали государственной телекоммуникационной компании Syrian Telecommunications Establishment. В данном случае источниками шпионского программного обеспечения оказались исполняемые файлы (чтобы загрузить вирус, пользователь должен был сознательно открыть файл), но это не означает, что жертвы шпионажа вели себя излишне беспечно. Одна сотрудница неправительственной организации загрузила такой файл, когда попыталась открыть неработающую ссылку, направленную ей, казалось бы, проверенным и оппозиционно настроенным активистом в ходе онлайн-разговора относительно потребностей страны в гуманитарной помощи. И только после окончания беседы женщина с огорчением узнала, что, очевидно, разговаривала с агентом спецслужб, укравшим пароль или взломавшим его: сам активист к тому моменту уже находился в тюрьме.

Люди, живущие в таких условиях, окажутся один на один со сплоченной враждебной командой правительственных агентов и их коррумпированных корпоративных союзников. Если с какой-то задачей спецслужбы не справятся сами, то смогут обратиться к подрядчикам,

готовым к сотрудничеству. С таким уровнем мониторинга понятие «причастности к преступлению» получит новое толкование. Достаточно будет оказаться одним из людей, запечатленных на фотографии, если среди них окажется известный диссидент, которого спецслужбам удастся идентифицировать при помощи программы распознавания лиц. Нежелательное внимание властей может привлечь любой случайный человек, просто оказавшийся «в неправильном месте в неправильное время», что будет зафиксировано или на фото, или в записи голоса, или по его IP. Конечно же, это ужасно несправедливо, и нас очень беспокоит, что если таких случаев будет много, то в обществе запустится механизм самоцензуры.

Доступ в сеть умножает возможности государства контролировать своих граждан, однако он же ограничивает возможности властей контролировать распространение новостей. Замалчивание информации, откровенная пропаганда и «официальные» версии событий не работают, когда общество получает информацию извне, а купюры в новостях только вредят режиму, если население хорошо информировано и активно пользуется современными средствами коммуникации. Люди смогут фиксировать событие, делиться происшедшим с другими и комментировать событие еще до того, как представители властей решат, как себя вести и что о нем говорить. Благодаря имеющимся у каждого недорогим мобильным устройствам информация будет распространяться практически мгновенно по всей территории даже очень большой страны. Так, в Китае, где действует одна из самых сложных и всеобъемлющих систем цензуры в мире, попытки скрыть те или иные потенциально опасные для властей новости все чаще проваливаются.

> В июле 2011 года в юго-восточной китайской провинции Вэньчжоу случилось крушение высокоскоростного поезда, которое повлекло гибель сорока человек и заставило общество говорить о том, что инфраструктурные проекты в стране продвигаются слишком быстро и не подкреплены должным изучением вопросов их безопасности. Хотя об этом инциденте вскользь сообщили даже официальные каналы, его освещение в прессе активно сдерживалось. Понадобились десятки миллионов сообщений в «Вейбос» — китайском сервисе микроблогов, аналогичном Twitter, — чтобы донести до всех истинную причину катастрофы: просчеты в проекте, а не плохая погода или перебой в подаче электричества, как сообщалось ранее. Более того, выяснилось, что вскоре после

аварии власти разослали в СМИ специальные директивы, в которых, в частности, говорилось: «Никакого самостоятельного расследования причин [случившегося] предпринимать не следует, нужно просто публиковать заявления официальных органов. Никаких сомнений, никакой дополнительной проработки [темы], никаких спекуляций и никакого распространения [информации] в личных микроблогах!» Директивой также предписывалось, что журналисты должны освещать событие в позитивных тонах: «С этого момента несчастный случай с поездом в Вэньчжоу должен преподноситься в свете “огромное несчастье — повод сильнее любить друг друга”». Но этой линии придерживались только официальные средства массовой информации, а авторы микроблогов писали правду, в результате чего китайские власти оказались в довольно неловкой ситуации.

Для таких стран, как Китай, это сочетание активности граждан, вооруженных современными высокотехнологичными устройствами, и жесткого правительственного контроля может стать весьма взрывоопасной смесью. Если государство полагается на тотальное управление восприятием любых событий, то все, что подрывает его монополию: каждый зафиксированный камерой телефона ошибочный ход, каждый случай лжи, разоблаченный с помощью поступившей из-за рубежа информации, — сеет семена сомнения, поощряющие деятельность оппозиции и диссидентов среди граждан, постепенно приводя ко все большей нестабильности.

* * *

В мире сегодня осталось всего несколько несостоятельных государств со слабыми или неэффективными правительствами, но зато они представляют собой модель всеобщего доступа в сеть в условиях полного вакуума власти. И действительно, похоже, что телекоммуникации — практически единственная отрасль, способная процветать в странах с несостоятельной государственной властью. В Сомали, например, телекоммуникационные компании заполняют множество прорех, созданных десятилетиями гражданской войны и бессильным правительством, предоставляя информацию, финансовые услуги и даже обеспечивая людей электроэнергией.

А в будущем, когда рынок таких стран накроет волна недорогих смартфонов, возможностей станет больше. Телефоны помогут получать образование, медицинскую помощь, обеспечивать

безопасность и возможности для торговли, то есть услуги, которые неспособно предоставить правительство. Мобильные технологии станут долгожданной интеллектуальной, социальной и развлекательной отдушиной для населения, психологически травмированного существующей средой. Возможность выхода в сеть сама по себе не может возродить несостоятельное государство, но способна значительно улучшить положение его граждан. Далее мы поговорим о новых способах решения многих проблем как во время внутреннего конфликта, так и после его завершения, в частности позволяющих создавать виртуальные общественные институты или базы данных квалифицированных рабочих диаспоры, ускоряя тем самым восстановление местного сообщества.

В условиях вакуума власти контроль над страной часто оказывается в руках авантюристов, которые стремятся активно пользоваться высокими технологиями в своих интересах. Недавно получившие доступ к сети жители несостоятельных государств будут подвергаться всем угрозам, связанным с невозможностью полного удаления данных, учитывая отсутствие системы общественной безопасности, способной оградить их от таких рисков. Командиры вооруженных формирований, бандиты, пираты и прочие преступники, если у них хватит ума, найдут способы стать сильнее, воспользовавшись персональными данными других людей. Это может означать выбор в качестве мишеней определенных слоев населения, например состоятельных кланов или влиятельных религиозных лидеров, причем вести себя злоумышленники будут прицельно и практически безнаказанно. Если из онлайн-данных (скажем, выписок о денежных переводах, сделанных посредством мобильных платформ) видно, что какая-то семья получает относительно крупные суммы денег от своих родственников из-за рубежа, местные бандиты могут потребовать заплатить им дань — возможно, также путем мобильного перевода. Сегодня полевые командиры зачастую богатеют за счет того, что облагают данью перемещение всевозможных ценностей, а завтра (притом что наркотики, минеральные ресурсы и денежные средства по-прежнему останутся для них привлекательными) не меньшую привлекательность приобретут и персональные данные. Главари незаконных вооруженных формирований будущего могут даже не

использовать эти данные сами, а просто перепродать кому-то, кто выразит готовность за них заплатить. Но важнее всего то, что выявлять и задерживать таких авантюристов станет еще сложнее: к сожалению, они получат в свои руки возможности обеспечения анонимности, недоступные обычным людям.

* * *

Многим обитателям Кремниевой долины такие понятия, как «вакуум власти», «полевые командиры» и «несостоятельные государства», могут показаться реалиями совершенно иного мира, не имеющего к ним никакого отношения, но вскоре все может измениться. Сегодня телекоммуникационные компании, как правило, недооценивают необходимость нести ответственность перед «населением» виртуального мира. Но после того как в сети добавится еще пять миллиардов человек, станет понятно, что характеристики этих пользователей и их проблемы намного сложнее, чем первых двух миллиардов. Многие представители этих пяти миллиардов живут в условиях бедности, цензуры и физической угрозы жизни. И технологическим компаниям, предоставляющим доступ в интернет, инструменты и онлайн-платформы, придется взять на себя часть бремени физического мира, если они хотят остаться верными доктрине ответственности перед *всеми* пользователями.

Компаниям отрасли высоких технологий необходимо будет оправдать ожидания своих потребителей в отношении охраны и тайны частной жизни, и личной безопасности. Тем, кто отвечает за архитектуру виртуального мира, предстоит нести ответственность и за не самые приятные события в нем. Да, некоторые компании, делающие ставки на высокие технологии, будут вознаграждены: в конечном счете их бизнес принесет дополнительную прибыль за счет быстрого расширения, но многие окажутся не у дел. В конце концов гораздо легче обвинить неудачный продукт или конкурента, чем признать личную ответственность за провал. И, конечно, останутся те, чье стремление к прибыли затмит их ответственность перед потребителями, хотя в будущем таким игрокам будет все труднее добиваться успеха.

Уже сейчас некоторые технологические компании остро осознают ответственность перед своими пользователями и всем мировым онлайн-сообществом. Именно поэтому, предлагая свои виртуальные продукты, они требуют ознакомиться с условиями обслуживания, а также принять на себя обязанность соблюдать их. Потребители должны прочесть документ, касающийся политики компании в отношении обеспечения приватности и безопасности, чтобы сознательно относиться к передаче своей информации. Количество поставщиков товаров услуг будет постоянно расти, а это значит, что пользователю придется выбирать из огромного количества предложений и, стало быть, их проверка становится важна как никогда. Разумный потребитель проанализирует не только качество самого продукта, но и степень безопасности передачи персональных данных такому поставщику. В обстановке, когда основную роль играет общественное мнение, а не законы, на текст соглашения об условиях обслуживания мало кто обращает внимание — скорее, значение имеет репутация компании-изготовителя или поставщика информационных продуктов. В ближайшее десятилетие такое положение дел сохранится.

В наступающие бурные времена эта тенденция, естественно, повлияет и на развитие бизнеса. Некоторые секторы отрасли высоких технологий, с которыми ассоциируется наибольшее количество негатива, столкнутся с трудностями при найме квалифицированных инженеров, привлечении пользователей и продаже своих продуктов, однако вырождение таких секторов не решит всех проблем отрасли (и в конечном счете лишь навредит сообществу пользователей, ограничив их доступ к некоторым благам инноваций). В годы новой цифровой эпохи высокотехнологичным компаниям придется стать «толстокожими»: общество им будет задавать много вопросов относительно безопасности и защищенности персональных данных пользователей. И уклониться от этого, как и от необходимости четко определить свою позицию, будет невозможно.

А еще придется нанимать больше юристов. Законодатели по-прежнему не успевают за судебной практикой, что подтверждается постоянными правовыми битвами по поводу интеллектуальной собственности, патентов, конфиденциальных данных и так далее с участием всех гигантов отрасли высоких технологий. Власти разных

стран время от времени подают иски против Google, обвиняя компанию в якобы имеющихся нарушениях авторских прав или национальных законов, и нам постоянно приходится убеждать своих пользователей, что в первую очередь Google стоит на страже их интересов, не выходя при этом за рамки закона. Но если бы компании приходилось останавливать разработку продуктов всякий раз, когда она сталкивается с иском со стороны того или иного правительства, ей бы вообще ничего не удалось создать.

Компаниям предстоит научиться управлять ожиданиями общества относительно возможностей и ограничений их продуктов. В корпоративных процедурах, по аналогии с политикой правительства, придется все больше учитывать различные местные и международные факторы, в частности политические риски, дипломатические межгосударственные отношения и особенности поведения людей. Конечно, о том, что технологии равнодушны к вопросам этики, а люди — нет, будут периодически забывать. А способность помнить об этом — основа успеха в цифровую эпоху.

Стратегии защиты информации

Разработка новых стратегий защиты информации в частном и государственном секторах будет постоянно усложнять жизнь пользователей — как частных лиц, так и организаций. Очень приблизительно эти стратегии можно разделить на четыре категории: корпоративные, законодательные, общественные и личные.

Если компании отрасли высоких технологий хотят избежать нежелательного вмешательства государства, способного затормозить их динамичное развитие, им придется не просто скрупулезно выполнять собственные обязанности по охране и защите персональных данных. Определенные профилактические меры уже принимаются: появился своего рода аналог кнопки «Извлечь», которая позволяет пользователям той или иной платформы скачать все свои данные; существуют возможности управления пользовательскими предпочтениями; личные идентификационные данные больше не продаются и не передаются рекламодателям. Однако, учитывая всеобщие опасения насчет сохранения тайны частной жизни, сделать

предстоит многое. Возможно, компаниям следует подписать какую-то совместную конвенцию, взяв на себя обязательства не передавать данные пользователей третьим лицам.

«Законодательная» стратегия защиты информации будет связана с развитием юридических норм. В ходе революции данных государства столкнутся со все возрастающим требованием граждан защитить их уязвимость, вызванную тем, что полностью информацию удалить невозможно. В демократических странах это повлечет за собой установление новых законов. Они окажутся несовершенными, излишне идеалистичными и, возможно, принятыми слишком поспешно, но в целом будут представлять собой попытки общества реагировать на хаотические и непредсказуемые перемены, которые несет с собой всеобщий доступ в сеть.

Напомним, что информационный след, формирующий наши будущие онлайн-личности, станет появляться раньше, чем большинство из нас сможет это осознать. Пристальное внимание взрослых, с которым в следующем десятилетии столкнутся дети и подростки, не имеет аналогов в прошлом. Сегодня может показаться, что такой коллективный «педсовет» невозможен, ведь страшно даже представить себе последствия того, что в его распоряжении окажется описание всей нашей жизни. А поскольку это затронет интересы большей части населения, под давлением общества и политиков новые законы, отражающие специфику цифровой эпохи, обязательно будут приняты.

Велика вероятность того, что появятся политики, которые выступят за присвоение грифа «конфиденциально» всем данным о *виртуальном* поведении молодежи, ведь вот-вот станет взрослым поколение, каждый шаг представителей которого в юности будет зафиксирован в цифровых хранилищах информации. Если подобный закон будет принят, то все, что сообщал о себе человек до наступления восемнадцатилетнего возраста, окажется помещенным «под замок» и не будет подлежать раскрытию под угрозой штрафа или даже тюремного заключения. В соответствии с законом эти сведения не смогут учитывать ни работодатели, ни судьи, ни ипотечные агентства, ни учебные заведения. Конечно, таким законам будет трудно пробить себе дорогу, но они помогут изменить существующие в обществе

нормы, в результате чего большинство проступков тинейджеров, совершенных в сети, в конечном счете будут приравниваться к «экспериментам» с наркотиками или алкоголем.

В попытке защитить тайну частной жизни и повысить ответственность за разглашение конфиденциальной информации могут быть приняты и другие законы. Кражу мобильного телефона приравняют к похищению персональных данных, а онлайн-вторжение (с помощью краденого пароля или взлома аккаунта) станет наказываться так же, как взлом и незаконное проникновение в помещение[19]. Где находится грань между информацией, которой делиться можно и которой нельзя, поскольку она слишком личная, все страны будут определять самостоятельно, исходя из своих культурных особенностей. То, что посчитает непристойным или даже порнографическим индийское правительство, французское одобрит не задумываясь. Представим себе общество, с одной стороны, глубоко озабоченное сохранением тайны частной жизни, а с другой — изобилующее смартфонами со встроенными камерами и дешевыми фотоаппаратами, которые можно купить в каждом магазине игрушек. В таком обществе понятия, принятые у фотографов-папарацци («публичное» и «частное»), могут быть расширены и отнесены к каждому человеку с выделением неких «зон безопасности», где сделать снимок можно будет только в случае явного согласия объекта съемки (или, как в Саудовской Аравии, с согласия мужчины, сопровождающего женщину). Такое разрешение люди будут получать при помощи специального приложения для смартфона, а поскольку на всех цифровых фотографиях фиксируется время съемки и проставляется цифровой водяной знак, их легальность определить будет очень легко. «Цифровым водяным знаком» называют определенную последовательность битов, добавляемую к цифровому изображению, аудио- или видеофайлу и содержащую информацию об авторских правах его создателя: имя, дату съемки, вид прав и так далее. Он помогает защищать объект авторского права от незаконных манипуляций: хотя цифровой копирайт невидим глазу, его можно считать при помощи специального программного обеспечения и

определить, является ли файл оригиналом или незаконно сделанной копией.

Переходя к третьей стратегии защиты информации — общественной, зададимся вопросом: а какой будет реакция на революцию данных со стороны негосударственных структур (местных сообществ и некоммерческих организаций)? Думается, что в следующем десятилетии появятся институты гражданского общества, предназначенные для защиты постоянных пользователей интернета от их правительств и от их собственной беспечности. Мощные лоббистские группировки «продавят» законы о контенте и охране тайны частной жизни. Заметив применение репрессивных методов, правозащитные организации станут выступать за принятие мер для лучшей защиты граждан. Сформируются инициативные группы, которые будут помогать людям разных возрастов справиться с последствиями такого явления, как вечное хранение данных. Образовательные учреждения постараются внушить школьникам, какими последствиями грозит слишком широкое распространение информации о себе («никогда не делись личными данными с незнакомцами»). Недавняя кампания против кибертравли в США стала лишь первой ласточкой: скоро мы окажемся свидетелями мощных социальных инициатив снизу, направленных на увеличение осведомленности общества о правилах поведения в сети, и слабых попыток политиков помешать этому. Учителя и администрация школ будут относиться к кибертравле так же, как к травле сверстников в реальном мире, то есть наказание будет сопоставимым, с той лишь разницей, что вызов в кабинет директора последует не в день совершения проступка, а на следующее утро после того, как школьник из дома напишет что-то в сети.

Помимо смягчения негативных последствий широкого доступа в интернет, неправительственным организациям придется генерировать новые идеи в области высоких технологий, призванные изменить мир к лучшему. Благотворительные организации, работающие в развивающихся странах, уже реализуют пилотные инновационные проекты, основанные на повсеместно доступных коммуникационных технологиях. По словам администратора американского Агентства международного развития (USAID) Раджива Шаха, во время голода

2011 года, вспыхнувшего в Восточной Африке, его организация смогла обойти запрет на предоставление помощи страдающему от недоедания населению, установленный исламистским незаконным вооруженным формированием «Аль-Шабааб», благодаря совместному использованию мобильных платформ и традиционной для арабских стран системы перевода денежных средств «хавала» (она основана на передаче денег через доверенных посредников в обход классических финансовых институтов). В результате широкого использования мобильной связи и доступа в интернет как нуждающимися, так и желающими помочь появились новые возможности. Особенно активно внедряют новые высокотехнологичные решения на заре новой цифровой эпохи неправительственные и благотворительные организации, поскольку понимают, что это позволит им лучше справляться с их задачами, при этом они более гибки, чем государственные структуры, и легче идут на риск, чем представители делового мира.

Четвертая стратегия защиты информации реализуется на индивидуальном уровне. Отчетливо прослеживается склонность людей полагаться на общение посредством анонимных пиринговых сетей. В мире «без кнопки Delete» для тех, кто хотел бы остаться незамеченным, пиринговые сети станут средой «по умолчанию». Уже сегодня современные мобильные пиринговые технологии вроде Bluetooth позволяют устанавливать связь между двумя устройствами непосредственно, без необходимости подключаться к сети. (Хотя обычные пиринговые файлообменные сети вроде BitTorrent работают как раз в интернете.) Для обоих вариантов пиринговой технологии характерно то, что пользователи соединяются друг с другом для приема и передачи информации без посредника в лице фиксированного сервера, принадлежащего третьей стороне. Поэтому в будущем пиринговые технологии предоставят людям заманчивую возможность мгновенно связаться, избежав при этом нежелательного контроля или мониторинга.

Функцией пиринговой связи сегодня снабжены практически все, даже дешевые смартфоны, а после того как в следующем десятилетии они захлестнут новые рынки, воспользоваться преимуществами этих продвинутых устройств сможет еще большее число людей. В

развивающихся странах уже приобрел огромную популярность Bluetooth, ведь эта функция, как правило, доступна даже в самых простых телефонах. В большей части Западной Африки, где мобильная связь намного более широко распространена, чем компьютеры и доступ в интернет, многие используют мобильные телефоны как стереосистемы, поскольку благодаря их пиринговым возможностям могут хранить музыку, слушать ее и обмениваться музыкальными файлами с друзьями при помощи своих сотовых аппаратов.

Появление в Мали мобильных музыкальных автоматов, возможно, стало ответом на специфические проблемы инфраструктуры этой страны, но и за ее пределами люди все чаще отдают предпочтение пиринговым технологиям: кто-то по эмоциональным (невозможность удалить историю своих действий), кто-то — по прагматическим (безопасность соединения) соображениям. В государствах с репрессивным режимом граждане все чаще пользуются для связи общими пиринговыми платформами и системами передачи закодированных сообщений, например мессенджером на базе смартфона BlackBerry Messenger (BBM) компании Research in Motion (RIM), что позволяет им меньше опасаться прослушки со стороны спецслужб. В будущем им станут доступны и другие технологии на базе пиринга.

Портативные высокотехнологичные устройства пока воспринимаются как предметы роскоши: наручные часы, способные вибрировать или мягко сжимать запястье в момент срабатывания будильника (некоторые модели уже появились в продаже), серьги с датчиком измерения кровяного давления и так далее[20]. Более интересные возможности смогут предложить обладателям портативных устройств приложения, основанные на технологии дополненной реальности: наложение тактильных ощущений, звуков или изображений из виртуальной реальности на объекты физического мира. В апреле 2012 года компания Google представила собственный прототип устройства, основанного на технологии дополненной реальности, разработанного в рамках проекта Project Glass: очки со встроенным дисплеем, закрепленным чуть выше одного из глаз. Они

способны отображать информацию, передавать сообщения при помощи голосовых команд, а также записывать и воспроизводить видеоизображение посредством встроенной камеры (аналогичные устройства разрабатываются и другими компаниями). В будущем на основе технологий портативных устройств, дополненной реальности и пиринговых коммуникаций удастся объединить информацию, которую человек получает при помощи своих органов чувств и по защищенным каналам передачи данных, что позволит создавать исключительно интересные и полезные устройства.

> Например, в странах, где в общественных местах постоянно присутствуют агенты религиозной полиции или спецслужб, критически важно замечать их в толпе. Какой-нибудь изобретатель, воспользовавшись указанными технологиями, разработает наручные часы, которые при помощи импульса будут предупреждать окружающих о том, что такой агент находится в пределах видимости. На основе тактильных данных может появиться новый язык: скажем, два импульса будут означать, что приближается сотрудник спецслужб, три — команду «убегай». Кроме того, такие часы, располагая данными с GPS-приемника, смогут передавать координаты человека его соратникам, которые, имея очки дополненной реальности, сразу же определят, откуда в их сторону направляется агент. И все эти сообщения
> будут передаваться с помощью пиринговых технологий, то есть непосредственно от устройства к устройству. Это означает большую безопасность и надежность, чем если бы приходилось связываться через интернет.

Ваше мобильное устройство будет знать об окружающих то, что сами вы никак не могли бы узнать: где они, кто они такие, что содержат их виртуальные профили. Уже сегодня при помощи сетей Wi-Fi можно делиться контентом своей библиотеки iTunes с незнакомцами, а со временем возможности расширятся. В таких странах, как Йемен, где консервативные социальные нормы ограничивают общение подростков с представителями противоположного пола, многие из них захотят скрывать информацию о себе в пиринговых сетях, находясь дома или в мечети (ведь неизвестно, кто может ее увидеть), но открывать ее в парках, кафе или на вечеринках.

И все же пиринговая технология при всех своих многочисленных преимуществах представляет собой довольно ограниченный аналог

интернета. Часто бывает так, что нам нужно сохранить историю своих действий и сообщений, чтобы потом что-то освежить в памяти, особенно когда хотим спустя время поделиться с кем-то определенной информацией. Кроме того, коммуникации даже на базе пиринговой технологии не являются идеальной защитой от прослушки и мониторинга. Если представителям властей (или преступных организаций) удастся идентифицировать одного из собеседников, они, как правило, могут найти и второго. Это касается и обмена мгновенными сообщениями, и интернет-звонков (по технологии VoIP, то есть в случае передачи голоса по сети интернет) в таких программах, как Google Voice или Skype, и видеочатов. Они считаются безопасными, но, несмотря на то что диалоги шифруются, прослушать их может всякий, у кого есть доступ к промежуточным узлам сети. Так, владелец беспроводной точки доступа способен слушать все разговоры подключенных к ней пользователей. Одной из самых коварных форм кибератак, с которой могут столкнуться пользователи пиринговых сетей, является атака методом перехвата и подмены ключей. Она относится к методам активной прослушки. Суть ее заключается в том, что злоумышленник подключается между собеседниками и автоматически перехватывает их сообщения, причем у участников диалога не возникнет даже подозрений. Он действует как невидимый посредник, выдающий себя за второго собеседника. Этот посредник может спокойно наблюдать за ходом общения (перепиской, разговором или видеосвязью), время от времени перехватывая информацию и сохраняя ее при необходимости (или, хуже того, внедряя в диалог ложную информацию). Атаки методом перехвата и подмены ключей встречаются при использовании любых протоколов связи, а не только в пиринговых сетях, но особенно опасны именно в них — просто потому, что люди, использующие эти платформы, *уверены*, что находятся в безопасности.

Даже шифрование не обеспечивает достаточно надежной защиты, особенно учитывая нормы регулирования, принятые в реальном мире. В США и некоторые законодатели, и ФБР уже намекнули на возможность принятия законов, обязывающих операторов, которые предоставляют услуги связи, в частности BlackBerry и Skype, выполнять распоряжения правоохранительных органов о

прослушивании разговоров: или давая возможность перехватывать сообщения, или предоставляя ключи, с помощью которых их можно расшифровать.

Пиринговые сети могут похвастаться длительной историей противостояния с властями, как демократическими — из-за авторских прав (например, в случае с Napster или Pirate Bay), так и авторитарными — по причине политического инакомыслия (вспомним Tor). В США сервис Napster, пионер в области пиринговых файлообменных сетей, был отключен еще в 2001 году после судебного решения, в котором компании предписывалось прекратить передачу по ее сети материалов, защищенных авторским правом. (Представители Napster заявили в суде, что компания способна блокировать передачу 99,4% таких материалов, но судья решил, что этого недостаточно.) В Саудовской Аравии и Иране религиозная полиция практически не в состоянии бороться с тем, что молодые люди пользуются телефонами, снабженными функцией Bluetooth, для совершения звонков и отправки текстовых сообщений абонентам, находящимся в зоне доступа, — и не только с целью пофлиртовать, но и для координации действий во время акций протеста. Так что, пока в стране не будут конфискованы все мобильные телефоны (а в полиции понимают, что эту задачу выполнить крайне сложно), у любящих пофлиртовать юных жителей Саудовской Аравии и Ирана остается как минимум одно преимущество перед их «воспитателями» в погонах.

Во всех коммуникаторах BlackBerry реализована функция шифрования передачи голоса и данных, и благодаря уникальному шифру эти устройства стали особой мишенью для властей многих стран. В 2009 году государственный оператор связи Объединенных Арабских Эмиратов Etisalat разослал почти 150 тысячам владельцев BlackBerry предложение провести обязательное обновление системы. Под «обновлением» на самом деле имелась в виду установка шпионского программного обеспечения, создающего несанкционированный доступ к конфиденциальной информации, сохраненной в телефонах пользователей. (Когда об этом стало известно, компания RIM, производитель BlackBerry, дистанцировалась от инициативы Etisalat и рассказала пользователям, как удалить эту программу.) Не прошло и года, как в ОАЭ и в соседней Саудовской

Аравии раздались призывы ввести полный запрет на телефоны BlackBerry и разрешить использовать лишь национальные протоколы шифрования. Так же поступила Индия, выдвинув RIM ультиматум: предоставить доступ к зашифрованным каналам связи или уйти с индийского рынка. (Во всех трех странах до запрета BlackBerry все же не дошло.)

Страны с репрессивными режимами не особенно церемонятся, стремясь запретить пиринговые сети полностью или получить над ними контроль. Демократическим государствам придется действовать более взвешенно.

> Яркий пример этого мы увидели во время августовских беспорядков 2011 года в Великобритании. Они вспыхнули после убийства полицейскими в Тоттенхэме 29-летнего Марка Даггана: протестовавшие требовали справедливого расследования этого инцидента. Через несколько дней толпа стала вести себя агрессивно, начав поджигать магазины, полицейские автомобили и автобусы. Насилие и грабежи продолжались несколько ночей подряд, перекинувшись в Бирмингем, Бристоль и другие города. Результатами беспорядков стали пятеро погибших, материальный ущерб в размере 300 млн фунтов стерлингов ($475 млн) и сильнейшее потрясение общественности. Масштаб погромов и скорость их распространения по стране застали полицию и правительство врасплох, причем главным катализатором этого распространения эксперты называли такие средства коммуникации, как Twitter, Facebook и особенно BlackBerry. В самый разгар событий полиция Тоттенхэма даже призвала BlackBerry приостанавливать по ночам оказание услуг, чтобы затруднить общение погромщиков. Когда массовые волнения начали стихать, тогдашний премьер-министр Великобритании Дэвид Кэмерон, выступая в парламенте, предложил полностью блокировать подобные сервисы в определенных обстоятельствах, особенно «когда мы знаем, что люди замышляют насилие, беспорядки или преступления». По его словам, цель состоит в том, чтобы «дать полиции инструмент для отслеживания людей в Twitter и BBM — или отключения их». (Встретившись с представителями отрасли, Кэмерон заявил об их готовности сотрудничать с правоохранительными органами.)

События в ОАЭ и Великобритании показывают серьезную озабоченность властей, но важно понимать, что пока их беспокоят только шифрование и возможности социальных сетей. В будущем общение будет происходить еще и с помощью мобильных пиринговых сетей, а это значит, что люди смогут связываться друг с другом, минуя интернет (чего не было на момент описанных событий в

Объединенных Арабских Эмиратах и Великобритании). Вот причина, по которой в борьбу с функцией непосредственной связи двух и более устройств могут вступить как самые демократические, так и самые авторитарные режимы. Власти будут утверждать, что без введения ограничений или специальных мер на случай чрезвычайных обстоятельств сильно усложнится поимка и наказание преступников и террористов (а также иная законная деятельность полиции) и при этом упростятся планирование и совершение преступлений, а также размещение в публичном пространстве клеветнической, ложной и иной потенциально вредной информации. Демократические правительства станут опасаться неконтролируемого потока клеветы и утечек информации, авторитарные — роста протестов. Но если считать, что главную озабоченность властей должна вызывать незаконная деятельность, основной проблемой будет сочетание виртуальной валюты с анонимными сетями, в которых скрыто физическое место оказания услуг. Уже сегодня в сети Tor преступники продают наркотики за биткоины (виртуальную валюту), имея возможность не связываться ни с наличными деньгами, ни с банками. Те же сети будут использовать и нарушители авторских прав.

Размышляя о том, как решать проблемы такого рода, понимаешь, что черно-белый взгляд на вещи неприемлем: большое значение имеет контекст. Так, в Мексике одними из самых эффективных пользователей анонимных средств шифрования как в пиринговых сетях, так и в самом интернете являются наркокартели. В 2011 году мы встречались с министром экономики этой страны Бруно Феррари, и он рассказал нам, как правительство пытается вовлечь население в борьбу с картелями, страх мести со стороны которых силен настолько, что люди боятся сообщать о преступлениях и информировать полицию о деятельности картелей в их районе. Еще больше ограничивают возможности граждан коррупция в рядах полицейских и недоверие к ним. По словам Феррари, «если не прибегать к анонимности, то непонятно, как можно добиться того, чтобы люди доверились полиции и начали сообщать о преступлениях, совершенных наркокартелями. Чтобы граждане включились в решение этой проблемы, жизненно важно обеспечить им истинную анонимность». Поскольку картели уже используют анонимные коммуникации, это уравняет шансы. «Если

аргументы в пользу запрета анонимного шифрования и имеют смысл, то только не в Мексике», — говорит Феррари.

Полицейское государство 2.0

С учетом сказанного баланс силы между гражданами и властью будет зависеть от того, какое количество оборудования для наблюдения сможет закупить, освоить и использовать правительство. В подлинно демократических странах в условиях революции данных может развернуться борьба за сохранение тайны частной жизни и контроль за личной информацией. В конечном счете это приведет к усилению позиции граждан, появлению более честных политиков и укреплению социальных контрактов. К сожалению, большинство стран мира или не являются демократиями, или являются ими только формально, и поэтому для их жителей последствия широкого распространения доступа в сеть — как позитивные, так и негативные — окажутся гораздо более выраженными, чем где бы то ни было.

В долгосрочной перспективе развитие телекоммуникационных технологий способно подорвать положение большинства авторитарных режимов, поскольку, как мы видели, их шансы в противостоянии с людьми, вооруженными персональными устройствами для проверки фактов, снижаются с каждым одиозным случаем, ставшим достоянием гласности. Другими словами, нельзя назвать совпадением то, что авторитарные режимы существуют сегодня в странах с самым низким в мире уровнем проникновения интернета. Однако в краткосрочной перспективе такие режимы смогут извлечь преимущества за счет подключения их граждан к сети, что уже используют в своих интересах законодательство и средства массовой информации. Среди авторитарных правительств уже складывается определенная тенденция: они стараются использовать всю мощь современных высоких технологий вместо того, чтобы бояться и запрещать их, то есть налицо сдвиг от явного тоталитаризма к более тонким формам контроля, который описал в своей отличной книге The Dictator’s Learning Curve («Кривая обучаемости диктатора») журналист Уильям Добсон[21]. Вот что он пишет: «Сегодняшние диктаторы и авторитарные правители гораздо умнее и

сообразительнее, чем раньше, и чаще руководствуются здравым смыслом. Видя растущее давление, самые умные из них не ужесточают свой режим до полицейского государства и не закрываются от внешнего мира; вместо этого они учатся и адаптируются. Вызовы, с которыми сталкиваются десятки авторитарных режимов в результате развития демократии, заставляют их экспериментировать, придумывать, хитрить». Добсон перечисляет множество средств, при помощи которых современные диктаторы концентрируют власть в своих руках, создавая при этом видимость демократии: псевдонезависимая судебная система; ручной «всенародно избранный» парламент; широкое толкование и селективное применение законов; медийный ландшафт, допускающий существование оппозиционных СМИ, но только до тех пор, пока оппоненты режима признают существование негласных границ, которые нельзя переходить. По словам Добсона, в отличие от диктатур и государств-изгоев прошлого, современные авторитарные государства — это «сознательно и искусно созданные проекты, их заботливо выстраивают, укрепляют и постоянно совершенствуют».

В своем исследовании Добсон рассматривает лишь небольшое количество примеров, и мы не вполне уверены в том, что благодаря наступлению новой цифровой эпохи такого рода преимущества получат *все* авторитарные режимы. Отношение диктаторов к повсеместному распространению интернета будет во многом определять их будущее, особенно если их страны намерены конкурировать на международной арене — политически и экономически. И централизация власти, и искусное балансирование между патронажем и репрессиями, и создание благоприятного имиджа самого государства — все элементы авторитарного управления зависят от контроля над виртуальным миром, в котором «живет» население страны.

В течение ближайшего десятилетия все автократии мира столкнутся с ситуацией, когда доступ к сети получит большинство населения страны, и для диктаторов, которые хотят остаться у власти, это будет означать зону повышенной турбулентности. К счастью, создание всеобъемлющей системы мониторинга и анализа всех видов диссидентской деятельности — непростая задача, требующая

принятия нестандартных решений, привлечения дорогостоящих консультантов, использования не самых распространенных технологий и расходования значительных средств. Понадобятся сотовые вышки, серверы и микрофоны, а также дата-центры для хранения информации; специализированное программное обеспечение для обработки собранных данных; квалифицированный персонал для их обслуживания; базовые ресурсы вроде электроэнергии и каналов связи, причем непрерывно и в больших количествах. Если авторитарные правители захотят построить государство, способное следить за каждым, это будет им дорого стоить — надеемся, дороже, чем они могут себе позволить.

В некоторых странах с репрессивными режимами население бедное, но там достаточно нефти, минералов и прочих ресурсов, которыми можно торговать. По аналогии со сделками «оружие в обмен на сырье» можно предсказывать расцвет сделок «технологии в обмен на сырье» между странами, бедными с точки зрения технологии, но богатыми минеральными ресурсами (скажем, Экваториальной Гвинеей) и технологически развитыми, но нуждающимися в ресурсах (очевидный пример — Китай). Не все смогут успешно заниматься торговлей такого рода, и будем надеяться, что если и смогут, то не сумеют эффективно и последовательно использовать то, что получат взамен.

Создав инфраструктуру, репрессивные режимы будут нуждаться в суперкомпьютерах, способных обработать огромные массивы собранной информации. Там, где доступ в интернет появился давно, власти располагали временем для изучения типов данных, создаваемых жителями страны, ведь темпы распространения информации были невысокими, а технический прогресс — сравнительно медленным. Однако у репрессивных режимов стран, где население получило доступ к интернету недавно, такой форы по времени нет: чтобы эффективно управлять, им придется очень быстро научиться использовать собранную информацию. Для этого они станут создавать мощные компьютерные банки данных, опирающиеся на гораздо большие вычислительные мощности, чем те, которыми обладают средние ноутбуки, и покупать или разрабатывать программное обеспечение, с помощью которого можно проводить глубинный анализ данных и мониторинг трафика в режиме реального

времени. Сегодня можно купить все, что требуется для построения страшного цифрового полицейского государства, причем ограничения на экспорт технологий не особенно эффективны, их легко обойти.

Как только хотя бы одному из репрессивных режимов удастся построить государство тотального контроля над гражданами, он поделится своими знаниями с другими. Известно, что авторитарные правители обмениваются друг с другом информацией, стратегиями управления и вооружением, поэтому логично ожидать, что разработанная в одной из таких стран конфигурация системы наблюдения (если она работает) распространится среди ее союзников. А компании — производители программного обеспечения для глубинного анализа данных, камер видеонаблюдения и прочих продуктов будут хвастаться своими государственными заказами в целях привлечения новых покупателей.

Самый важный тип данных, который стремятся получить репрессивные режимы, — это не посты в Facebook и не комментарии в Twitter. Это биометрическая информация, которую можно использовать для уникальной идентификации индивидуума по его физическим и биологическим характеристикам. Сегодня всем известны такие виды биометрических данных, как отпечатки пальцев, фотографии и анализ ДНК. Но когда вы окажетесь в Сингапуре, то с удивлением узнаете о требованиях службы безопасности аэропорта не только заполнить карточку прибытия, но еще и записать свой голос. А в будущем программное обеспечение распознавания голоса и лиц намного превзойдет своих предшественников в точности и широте применения.

В сегодняшних системах распознавания лиц используется фотокамера, делающая снимок глаз, рта и носа человека и выделяющая «вектор свойств», то есть набор значений, описывающих ключевые параметры лица, например точное расстояние между глазами (не забывайте, что цифровой снимок — это всего лишь цифры). Найденные значения загружаются в большую базу данных для последующего поиска соответствий. Многим это покажется фантастикой, да и точность работы такого программного обеспечения пока ограниченна (помимо прочего, не распознаются лица, снятые в

профиль), но за последние несколько лет в этой области достигнут значительный прогресс.

> В 2011 году команда исследователей из Университета Карнеги–Меллон продемонстрировала результаты исследования, в рамках которого благодаря сочетанию стандартного программного обеспечения распознавания лиц и находящихся в открытом доступе онлайн-данных удалось очень быстро находить соответствия черт и определять людей, причем с применением «облачных» вычислений. В одном из экспериментов безымянные фотографии с сайтов знакомств (где люди часто пользуются псевдонимами) сравнивались со снимками, размещенными в аккаунтах на сайтах социальных сетей, которые можно найти с помощью поисковых машин (то есть не авторизуясь), и результаты сравнения оказались статистически значимыми. Ученые отметили, что вручную такой поиск провести невозможно, но благодаря «облачным» вычислениям на поиск среди миллионов лиц требуются считаные секунды. Точность поиска оказалась выше в случае, когда пользователь размещал в интернете большое количество фотографий, а во времена Facebook таких большинство.

Как и многие другие технологические новшества, сбор всеобъемлющих биометрических данных в перспективе может помочь решить застарелые социополитические проблемы, что вызывает у диктаторов обильное слюноотделение. Однако на каждый репрессивный режим, собирающий биометрические данные для притеснения собственного населения, найдется открытое, стабильное и прогрессивное общество, делающее такие же инвестиции по совершенно иным причинам.

Самым крупным биометрическим проектом стала индийская Программа уникальной идентификации (UID). Целью кампании, запущенной в 2009 году и известной в Индии под названием «Аадаар» («основание», «поддержка»), является обеспечение каждого жителя страны — а их 1,2 млрд — картой, содержащей уникальный 12-значный номер, со встроенным чипом, на котором записаны биометрические данные человека, в том числе его отпечатки пальцев и сканированное изображение сетчатки глаза. Эта программа видится ее инициаторам как инструмент решения проблем неэффективности, коррупции и мошенничества, присущих существующей системе, в которой благодаря множеству юрисдикций предполагается использование до двадцати разных документов, удостоверяющих

личность, выпускаемых различными местными и национальными органами власти.

Многие индийцы верят, что по мере реализации программы «Аадаар» удастся помочь тем, кто сейчас исключен из поля зрения правительственных институтов и сетей распределения помощи. Для представителей каст и племен, традиционно находящихся внизу социоэкономической шкалы, «Аадаар» станет шансом получать государственную поддержку в виде муниципального жилья и продуктовых пайков, что технически было возможно и раньше, но практически оказывалось им недоступно из-за того, что многих потенциальных получателей помощи невозможно было идентифицировать. Благодаря «Аадаар» смогут открывать банковские счета, получать водительские удостоверения, обращаться за государственной поддержкой, голосовать и платить налоги и другие категории населения, испытывающие проблемы с идентификацией, например внутренние мигранты, работающие не по месту жительства. Включенный в схему человек сможет открыть счет в банке, привязанный к своему UID-номеру. Это позволит правительству легко отслеживать субсидии и льготы.

* * *

В политической системе, пораженной коррупцией и придавленной самим масштабом проблемы (меньше 3% индийцев зарегистрированы для уплаты подоходного налога), эти усилия, похоже, предпринимаются в интересах всех честных граждан. У бедняков и жителей деревень появятся удостоверения личности, государственная система станет эффективнее, а все стороны гражданского общества (включая голосование на выборах и уплату налогов) — более прозрачными и охватывающими больший процент населения. Но у «Аадаар» есть и противники — это те, кто считает ее по сути и масштабу оруэлловской, направленной на повышение возможностей индийских властей контролировать общество за счет индивидуальных свобод и тайны частной жизни. (И действительно, правительство может при помощи «Аадаар» отслеживать передвижения, телефонные разговоры и финансовые операции лиц, подозреваемых в терроризме.)

Те же оппоненты программы отмечают, что на самом деле индийцам не обязательно иметь карту с UID, поскольку пока государственные органы не имеют права требовать ее предъявления при оказании услуг. Опасения по поводу того, не вторгается ли индийское правительство в сферу гражданских свобод, стали своеобразным эхом протестов оппозиции по поводу аналогичного проекта, инициированного в Великобритании с принятием закона «Об удостоверениях личности» 2006 года. (После нескольких лет борьбы за реализацию этой программы недавно избранное коалиционное правительство страны в 2010 году приняло решение от нее отказаться.)

Что касается Индии, то вполне возможно, что потенциальные выгоды этого проекта перевешивают сомнения, но само их наличие доказывает, что даже в демократических странах возможны опасения: кому в конечном счете послужат огромные массивы биометрической информации — гражданам или государству? И что если биометрические данные начнут всерьез собирать наименее демократические страны? Некоторые уже делают это, начав с паспортов.

Биометрическими данными заинтересуются не только правительства. К созданию или приобретению таких баз данных будут стремиться командиры вооруженных формирований, наркокартели и террористические группы с целью проверки новобранцев, мониторинга потенциальных жертв и вообще контроля за своими организациями. Здесь сработает та же логика, что в случае с диктаторами: если у них есть чем торговать, нужные технологии они получат.

Учитывая стратегическую ценность биометрических данных, государствам следует присвоить защите информации о своих гражданах такой же высокий приоритет, как и защите оружия массового поражения. Сейчас к созданию системы биометрических данных населения идет Мексика, правительство которой стремится повысить эффективность правоохранительных органов, надежность границ, а также идентифицировать преступников и лидеров наркокартелей. Но поскольку картели уже наводнили своими агентами полицию и многие национальные институты, существует реальная опасность того, что кто-то может получить незаконный доступ к

ценным сведениям о мексиканцах. В конечном счете правительственную биометрическую базу данных похитит или иным незаконным образом получит в свое распоряжение некая преступная группировка, и, возможно, только после того, как это случится, государство решит сделать полномасштабные инвестиции в надежную систему защиты такой информации.

Население, как правило, согласно с тем, что биометрические данные следует хранить вне пределов досягаемости преступных групп, однако власти большинства стран приложат все усилия, чтобы не допустить к ним и простых граждан. Законодательство о защите биометрических данных, как и иных персональных данных пользователей, будет различаться от страны к стране. Так, в Европейском союзе, который уже имеет несколько огромных баз биометрических данных, от стран-участников на законодательном уровне требуется обеспечить недопустимость нарушения права человека на тайну частной жизни. Прежде чем вводить биометрические данные в систему, необходимо получить от индивидуума явное и информированное согласие на это, оставив ему право отозвать свое согласие в будущем без каких-либо санкций. От стран-участниц требуется отслеживать жалобы и обеспечивать компенсацию ущерба потерпевших. Вероятно, в США будут приняты аналогичные законы, ведь там также звучат опасения по поводу возможных утечек персональных данных. В странах с репрессивным режимом эта информация, скорее всего, окажется в распоряжении министерства внутренних дел, а это означает, что в первую очередь она будет использоваться в интересах полиции и спецслужб. В таких странах агенты правительства получат доступ к программному обеспечению распознавания лиц, а также к инструментам слежки за неугодными через их же мобильные устройства. Так смартфон окажется для спецслужб полезнее пистолета.

* * *

Рассуждая о сохранении тайны частной жизни и безопасности, мы редко объединяем эти темы и задаемся вопросом: а какова здесь роль интернета? Дело в том, что и в самых репрессивных государствах

мира, и в наиболее демократических людей пугает одно и то же: неизвестность, опасности и стресс, которые проникают в их жизнь в результате общения с незнакомыми людьми, имеющими доступ в сеть. Для тех же, кто уже подключен к интернету, совершенно естественно жить одновременно в двух мирах — реальном и виртуальном, это стало частью их натуры. По мере того как мы привыкаем к переменам, становится понятно, что эти два мира не являются взаимно исключающими, ведь то, что происходит в одном из них, имеет свои последствия в другом.

Дискуссия, которая сейчас в основном касается безопасности и сохранения тайны частной жизни, вскоре будет расширена до обсуждения вопроса, кто контролирует виртуальные личности и влияет на них, а следовательно, и на их владельцев. Демократические страны попадут в большую зависимость от коллективной мудрости их жителей (неясно, хорошо это или плохо), небогатые авторитарные режимы постараются найти ресурсы для того, чтобы расширить контроль за населением и виртуальным миром, а более богатые диктатуры построят современные полицейские государства, еще сильнее прижав своих граждан. В результате всех этих перемен выработаются новые привычки и появятся прогрессивные законы, но, учитывая сложность высоких технологий, в большинстве случаев людям придется смириться с тем, что они потеряют ту степень защищенности, которой обладают сегодня. Поведение населения, бизнеса и государственных структур в ходе грядущих изменений будет в значительной степени зависеть от принятых в обществе социальных норм, законодательной базы и конкретных национальных особенностей.

А мы рассмотрим вопрос о влиянии повсеместного распространения интернета на то, как государства взаимодействуют, торгуют и воюют друг с другом. Никогда раньше дипломатия не была такой интересной, как в новую цифровую эпоху. Многим странам, традиционно играющим ведущие роли на мировой арене, придется пересмотреть подходы к своей внешней и внутренней политике в мире, где тактика поведения в реальном и виртуальном мирах не всегда одинакова.

Примечания к главе 2

ГЛАВА 3

Будущее государства

Большинство людей очень смутно представляют себе, как работает интернет, и во многих случаях это нормально. Чтобы свободно чувствовать себя в виртуальном мире, не обязательно понимать внутреннюю архитектуру сети и знать, для чего нужна хэш-функция. Но перед тем как начать обсуждать взаимовлияние государства и интернета, имеет смысл определить некоторые базовые понятия, чтобы легче было воспринимать дальнейший текст.

Изначально интернет задумывался как «сеть сетей», то есть огромная децентрализованная паутина компьютерных систем, предназначенная для передачи информации с использованием стандартных протоколов. То, что видит конечный пользователь, например сайты и веб-приложения, — это лишь «флора» и «фауна» интернета. За этим стоят миллионы машин, с невероятной скоростью передающих, обрабатывающих и принимающих пакеты данных по оптоволоконным и медным кабелям. Все, с чем мы сталкиваемся онлайн, и все, что сами отправляем, — это в конечном счете лишь последовательности цифр, которые упакованы и отправлены по частям через несколько маршрутизаторов, расположенных в разных частях мира, а затем снова собраны в единое целое у получателя.

Часто мы называем интернет «пространством без законов», которым никто не управляет и которое неуправляемо по определению. Его децентрализованная концепция и постоянно мутирующая структура взаимных связей делают тщетными любые попытки правительства «контролировать» сеть. Однако при этом государство обладает огромной властью над *механической составляющей* интернета, расположенной на его территории. Это связано с тем, что оно действительно способно контролировать физическую инфраструктуру, необходимую для доступа в сеть: передающие вышки, маршрутизаторы, коммутаторы, то есть точки входа, выхода и

промежуточные точки передачи интернет-данных. Правительство может регулировать контент, ограничивать людей в приобретении и использовании оборудования и даже создавать отдельные «интернеты». От возможности выхода в сеть выигрывают и государства, и их граждане, но по-разному. Людей делает сильнее информация, к которой они имеют доступ, а власть — ее роль «привратника».

До сих пор шла речь о том, что произойдет, когда доступ к сети получат миллиарды новых пользователей (как они будут использовать интернет, с помощью каких устройств это делать, как изменится при этом их жизнь?). А вот на что будет похожа сама сеть? Каким окажется влияние на нее тех или иных шагов различных стран в реальном и виртуальном мире в рамках межгосударственного взаимодействия и отношений властей с собственным населением? Важность этих вопросов возрастает по мере того, как доступ к интернету получают народы с различными алфавитами, интересами и культурными нормами, чьи лидеры имеют разные цели, разных врагов и одинаково ограниченные ресурсы. И вполне возможно, что главный вопрос следующего десятилетия будет состоять не в том, использует ли общество интернет, а в том, какую версию интернета оно использует.

По мере того как правительства все большего количества стран привыкают к тому, что основная масса жителей имеет доступ к сети, они начинают стремиться к контролю над ней как на местном, так и на глобальном уровне. В результате наступления виртуальной эры какие-то государства укрепятся, став безопаснее, влиятельнее и получая выгоду от надежных альянсов и разумного использования цифровой мощи. Другие будут бороться лишь за то, чтобы не отстать и адаптироваться к технологическим изменениям внутри страны и за рубежом. Межгосударственные союзы, альянсы и вражда распространятся и на виртуальный мир, добавив к традиционной политике новое интригующее измерение. Во многом на интернет можно смотреть как на воплощение известной в международных отношениях классической теории об анархическом мире без лидеров. Поговорим о том, каким нам видится взаимодействие государств друг с другом и со своими гражданами.

«Балканизация» интернета

Каждая страна мира живет в соответствии со своими законами, культурными нормами и понятиями о приемлемом поведении. После того как в следующем десятилетии миллиарды людей получат доступ в сеть, многие поймут, что обрели независимость идей, речей, общения, благодаря чему им станет тесно в национальных границах. В то же время любое государство, напротив, предпочло бы, чтобы такие пользователи оказались в таком виртуальном мире, где власть зеркально соответствует возможностям контроля в мире физическом. Понятное, хотя и удивительно простодушное желание! Так что каждое государство постарается регулировать интернет и загнать его в собственные рамки. Вообще побуждение спроецировать законы реального мира на виртуальное пространство является универсальным для всех стран — от самых демократических до наиболее авторитарных. Всего, с чем они не могут справиться в реальном мире, они попробуют добиться в мире виртуальном: исключить ненавистные им элементы общественного устройства, да и вообще все, что противоречит их законам, все, что кажется им угрожающим.

С той или иной формой цензуры (известен ее эвфемизм «фильтрация») сталкиваются большинство пользователей интернета, но то, как она работает, во многом зависит от политики государства и его технологической инфраструктуры. Не все, что связано с цензурой (даже не большая часть этого), относится к политике (так, прогрессивные страны методично блокируют довольно незначительное количество сайтов, содержащих детскую порнографию).

В одних странах для доступа в интернет можно использовать несколько точек входа, подконтрольных определенным частным телекоммуникационным компаниям, деятельность которых определенным образом регулируется. В других странах точка входа всего одна — государственный интернет-провайдер, пропускающий через себя весь трафик. В последнем случае организовать фильтрацию сравнительно легко, в первом — сложнее. Многообразие применяемых сегодня в мире систем фильтрации вызвано именно этими различиями

в инфраструктуре, а также культурными особенностями и целями регулирующих ведомств.

В большинстве стран фильтрация организована на уровне интернет-провайдеров. Обычно правительства ограничивают трафик через маршрутизаторы, соединяющие страну с остальным миром, и через DNS-серверы (серверы системы доменных имен). Это позволяет им или полностью блокировать сайт (YouTube в Иране), или обрабатывать сетевой контент при помощи технологии фильтрации сетевых пакетов по их содержанию (Deep Packet Inspection, DPI). Технология DPI реализована на базе специального программного обеспечения, позволяющего маршрутизатору «заглядывать» в пакеты данных и, кроме прочего, проверять их на наличие запрещенных слов (еще встречается использование программ анализа настроения, отслеживающих, например, негативные высказывания о политиках), после чего при необходимости блокировать пакеты. Ни один из методов не имеет полноценной «защиты от дурака»: блокированные сайты можно посетить, используя обходные пути вроде прокси-серверов (они обманывают маршрутизаторы) или безопасные протоколы шифрования https (позволяют организовывать закрытый канал связи через интернет, который, по крайней мере в теории, недоступен никому, кроме вашего компьютера и сайта, на который вы заходите). Кроме того, DPI редко удается выловить все случаи появления запрещенного контента. Наиболее продвинутые с точки зрения цензуры страны инвестируют огромные ресурсы в создание таких систем, а затем вводят серьезные наказания для тех, кто пытается их обходить.

Когда специалисты в области информационных технологий стали замечать, что отдельные государства пытаются регулировать виртуальное пространство и влиять на него, то заговорили о «балканизации» интернета: из-за фильтрации на национальном уровне и прочих ограничений некогда «глобальный» интернет постепенно трансформируется в связанную совокупность национальных сетей (рекомендуем прочитать на эту тему книгу Джека Голдсмита и Тима By Who Controls the Internet — «Кто контролирует интернет»). В результате этого всемирная паутина распадется на фрагменты и секторы: появится «русский интернет», «американский интернет» и

так далее, которые будут сосуществовать и иногда пересекаться, но останутся изолированными в существенных аспектах. И каждый из них будет иметь уникальные национальные черты. В основном информационные потоки ограничатся рамками страны, не выходя за ее пределы, по причине фильтрации, языковых барьеров или просто предпочтений пользователей. (Есть данные, что большинство пользователей в виртуальном мире, как правило, не покидают свою культурную среду, и не столько из-за цензуры, сколько в силу привычного языка, общих интересов и удобства. Кроме того, в этом случае интернет работает быстрее, ведь сетевое кэширование, или временное хранение контента в местных дата-центрах, позволяет значительно повысить скорость доступа пользователей.) Вначале этот процесс будет едва заметным, но затем углубится и в конечном счете полностью изменит интернет[22].

Уже начался первый этап этого процесса — агрессивная и явная фильтрация трафика. Вероятность реализации того или иного варианта описанного выше сценария очень высока, а вот какого именно, во многом определится тем, что будет происходить в следующие десять лет с недавно получившими доступ к интернету странами; тем, какой путь они выберут, на кого станут равняться, с кем сотрудничать, какими принципами руководствоваться. Чтобы наметить возможные варианты, рассмотрим применяемые сегодня подходы к фильтрации. Мы выделили как минимум три модели: агрессивную, умеренную и приемлемую (с политической и культурной точек зрения).

Начнем с агрессивной: активнее и энергичнее всех в мире фильтрацией трафика занимается Китай. Китайским правительством заблокированы целые платформы, невероятно популярные в мире: Facebook, Tumblr, Twitter. В виртуальном публичном пространстве страны отсутствуют некоторые понятия, например «Фалуньгун» (это название запрещенной религиозной группы, ассоциирующейся с одним из флангов оппозиции), ставшие жертвой официальных цензоров или самоцензуры. В китайском интернете вам не найти упоминаний политически острых тем вроде протестов на площади Тяньаньмэнь, объективной информации о властях страны, о движении за освобождение Тибета и далай-ламе — ничего, что касалось бы прав

человека, политических реформ или вопросов суверенитета. Когда речь заходит об этом, жертвой цензуры становятся даже самые известные западные СМИ. В июне 2012 года были блокированы Bloomberg News, причем как на китайском, так и на английском языках, после публикации репортажа об огромном состоянии семьи тогдашнего вице-президента (и нынешнего президента) страны Си Цзиньпина. Спустя четыре месяца подобная участь постигла газету New York Times, на сайте которой была размещена аналогичная история о тогдашнем премьере Вэнь Цзябао. Неудивительно, что информация о способах обхода цензуры также блокируется. О том, как четко и тщательно могут работать ведомства, отвечающие за цензуру в Китае, мы узнали в 2011 году, когда после неоднозначного визита в Пекин Эрика, председателя совета директоров Google, из китайского интернета были удалены все упоминания о его поездке, хотя в остальных сегментах сети ее описание журналистами по-прежнему можно было найти.

Для среднего китайского пользователя работа цензуры выглядит «бесшовной»: ему может показаться, что некоторых идей или событий вообще никогда не существовало. Усугубляет дело использование китайским правительством упреждающей тактики: по одной из оценок, сделанных в 2010 году, на службе у властей находится почти 300 тысяч «онлайн-комментаторов», пишущих хвалебные посты о своих начальниках, правительстве и Коммунистической партии. (Такая деятельность — ее часто называют «астротурфингом», — то есть создание видимости общественной поддержки, довольно популярна в мире и используется рекламными агентствами, а также в ходе пиар- и избирательных кампаний.)

Власти Китая ничуть не стесняются защищать свою жесткую позицию в отношении цензуры. В выпущенном в 2010 году официальном правительственном докладе интернет назван «кристаллизованной мудростью человечества», однако там же отмечено, что китайские «законы и нормы регулирования явным образом запрещают распространение информации, направленной на низвержение государственного строя, подрыв национального единства или посягательство на честь или интересы страны». «Великая китайская межсетевая стена», как уже называют набор инструментов,

использующихся государством для блокировки трафика, ни много ни мало стоит на страже китайской государственности: «На территории Китая интернет находится под китайской суверенной юрисдикцией. Следует уважать и защищать интернет-суверенитет Китая». Такой беззастенчивый и безжалостный подход к цензуре, естественно, привлекателен и для других стран, властям которых свойственны авторитарные черты, а также для стран с очень однородным населением (на эмоциональном уровне опасающимся информации извне).

Пример умеренной интернет-фильтрации являет Турция, которая использует гораздо более мягкий подход, чем Китай, и даже как-то реагирует на выдвигаемые обществом требования свободы интернета, тем не менее шизофренически продолжая свою политику цензурирования. У турецких властей непростые отношения с сетью: мягче, чем у правительств многих соседних стран, но все же намного жестче, чем у их европейских союзников. В Турции невозможно получить нефильтруемое подключение к интернету, что сильно отличает ее от западных стран. Более двух лет турецкое правительство блокировало работу YouTube после того, как компания отказалась удалить видеоролик, названный властями страны клеветническим по отношению к ее основателю Мустафе Кемалю Ататюрку. (В соответствии с требованиями закона 1951 года, в котором публичные нападки на Ататюрка признаются уголовным преступлением, YouTube согласилась блокировать показ видеоролика для турецкой аудитории, но правительство настаивало, чтобы он был удален и с глобальной платформы.) Тот запрет был очень заметным, а вот последующие шаги цензуры оказались не столь явными: сегодня в Турции блокируются около восьми тысяч сайтов, причем без какого-либо уведомления или подтверждения со стороны властей.

Умеренная модель фильтрации используется правительствами, пытающимися сохранить баланс между противоречивыми убеждениями, нормами поведения и тревогами жителей страны. Но, вставая на этот путь, власти сами рискуют превратиться во врагов, если будут действовать опрометчиво или если их манипуляции станут известны общественности.

Вот недавние события в той же Турции: в 2011 году правительство страны объявило о создании новой национальной программы фильтрации интернет-трафика, предусматривающей четыре уровня цензуры, из которых граждане могли сами выбирать устраивающий их (по мере ослабления: «детский», «семейный», «местный», «стандартный»). Агентство информационных и телекоммуникационных технологий (в Турции известное по аббревиатуре ВТК) заявило, что эта схема призвана защитить малолетних детей, и обещало, что выбравшие «стандартный» уровень фильтрации совсем не столкнутся с цензурой. Многие скептически настроенные пользователи интернета не поверили заверениям ВТК относительно прозрачности этой схемы. Обнародованный план вызвал такую бурю недовольства, что тысячи людей более чем в тридцати турецких городах вышли на улицы, протестуя против предложенных изменений.

Под этим давлением правительство изменило свой первоначальный план, в итоге оставив на выбор всего два фильтра контента: «детский» и «семейный». Но на этом противостояние не прекратилось. Организации, выступающие за свободу СМИ, сообщают, что их собственные тесты на наличие цензуры выявляют гораздо более агрессивную фильтрацию, чем признает ВТК. Оказалось, что помимо ожидаемого запрета на слова, связанные с порнографией и насилием, в новой системе блокируются и обычные новостные сайты, контент которых или слишком либерален с культурной точки зрения (например, все, что содержит слово «гей», а также информация об эволюции на планете), или связан с курдским меньшинством. Некоторые активисты считают, что блокирование информации о курдских сепаратистских организациях в рамках «детского» фильтра представляет собой доказательство недобрых намерений властей; «цензурой с черного хода» назвала тактику турецкого правительства международная неправительственная организация «Репортеры без границ».

Нельзя сказать, что власти Турции не реагируют на критику своей новой системы. Когда одна из турецких газет сообщила, что образовательные сайты, рассказывающие о научной эволюции, блокируются, а публикации одного из известных в стране сторонников божественного происхождения человека — нет, блокировка была немедленно снята. Однако новая политика совсем или почти совсем непрозрачна в вопросе о том, какой контент подвергается цензуре, в результате чего правительство вынуждено реагировать лишь после того, как о подобных несоответствиях становится известно всем. Таким образом, умеренная модель фильтрации интернет-трафика сочетает в себе умение властей избежать подотчетности с готовностью делать конструктивные шаги под давлением общественности. Этот подход привлекателен для стран с крепнущим гражданским обществом

и сильными государственными институтами или тех стран, где у правительства недостаточно широкая поддержка, но достаточно полномочий, чтобы можно было принимать такие решения.

Третий подход, а именно фильтрация, приемлемая с политической и культурной точек зрения, применяется в таких непохожих друг на друга странах, как Южная Корея, Германия и Малайзия. В этом случае фильтры используются ограниченно и избирательно, причем в отношении совершенно конкретного контента, основаны на законе, не пытаются замаскировать цензуру, за ними нет какой-то иной скрытой мотивации. Кто-то, может, и недоволен политикой фильтрации, но большая часть населения принимает ее, считая полезной с точки зрения общественной безопасности и благополучия всех граждан. Например, в Южной Корее закон «О национальной безопасности» явно называет уголовным преступлением публичное выражение поддержки Северной Кореи как в реальном мире, так и в виртуальном пространстве. Контент, связанный с северным соседом, регулярно фильтруется южнокорейским правительством: сообщается, что в 2010 году были заблокированы около сорока сайтов, связанных с северокорейским режимом или поддерживающих его, закрыт десяток аккаунтов сторонников Пхеньяна в социальных сетях (Facebook и Twitter), администраторов различных сайтов принудили удалить более сорока тысяч просеверокорейских постов.

В Германии в соответствии с законодательством запрещены разжигание ненависти, отрицание Холокоста и неонацистская риторика, соответственно, на территории страны блокируются все сайты, где выражаются такие взгляды.

Малайзия, несмотря на обещание никогда не подвергать интернет цензуре, к тому же закрепленное на законодательном уровне — в законе «О гарантиях», в 2011 году внезапно заблокировала доступ к файлообменным сайтам, таким как Megaupload и Pirate Bay, заявив, что они нарушают закон «Об авторском праве» 1987 года. В заявлении Малайзийской комиссии по телекоммуникациям и мультимедиа говорилось: «Требование соблюдения законов не может считаться цензурой». Несмотря на протест многих малайзийцев, такая блокировка сайтов остается политически и юридически приемлемой.

Хочется надеяться, что последний описанный подход станет нормой для всех стран мира, но это кажется маловероятным: настолько прозрачными и сдержанными могут быть лишь страны с хорошо информированным и вовлеченным в политическую жизнь населением. А поскольку большинство правительств принимают такие решения до того, как все граждане получат доступ в сеть, у них не будет стимулов продвигать идею свободного и открытого интернета, что привело бы к созданию в стране «политически приемлемой модели» фильтрации контента.

* * *

Эти тенденции сохранятся и далее, что, в общем, предсказуемо. Властям разных стран будет казаться, что борьба с интернетом, бесконечно изменчивым и воспроизводящимся, обречена на поражение и его «балканизация» может стать популярным способом решения встающих перед ними проблем. Следующим этапом на этом пути для многих государств окажется коллективное редактирование — формирование неких сообществ по интересам с целью совместной правки контента, основанного на общих ценностях или интересах геополитики. Такие коллективные действия как в реальном, так и в виртуальном мире станут логичным шагом для тех стран, которые решат, что по отдельности у них недостаточно ресурсов или возможностей для того, чтобы оказывать сколь-нибудь значительное влияние на интернет. Но даже при условии балканизации киберпространство слишком велико для тех, кто хочет его освоить, поэтому так же, как государства поддерживают друг друга в военном отношении, чтобы обезопасить большую территорию, они будут формировать альянсы для контроля над большей частью виртуального мира. Для крупных стран совместные усилия в этом направлении позволят сделать легитимными их собственные действия по фильтрации контента и избежать нежелательного внимания к ним (с помощью оправдания вроде «смотрите, все так делают»). А мелким альянсы такого рода помогут без особых затрат добиться расположения более серьезных игроков, впоследствии получив

некоторые недостающие им полезные технические навыки и возможности.

Коллективное редактирование может начать работать в случае схожих культур, одинаковых предпочтений и антипатий: неприятия тех или иных религиозных меньшинств, отношения к другим государствам или историческим фигурам вроде Владимира Ленина, Мао Цзэдуна или Мустафы Кемаля Ататюрка. В виртуальном мире общие культурные и поведенческие характеристики способны притягивать друг к другу даже такие страны, которые в реальной жизни не имеют поводов для сотрудничества. Но привлекать это будет не столько крупные государства (у них достаточно своих технических возможностей), сколько мелкие, так что полезным такой метод объединения ресурсов найдут именно они. Скажем, если некоторым странам — членам Содружества Независимых Государств (СНГ), объединения бывших республик СССР надоест настойчивое насаждение Москвой во всем регионе русского языка, они могут объединиться и отфильтровать весь русскоязычный контент в своих национальных сегментах интернета, тем самым ограничив влияние России на население.

Вероятнее всего, основными факторами такого сотрудничества станут идеологические и религиозные установки. Они уже сейчас во многом определяют работу цензуры.

> Представьте, что будет, если группа глубоко консервативных мусульманских стран, большинство жителей которых — сунниты (скажем, Саудовская Аравия, Йемен, Алжир и Мавритания), сформирует онлайн-альянс, основанный на общих ценностях и стратегических целях, и решит создать «суннитский интернет». Оставаясь технически частью «большого интернета», для населения этих стран он превратится в основной источник информации, новостей и исторических знаний. В течение долгих лет развитие и распространение интернета во многом определялось его англоязычными стандартами, но сейчас все меняется: продолжается внедрение интернационализированных доменных имен (IDN), которые позволяют людям использовать названия сайтов, написанных не только символами латинского алфавита (например, http://إختبار.مثال). Создание «суннитского интернета» — да на самом деле любого национального сегмента сети — становится вероятнее, если пользователи могут получить доступ к версии интернета на своем языке.

Именно при условии существования «суннитского интернета» можно было бы добиться его соответствия нормам шариата (конечно, это зависит и от того, кто будет участвовать в его создании и возглавлять разработку): иначе выглядели бы интернет-торговля и интернет-банкинг, ведь в исламе существует запрет на ссудные проценты; религиозная полиция могла бы проводить мониторинг онлайн-выступлений и совместно с местными правоохранительными органами наказывать нарушителей; были бы однозначно запрещены сайты для геев и лесбиянок; значительно снизилась бы онлайн-активность за права женщин; был бы установлен пристальный контроль за деятельностью этнических и религиозных меньшинств (более того, она могла быть ограничена или полностью запрещена). В этом сценарии для технически продвинутых местных жителей возможности обойти наложенные ограничения и выйти в глобальный интернет зависели бы от страны, в которой они живут: допустим, у властей Мавритании может не оказаться желания или сил их остановить, а Саудовской Аравии это, скорее всего, удастся. С другой стороны, если мавританское правительство выразит озабоченность тем, что граждане страны обходят цензуру «суннитского интернета», его новые цифровые партнеры наверняка помогут ему возвести более высокую «ограду». В рамках альянсов по коллективному редактированию контента наименее параноидальные страны могли бы позволить своим гражданам иметь доступ к обеим версиям интернета (по аналогии с возможностью пользоваться родительским контролем при просмотре телевизора), делая ставку вместо грубой силы на то, что пользователи предпочтут безопасный и уникальный контент.

В некоторых случаях авторитарные и демократические правительства станут использовать одинаковые подходы к редактированию интернета. Обычно это проявляется в ситуации, когда слабая демократия находится в окружении сильных авторитарных государств, вынуждающих ее идти в виртуальном мире на те же геополитические компромиссы, которые характерны для мира реального. Это тот редкий случай, когда физическая близость может действительно влиять на виртуальный мир. Возьмем Монголию — молодое демократическое государство с открытым интернетом, «зажатое» между Россией и Китаем — двумя крупными странами с

различными, но одинаково основанными на ограничениях интернет-политиками. Бывший монгольский премьер-министр Батболд Сухбаатарын рассказывал нам о желании превратить Монголию в страну с собственным уникальным лицом. Это означает, по его словам, что ей нужно поддерживать хорошие отношения с соседями, не позволяя им вмешиваться в ее внутренние дела. «Мы уважаем сделанный каждой из этих стран выбор собственного пути развития, — сказал он. — Если говорить о Китае, то мы понимаем, что не нужно касаться проблем Тибета, Тайваня и далай-ламы, и тогда они не будут касаться наших проблем. Это же относится и к России, с которой у нас сложились долгосрочные партнерские отношения».

Состояние невмешательства гораздо легче поддерживать в реальном мире. Виртуальное пространство серьезно усложняет эту модель, поскольку контроль над ним принадлежит людям. А люди, симпатизирующие оппозиционным движениям и этническим меньшинствам в Китае и России, могут решить, что Монголия идеально подходит им в качестве плацдарма. Сторонники уйгурских, тибетских и чеченских повстанцев захотят использовать монгольское интернет-пространство в качестве базы, с помощью которой можно проводить мобилизацию активистов, устраивать онлайн-кампании и создавать виртуальные движения. И если это произойдет, монгольское правительство, несомненно, столкнется с давлением со стороны и Китая, и России, и не только дипломатическим, ведь ее национальная инфраструктура не сможет выдержать киберагрессию соседей. Тогда, стремясь смягчить их и сохранить собственный физический и виртуальный суверенитет, Монголия решит выполнить ультиматум Китая или России и начать фильтрацию интернет-контента, связанного с «горячими» темами. В результате такого компромисса проиграют жители Монголии, чья онлайн-свобода будет принесена в жертву эгоистичным иностранным тяжеловесам с крепкими кулаками.

* * *

В ходе «балканизации» интернета сотрудничать будут готовы не все страны, однако конечный результат окажется одинаковым: мешанина национальных интернетов и виртуальных границ. Уже сложилась

тенденция формирования глобальных платформ вроде Facebook и Google, и это означает, что технологии, скорее всего, станут распространяться и дальше, соответственно, в распоряжении людей окажутся инженерные средства для создания собственных онлайн-структур. Без государственного регулирования, замедляющего инновации, развитие этой тенденции пойдет очень быстро. Вначале определить, что находишься в интернете другой страны, окажется практически невозможным, поскольку выглядеть сеть будет везде одинаково, как и сейчас. Пока страны работают над закреплением своей автономии в виртуальном мире, большинство пользователей практически не заметят перемен.

Однако такой гомеостаз не продлится долго. То, что начиналось как всемирная паутина, начнет походить на сам мир, разделенный на части и наполненный взаимоисключающими интересами. В интернете появится необходимость получения некоего аналога виз. Сделать это можно будет быстро, в электронном виде: механизм, обеспечивающий передачу информации в обоих направлениях, запустится после того, как пользователь, желающий попасть в интернет той или иной страны, зарегистрируется и согласится с определенными условиями. Если Китай решит, что для доступа в китайский интернет всем иностранцам нужна виза, резко ослабнут человеческие связи, станет труднее заниматься международным бизнесом и проводить аналитические исследования. А если добавить к этому внутренние ограничения, в XXI веке возникнет аналог известной в семнадцатом столетии японской доктрины *сакоку* («закрытой страны»), направленной на практически полную изоляцию страны.

Некоторые страны захотят ввести визовые требования и в качестве средства мониторинга иностранных посетителей, и для получения дохода: при пересечении виртуальной границы государства будет автоматически списываться небольшая сумма, а за нарушение условий выданной визы в результате определенных действий пользователя (что можно отследить при помощи куки-файлов и иных средств) — взиматься штраф. Виртуальные визы могут появиться в качестве реакции на кибератаки, и, если ваш IP-адрес относится к стране, включенной в черные списки, вы столкнетесь с более тщательной проверкой и более пристальным мониторингом.

А некоторые страны решат сделать красивый жест и откажутся от требования визы, чтобы продемонстрировать свою открытость и побудить другие государства последовать своему примеру. В 2010 году первой страной в мире, на законодательном уровне установившей сетевой нейтралитет, стала Чили. Сегодня почти половина 17-миллионного населения Чили имеет доступ к интернету, государство продолжает совершенствовать технологическую инфраструктуру, и нет никаких сомнений, что подобные публичные жесты побудят и других поддержать дальновидную чилийскую политику в области коммуникаций. Власти стран, население которых только-только начинает выходить в сеть, теперь смогут оценить модель, выбранную Чили, и сравнить ее с иными подходами. В конечном счете возможно подписание соглашений о безвизовом обмене информацией с другими странами, что позволит выстраивать торговые отношения в области интернет-торговли и иных онлайн-платформ. Это был бы действующий в виртуальном пространстве аналог Шенгенского соглашения о безвизовом перемещении по Европе.

Если это случится, то появятся и первые политические интернет-беженцы. Скажем, диссидент, не чувствующий себя свободным в условиях авторитарного регулирования виртуального пространства и не имеющий доступа к иностранным сетям, может решиться на то, чтобы попросить политического убежища в другой стране и обрести виртуальную свободу в рамках ее интернета. А еще может возникнуть возможность получить виртуальное политическое убежище: в этом случае принимающая страна предоставляет диссиденту набор сложных прокси-средств и инструментов обхода цензуры, позволяющих ему связываться с внешним миром. Предоставление виртуального политического убежища может быть первым шагом на пути к «физическому», показателем доверия к кандидату без обязательств по отношению к нему. Оно может также служить аналогом испытательного срока на то время, пока суд будет принимать решение о предоставлении «физического» политического убежища.

Но такой инструмент, как виртуальное политическое убежище, не будет работать в случае развития событий по самому жесткому сценарию — создания альтернативной системы доменных имен (DNS) или агрессивного и повсеместного вмешательства властей в работу

аппаратных и программных средств пользователей с целью реализации государственных интересов. Сегодня в интернете, каким мы его знаем, DNS используются для того, чтобы связывать компьютеры и прочие устройства с соответствующими источниками данных путем преобразования IP-адресов (набора цифр)
в названия сайтов, и наоборот. Надежность интернета основана на том, что все компьютеры и компьютерные сети используют одни и те же домены верхнего уровня (за их перечень отвечает интернет-корпорация по присвоению имен и адресов — ICANN), названия которых появляются в качестве суффиксов веб-адресов: .edu, .com, .net и другие.

Существуют и альтернативные домены верхнего уровня, действующие параллельно с интернетом, но не связанные с ним. Большинство специалистов в области информационных технологий убеждены, что использование альтернативных DNS противоречит тому, чем является интернет и ради чего он создавался, в частности свободному распространению информации. Пока альтернативную систему доменных имен не разработало ни одно правительство мира[23], но, если это кому-то удастся, население будет фактически отключено от глобального интернета и окажется замкнутым в рамках закрытой национальной сети. С технической точки зрения это означает создание подцензурного шлюза между страной и остальным миром, причем обмен данными с внешними пользователями, например в государственных интересах, будет включаться только в ручном режиме.

Для населения такой страны окажутся абсолютно бесполезными все популярные прокси-средства вроде VPN или Tor, поскольку им не с чем будет соединиться. Это явится наиболее радикальной версией известной среди специалистов модели «огороженный сад». В интернете так называется среда, в которой доступ пользователя к онлайн-информации и услугам ограничен. (Это не связано исключительно с цензурой, но имеет глубокие корни в истории интернета: с модели «огороженный сад» начинали свою работу такие интернет-гиганты своего времени, как AOL и CompuServe.) Чтобы добиться полного отсоединения от внешнего мира, правительству

останется лишь настроить маршрутизаторы так, чтобы они не выдавали IP-адреса сайтов (в отличие от DNS, IP-адреса, неразрывно связанных с самими сайтами), в результате чего они окажутся словно на далеком, практически недоступном острове. Какой бы контент ни существовал в такой национальной сети, он будет циркулировать лишь в ее рамках, запертый в замкнутом пространстве, как плавающие пузыри в экранной заставке, а любые попытки связаться извне с пользователем такой сети наткнутся на стену. Одно движение рубильника — и из интернета исчезает целая страна.

> Это не паранойя, как может показаться. Еще в 2011 году появилась первая информация о том, что иранское правительство приступило к созданию «халяльного интернета», а спустя год стало понятно, что его запуск неотвратимо приближается. В декабре 2012 года представители властей объявили о начале работы сервиса Mehr — версии YouTube, содержащего «одобренные государством видеоролики», что стало еще одним подтверждением серьезного отношения режима к этому проекту. Его подробности по-прежнему неизвестны, но, по словам официальных лиц Ирана, на первом этапе национальный «чистый» интернет будет сосуществовать с его глобальной версией (также подвергаемой жесткой цензуре), а затем полностью заменит ее. В результате все «халяльные» сайты окажутся привязанными к определенному блоку IP-адресов, что позволит очень просто отфильтровывать площадки, не входящие в этот блок. Источником контента для национального интранета станут государственные и аффилированные с правительством организации, которые будут или брать его из глобального интернета с последующей очисткой, или создавать самостоятельно. Вся деятельность в сети попадет под пристальное внимание специальных государственных ведомств по контролю за компьютерной инфраструктурой и программным обеспечением (этому иранское правительство придает очень большое значение, судя по введенному в 2012 году запрету на иностранное противовирусное ПО). Глава министерства экономики Ирана в интервью государственному агентству новостей выразил надежду, что халяльный интернет со временем заменит глобальный и в других мусульманских странах (или как минимум тех, чье население говорит на фарси). Нечто подобное обещал построить и Пакистан.

Вполне возможно, что угроза Ирана не более чем мистификация. Как именно власти этой страны собираются реализовать задуманное, неясно — ни с технической, ни с политической точки зрения. Удастся ли им избежать гнева заметной части жителей, уже имеющих доступ к интернету? Некоторые наблюдатели уверены, что полностью отключить Иран от глобального интернета не получится, ведь

экономика страны очень сильно зависит от внешних связей. Другие считают, что, даже если иранским властям и не удастся создать альтернативную систему доменов верхнего уровня, Иран станет пионером в использовании модели двухуровневого интернета, которую захотят внедрить и другие страны с репрессивными режимами. Каким бы путем ни пошел Иран, если его проект увенчается успехом, халяльный интернет перехватит у Великой китайской межсетевой стены первенство в качестве самой экстремальной версии информационной цензуры в истории. Интернет, который мы знаем, изменится навсегда.

Виртуальные союзы

Одновременно с «балканизацией» интернета мы столкнемся с ростом количества виртуальных союзов, основанных на идеологической или политической солидарности их участников, которая толкает и государства, и бизнес к работе в рамках официально созданных альянсов. Такие страны, как Беларусь, Эритрея, Зимбабве и Северная Корея — с репрессивным режимом, мощным культом личности и статусом государства-изгоя, — ничего не потеряют от присоединения к авторитарному киберсоюзу, в рамках которого можно обмениваться стратегиями и инструментами цензуры и мониторинга сети. И если такие страны объединятся вокруг идеи создания виртуального полицейского государства, западным компаниям будет все труднее вести там бизнес, даже законный — это может повлиять на их репутацию. Воспользоваться ситуацией, занять освободившуюся нишу и начать играть более активную роль в рамках союза авторитарных государств смогут конкуренты западных игроков, акционеры которых не столь разборчивы в средствах и которые сами привыкли работать в подобном окружении.

Не случайно 75-процентной долей Koryolink, единственного оператора сотовой связи в Северной Корее, владеет египетская телекоммуникационная компания Orascom, процветавшая во времена долгого правления Хосни Мубарака. (Оставшиеся 25 процентов принадлежат министерству почты и телекоммуникаций Северной Кореи.) Для своих северокорейских абонентов Koryolink является

типичным «огороженным садом» — платформой с сильно ограниченным, самым базовым функционалом. Клиенты оператора не могут совершать и принимать международные звонки, у них нет доступа в интернет. (Некоторые жители Северной Кореи могут выходить в северокорейский интранет, представляющий собой мешанину из устаревшего контента, надерганного чиновниками из интернета.) Практически все местные звонки прослушиваются, а текстовые сообщения отслеживаются, кроме того, журнал The Economist пишет, что сотовая сеть превратилась в платформу распространения официальной пропаганды: ежедневная северокорейская газета Rodong Sinmun рассылает ее абонентам новости в формате SMS. Хотя официально такого требования не существует, людей «поощряют» оплачивать свои телефонные счета в евро (неофициально имеющих обращение в стране), а это непростая задача для большинства жителей Северной Кореи. Но, несмотря на все это, спрос на телефоны настолько велик, что они распространяются по стране с невероятной скоростью: всего за восемнадцать месяцев количество абонентов сотовой связи увеличилось в три раза, к началу 2012 года превысив отметку в миллион человек. Валовая прибыль Koryolink равна 80 процентам, то есть это отличная сделка для Orascom.

Вслед за показательной репрессивной акцией по уничтожению «зеленого движения», предпринятой властями Ирана в 2009 году, западные технологические компании, такие как Ericsson и Nokia Siemens Network (NSN), решили дистанцироваться от правящего режима. Их отсутствием воспользовался китайский телекоммуникационный гигант Huawei, установивший господство над огромным (и подконтрольным государству) иранским мобильным рынком. В то время как его западные предшественники сталкивались с негативной реакцией соотечественников на поставки оборудования иранскому правительству, которое использовало его для слежки за демократическими активистами и давления на них, Huawei активно продвигал свой продукт в благоприятном для авторитарного режима свете. По словам автора одной статьи в The Wall Street Journal, в каталоге компании были без всякого стеснения представлены оборудование для определения местоположения абонента,

предназначенное для правоохранительных органов (и недавно приобретенное крупнейшим иранским оператором сотовой связи), и очень удобная для целей цензуры служба мобильных новостей. Главный местный партнер Huawei, компания Zaeim Electronic Industries Co., также является фаворитом государственных органов, включая Корпус стражей исламской революции и администрацию президента.

Официально Huawei утверждает, что продает Zaeim только «коммерческие продукты для широкого использования», но, по данным The Wall Street Journal, в неофициальных беседах с иранскими чиновниками представители компании объяснили, что имеют огромный опыт в области цензуры информации, полученный в Китае. (Вскоре после этой публикации компания Huawei выпустила пресс-релиз, в котором опровергла некоторые ее положения, а месяц спустя заявила, что «добровольно ограничивает» свои операции в Иране из-за того, что «ситуация становится все более сложной».)

* * *

В качестве ответной меры на такое сотрудничество между авторитарными государствами демократические страны захотят создать аналогичные альянсы и частно-государственные партнерства, чтобы продвигать еще более открытый, еще более свободный с политической, экономической и социальной точки зрения интернет. Одна из целей — сдерживать распространение репрессивных технологий фильтрации и мониторинга в странах с низким, но растущим проникновением интернета. Проявляться это может во множестве различных стратегий, в частности, что мешает заключать двусторонние соглашения о предоставлении помощи на определенных условиях или присваивать вопросам развития интернета высший приоритет при постановке задач для послов? Можно также начать транснациональную кампанию по изменению международной правовой базы, имеющей отношение к свободному выражению своего мнения и программному обеспечению с открытым кодом. Поскольку у этих стран есть общая цель — свободный доступ к информации, свободное выражение своего мнения, прозрачность, — удастся

преодолеть незначительные политические или культурные различия и создать своего рода Ганзейский союз эпохи интернета. Существовавший с тринадцатого по пятнадцатый век в Северной Европе Ганзейский союз — экономический альянс соседних городов-государств — обладал огромной экономической мощью; его современный эквивалент мог бы быть основан на аналогичных принципах взаимопомощи, но в гораздо более крупном, глобальном варианте. Больше альянсы не будут так сильно зависеть от географии, ведь в виртуальном пространстве все находится одинаково близко. Если Уругвай и Бенин вдруг захотят поработать вместе над каким-то проектом, сделать это будет проще, чем когда бы то ни было.

Тема защиты свободы информации и свободы выражения собственного мнения станет новым элементом военной помощи. При подготовке контрактов в спецификацию вместо танков и слезоточивого газа будут включать техническую помощь и инфраструктурную поддержку — впрочем, танки и газ тоже, вероятно, останутся в повестке дня. Технологические компании и разработчики средств компьютерной безопасности станут для двадцать первого века тем, чем была Lockheed Martin для века двадцатого. Такие лидеры отрасли традиционных вооружений, как Northrop Grumman и Raytheon, уже сотрудничают с правительством США в области кибервозможностей. Но волноваться производителям оружия, самолетов и прочих средств военно-промышленного комплекса не стоит — традиционным войскам всегда будут нужны автоматы, танки и вертолеты, — однако в крупных военных бюджетах, значительная доля которых и так уже достается частным компаниям, обязательно найдется строка для технической поддержки.

В рамках новых альянсов приобретут цифровое измерение и проекты по совместному развитию инфраструктуры, и иная иностранная помощь. Суть таких сделок — обмен поддержки из-за рубежа на влияние в будущем — не изменится, а вот ее компоненты поменяются. В каждой развивающейся стране можно в качестве иностранной помощи строить дороги и делать инвестиции в сельское хозяйство, а можно разворачивать оптоволоконную сеть и возводить вышки сотовой связи. В цифровую эпоху современные технологии станут еще одним средством создания альянсов с развивающимися

странами: не стоит недооценивать то, насколько важным окажется для таких стран и их властей зарубежный опыт в области технологий. Ведь спрос на иностранную помощь в деле создания быстрых сетей, поставки современных устройств, организации дешевых и мощных каналов связи может исходить от населения, которое оказывает давление на правительство и вынуждает его соглашаться на условия выделения такой помощи. В общем, какими бы ни были мотивы, развивающиеся страны сделают долгосрочную ставку на современные технологии связи и будут строить дипломатические отношения в соответствии с этим.

Новые альянсы будут выстраиваться также вокруг коммерческих интересов, в частности авторских прав и вопросов интеллектуальной собственности. По мере того как торговля все больше перемещается в интернет, тема авторских прав станет еще одним поводом для дружбы или вражды между странами. Большинство законов об авторских правах и интеллектуальной собственности по-прежнему опираются на понятие физического товара, а относительно того, считать ли кражу или подделку онлайн-продукта (фильмов, музыки и тому подобного контента) эквивалентом кражи их материальной копии, мнения сильно разнятся. В будущем страны станут активнее вступать в судебные баталии по делам, связанным с авторским правом и интеллектуальной собственностью, поскольку на кону окажется благополучие их коммерческого сектора.

Существует множество международных соглашений по вопросам интеллектуальной собственности: Бернская конвенция 1886 года, предусматривающая взаимное признание авторских прав стран, ее подписавших; Соглашение по торговым аспектам прав интеллектуальной собственности 1994 года, в котором установлены минимальные стандарты в этой области для членов Всемирной торговой организации (ВТО); подписанный в 1996 году под эгидой Всемирной организации интеллектуальной собственности (WIPO) Договор по авторскому праву, защищающий от посягательств авторские права на продукты информационных технологий. Вообще законы об авторском праве во всем мире примерно одинаковы. А вот их применение на своей территории каждое государство обеспечивает самостоятельно, и здесь не все проявляют одинаковую настойчивость.

Учитывая легкость, с которой информация пересекает границы, люди, специализирующиеся на продаже пиратских продуктов, обычно находят виртуальные «безопасные гавани» в странах, где власти ведут себя не слишком педантично с точки зрения применения закона.

Наибольшую озабоченность специалистов по интеллектуальной собственности вызывает Китай. Подписав упомянутые конвенции, государство обязано соблюдать те же стандарты, что и остальные страны, включая США. На саммите стран Азиатско-Тихоокеанского экономического сотрудничества (АПЕС), состоявшемся в 2011 году, тогдашний президент Китая Ху Цзиньтао заявил на неофициальной встрече с небольшой группой бизнес-лидеров, что его страна будет «полностью выполнять все законы об интеллектуальной собственности, которые предусмотрены Всемирной торговой организацией, а также учитывать современную западную практику». Мы были на той встрече и видели, с каким скепсисом восприняли представители американского бизнеса это заявление Ху Цзиньтао. И на то есть свои причины: по некоторым оценкам, только в 2009 году американские компании недополучили около $3,5 млрд из-за китайских пиратских музыкальных записей и программного обеспечения; 79% конфискованной в США контрафактного продукта, нарушающего чьи-либо авторские права, было произведено в Китае. Понятно, что эта проблема вызвана не отсутствием законов, а непоследовательным их применением. Формально производство контрафактного продукта и копирование защищенных авторским правом произведений противоречит китайским законам, но на практике правоохранительные органы неохотно преследуют их нарушителей, позволяя им получать свою прибыль. Более того, санкции за нарушение этих законов слишком незначительны и применяются достаточно нерегулярно, чтобы оказаться эффективными в деле пресечения таких действий, а коррупция на местном и региональном уровнях приводит к тому, что официальные лица смотрят на преступления сквозь пальцы.

Естественно, Китай не единственная страна, не желающая или неспособная соблюдать международные нормы по охране интеллектуальной собственности. Подобные проблемы существуют в России, Индии и Пакистане. Израиль и Канаду не назовешь

рассадником пиратства, однако они не в полной мере реализовали стандарты и правила ВТО, что делает их удобной гаванью для интернет-пиратов. А в некоторых странах, надежно защищающих правообладателей, обычно имеются расхождения в интерпретации законов, что выгодно их нарушителям. Так, понятие «законное использование» (термин, принятый в США), или «добросовестное использование» (британский вариант), означающее разрешение ограниченно использовать защищенные авторским правом материалы без согласия правообладателя, в Европейском союзе трактуется гораздо жестче, чем в США или Великобритании.

Виртуальная государственность

Мы часто возвращаемся к тому, что в виртуальном пространстве размер не имеет большого значения. Благодаря информационным технологиям умножаются силы всех сторон, что позволяет даже незначительным игрокам играть непропорционально заметные роли. И эти игроки не обязательно должны быть хорошо известными или иметь официальный статус. Да, мы убеждены, что есть вероятность создания виртуальных государств, и, когда это произойдет, онлайн-карта мира кардинально изменится.

Сегодня в мире существуют сотни активных насильственных и ненасильственных сепаратистских движений, и вряд ли что-то изменится в будущем. Значительная их часть подпитывается убежденностью их сторонников в существовании этнической или религиозной дискриминации. Вскоре мы поговорим о том, как физическая дискриминация и преследование таких групп проявляются в сети — в иной форме, но сохранив свою суть. В реальном мире представители преследуемых групп нередко становятся жертвами избирательного применения законов и необоснованных задержаний, внесудебных казней, отсутствия права на справедливый суд и всевозможных ограничений их гражданских прав и человеческих свобод. Большинство таких действий найдут свое отражение в интернете, причем в значительной степени этому будут способствовать технологии, позволяющие режиму вычислять представителей

непокорного меньшинства, следить за ними и оказывать на них давление.

Группы, преследуемые в реальном мире и в виртуальном пространстве и не имеющие формальной государственности, возможно, захотят ее имитировать. И хотя объявление виртуального суверенитета не столь законно и действенно, как реальная независимость, возможность сделать это может оказаться при благоприятном исходе серьезным шагом в сторону официального признания, а при неблагоприятном — привести к эскалации противостояния, которая подтолкнет обе стороны к полномасштабному гражданскому конфликту. Курдское население в Иране, Турции, Сирии и Ираке — четырех странах с наибольшей концентрацией курдов — может построить Курдский интернет, чтобы обеспечить себе виртуальную независимость. Иракский Курдистан уже получил некое подобие автономности, так что этот проект может начаться оттуда. Курды, например, создадут домен верхнего уровня .krd (с адресами вроде www.yahoo.com.krd), где krd означает «Курдистан», зарегистрировав его в нейтральной или союзной стране и там же разместив серверы. И потом двинутся дальше.

Виртуальная государственность может оказаться чем-то гораздо большим, чем красивый жест и доменное имя. Курдское онлайн-присутствие будет заметнее при условии реализации специальных проектов. Если приложить достаточные усилия, Курдский интернет вполне способен стать достойным соперником сетей других стран — естественно, на курдском языке. Инженеры-курды и другие сочувствующие курдам разработчики создадут для него веб-приложения, сайты и базы данных, которые не только поддержат курдское движение, но и облегчат выполнение стоящих перед ним задач. В виртуальном курдском сообществе будут проводиться выборы и создаваться министерства для доставки товаров первой необходимости. Можно даже ввести уникальную виртуальную валюту. Виртуальный министр информации станет управлять потоками данных, которыми обмениваются «граждане» Курдистана. Министр внутренних дел сосредоточится на обеспечении безопасности виртуального государства и защите его от кибератак. Министр иностранных дел станет налаживать дипломатические отношения с

«настоящими» странами; министр экономики и торговли — продвигать идею интернет-торговли между курдскими сообществами и внешними заинтересованными в этом сторонами.

Сепаратисты, стремящиеся к собственной государственности в реальном мире, обычно встречают жесткое сопротивление со стороны властей той страны, в которой живут, и с таким же противостоянием они столкнутся в своих онлайн-маневрах. Создание виртуальной Чечни способно укрепить этническую и политическую солидарность ее сторонников на Кавказе, но, несомненно, ухудшит отношения с правительством России, которое посчитает такой шаг нарушением суверенитета страны. И тогда на виртуальную провокацию Кремль может ответить физическим нападением, направив в Чечню танки и солдат для подавления «бунта».

В ситуации с курдами, живущими на территории нескольких стран, риск еще выше, поскольку кампания по объявлению виртуального суверенитета Курдистана может встретить сопротивление соседних стран, даже тех, где курдов нет: их напугает возможность дестабилизации ситуации в регионе. Они не пожалеют средств, чтобы разрушить виртуальные институты Курдистана при помощи компьютерного давления и шпионажа, кибератак, кампаний по распространению дезинформации и клеветы. На население обрушатся наказания. Властям, естественно, сыграют на руку огромные объемы данных, созданные пользователями: найти тех, кто занимается проектом виртуальной государственности или поддерживает его, не составит никакого труда. У очень небольшого количества сепаратистских движений хватит ресурсов и международной поддержки, чтобы устоять против столь мощной атаки.

Провозглашение виртуальной независимости будет считаться государственной изменой, причем не только в неспокойных регионах, а вообще в мире: это слишком опасный путь, чтобы оставлять его открытым. Ведь сама идея создания виртуальных институтов может придать новые силы сепаратистским группам, пытающимся, но неспособным добиться заметных результатов при помощи насильственных методов, таким как баскские сепаратисты в Испании, абхазские националисты в Грузии или Фронт исламского освобождения Моро в Филиппинах. А один неудачный или

неправильный шаг в состоянии привести к провалу эксперимента в целом. Если, к примеру, убежденные сторонники суверенитета Техаса выступят с инициативой создания виртуальной Республики Техас, но столкнутся с насмешками, на какое-то время может быть похоронена сама идея виртуальной государственности. Пока мы не знаем, насколько успешными окажутся виртуальные государства (да и, в конце концов, каковы критерии их успеха?), но сама привлекательность этой концепции уже говорит в пользу постепенного ослабления могущества традиционного государства в цифровую эпоху.

Цифровые провокации и кибервойны

Картина будущего стран в цифровую эпоху останется неполной, если мы не рассмотрим худшее из того, что они могут сделать в виртуальном пространстве, — развязывание кибервойн. Кибероружие — понятие не новое, хотя и не все его характеристики точно определены. Специалисты по компьютерной безопасности продолжают спорить о том, насколько велика угроза, в чем она выражается и что, собственно, представляют собой военные действия в ходе кибервойны. В нашей книге мы будем использовать определение кибероружия, данное бывшим руководителем американского ведомства по борьбе с терроризмом Ричардом Кларком: это действия государства по проникновению в компьютеры или компьютерные сети другого государства с целью нанесения ущерба или убытков[24].

Мы уже говорили о том, что кибератаки, в том числе электронный шпионаж, саботаж, проникновение в компьютерные сети и другие подобные действия, очень трудно отслеживать и при этом они способны нанести огромный ущерб. Использовать тактику кибервойн могут и террористические группы, и власти страны, хотя последние больше концентрируются на сборе информации, чем на явно деструктивных действиях. Для государств кибервойна имеет в первую очередь разведывательное значение, даже если применяются те же средства, которые в руках независимых игроков служат для нанесения ущерба. Кибератаки стран друг на друга станут включать в себя весь набор традиционных методов разведки: кражу коммерческих секретов,

получение несанкционированного доступа к секретной информации, проникновение в государственные компьютерные системы, распространение дезинформации. Многие специалисты в корне не согласны с нашей позицией, считая, что страны будут стремиться уничтожить своих врагов с помощью таких тяжеловесных методов, как дистанционное отключение электричества или обрушение фондовых рынков. В октябре 2012 года министр обороны США Леон Панетта выступил с предупреждением: «Агрессивные нации... могут использовать компьютерные инструменты такого рода для получения контроля над критически важными диспетчерскими системами. И после этого вызвать крушение пассажирского поезда или, что еще хуже, столкновение его с поездом, везущим химикаты. Они могут отравить водопровод в крупном городе или отключить электричество на значительной территории страны». Мы же смотрим в будущее оптимистично (по крайней мере в этом вопросе) и считаем, что эскалация конфликта такого рода возможна, но маловероятна: та страна, которая первой начнет подобные действия, сама превратится в мишень, а также продемонстрирует, что быть разборчивыми в средствах следует даже самым непредсказуемым режимам.

Не будет преувеличением сказать, что мы уже живем в эпоху кибервойн с участием государств, даже если большинство из нас об этом и не подозревают. Прямо сейчас спецслужбы какой-то из стран взламывают базы данных вашего правительства, стирают информацию на его серверах или прослушивают его переговоры. Внешнему наблюдателю нынешняя стадия кибервойны может показаться довольно мягкой (а кто-то вообще решит, что это никакая не «война», так как не соответствует классическому высказыванию Клаузевица: «Война есть не что иное, как продолжение государственной политики иными средствами»). Работающие на правительство инженеры могут пытаться проникнуть в корпоративные и государственные информационные системы других стран или отключить их, но в конце концов никого ведь не убьют и не ранят. Мы так мало сталкиваемся с влиянием этих кибервойн на обычную жизнь, что для непосвященных кибератака представляется скорее дискомфортом, чем угрозой — чем-то вроде обычной простуды.

Но горе тому, кто недооценивает угрозу кибервойны! Пусть оправданы не все связанные с ней страхи, но риск вполне реален. Кибератаки с каждым годом происходят все чаще и планируются все точнее. Все более тесное переплетение наших жизней с компьютерными информационными системами делает нас уязвимее с каждым кликом. А поскольку в ближайшем будущем доступ к интернету будут получать все новые и новые страны, эта уязвимость только усугубится.

Кибератаки могут стать идеальным оружием государства: мощным, гибким и анонимным. Такие тактики, как взлом сетей, распространение компьютерных червей и троянов, другие формы виртуального шпионажа позволяют странам достичь большего, чем традиционные средства вооружения или разведывательные операции. Они почти не оставляют следов, обеспечивают эффективным камуфляжем того, кто их совершает, и серьезно ограничивают возможности ответных мер со стороны жертв. Даже если и удается проследить источник нападения до региона или города, определить ответственных за него практически невозможно. А как назначить наказание, если не доказана вина? По мнению Крэйга Манди, директора по исследованиям и стратегии компании Microsoft и ведущего специалиста по интернет-безопасности, невозможность установления авторства — очень хорошо знакомая нам проблема — означает, что эта война ведется в темноте, потому что «намного труднее понять, кто же нанес вам удар». Манди называет тактику кибершпионажа «оружием массового разрушения». «Распространяться такие конфликты будут намного быстрее, но гораздо незаметнее, чем война в традиционном понимании», — говорит он.

В виртуальном мире государства будут позволять себе то, что считалось бы слишком провокационным в мире реальном, считая допустимым эскалацию онлайн-конфликтов при внешне спокойной офлайн-обстановке. Возможность сохранить практически полную анонимность делает кибератаки крайне привлекательными для тех стран, которые не хотят выглядеть слишком агрессивными, но при этом стремятся ослабить своих врагов. До тех пор пока технические специалисты не начнут определять источник кибератак, а закон не сможет призывать их инициаторов к ответу, все новые страны будут

вступать в игру, которую мы наблюдаем уже сегодня. Вскоре начнут проводить свои кибератаки, как минимум для пробы, целые группы стран в Латинской Америке, Юго-Восточной Азии и на Ближнем Востоке, уже имеющие и доступ в сеть, и технические возможности для кибервойны. Не нужно обладать выдающимися способностями, чтобы получить необходимые инструменты (это смогут сделать даже местные инженеры или хакеры).

Чтобы лучше проиллюстрировать вселенную кибервойн, рассмотрим несколько примеров. Наверное, самым знаменитым компьютерным «червем» стал Stuxnet, обнаруженный в 2010 году и считавшийся наиболее сложным образцом вредоносного программного обеспечения из когда-либо созданных, пока выявленный в 2012 году вирус Flame не отобрал у него этот титул. Целью Stuxnet было специализированное программное обеспечение определенного типа, работавшее под Windows, и он смог успешно проникнуть в систему мониторинга иранского завода по обогащению ядерного топлива в Натанце, одновременно с этим отключив систему оповещения об опасности, после чего заставил газовые центрифуги резко изменить скорость вращения, пока они не разрушились. Поскольку иранская сеть не имела выхода в интернет, червь мог попасть в нее только напрямую. Возможно, какой-нибудь служащий завода по незнанию пронес его на USB-накопителе. Позже уязвимости Windows были устранены, но иранской ядерной программе уже был нанесен определенный ущерб, что признал даже президент страны Махмуд Ахмадинежад.

Первые попытки выявить создателей червя оказались безуспешными, хотя большинство специалистов считали, что, учитывая его цель и степень сложности, здесь не обошлось без государственной поддержки. Помимо прочего, специалисты по компьютерной безопасности, изучившие код червя (это стало возможным потому, что он «вырвался на волю», то есть за пределы завода в Натанце), заметили, что в нем содержатся специфические ссылки на даты и библейские истории, очень символичные для Израиля. (Их оппоненты считали, что эти подсказки слишком очевидны и поэтому представляют собой ложный след.) Использованные для создания червя ресурсы также указывали на

участие государства: эксперты считали, что его писали не менее тридцати человек на протяжении нескольких месяцев. Кроме того, было использовано беспрецедентное количество уязвимостей «нулевого дня», то есть возможностей для нападения («дыр» в безопасности), неизвестных разработчику программного обеспечения (в данном случае компании Microsoft) на момент атаки, у которого, соответственно, есть «ноль» дней на подготовку к ней. Обнаружение уязвимости «нулевого дня» считается довольно редким событием, и такую информацию можно продать на черном рынке за сотни тысяч долларов, поэтому специалисты по безопасности были шокированы тем, что первый вариант Stuxnet использовал *пять* таких уязвимостей!

В июне 2012 года удалось выяснить, что за созданием червя Stuxnet стояло даже не одно, а два государства. Анонимный источник в администрации президента Обамы подтвердил журналисту New York Times Дэвиду Сангеру, что Stuxnet был совместным проектом США и Израиля, направленным на срыв иранской программы создания ядерного оружия[25].Начат он был еще при Джордже Буше, назывался «Олимпийские игры», затем перешел «по наследству» к следующему президенту. Как оказалось, Барак Обама лично санкционировал применение этого кибероружия.

После завершения разработки и тестирования червя на действующей модели завода в Натанце, построенной в США, когда выяснилось, что он действительно способен разрушать центрифуги, администрация дала согласие на его запуск. Американские официальные лица не отрицают значимость этого события[26]. Как сказал Сангеру бывший директор ЦРУ Майкл Хэйден, «прежде кибератаки ограничивались вредом для компьютеров. Это первое крупное нападение, в ходе которого кибероружие привело к физическим разрушениям. Кто-то перешел Рубикон».

Спустя два года обнаружил себя вирус Flame. Согласно первым сообщениям специалистов по безопасности, он не был связан со Stuxnet: Flame был намного больше, его написали на другом языке программирования, он работал по-другому, скрытно собирая данные вместо того, чтобы разрушать центрифуги. А еще его создали минимум на четыре года раньше, чем Stuxnet (это выяснилось в

результате анализа). По словам Сангера, официальные лица США отрицали, что Flame являлся частью проекта «Олимпийские игры». Но уже через месяц после того, как общественность узнала об этом новом кибероружии, специалисты из «Лаборатории Касперского» — признанной во всем мире компании, специализирующейся на компьютерной безопасности, — пришли к выводу, что две команды, создавшие Stuxnet и Flame, сотрудничали как минимум на ранней стадии проекта. В первой версии Stuxnet удалось обнаружить один модуль под названием Resource 207 с кодом, аналогичным коду Flame. «Похоже, что платформа Flame послужила стартовой площадкой для проекта Stuxnet, — заявил руководитель исследовательской группы “Лаборатории Касперского”. — Но работа над ними шла отдельно, возможно, потому, что код Stuxnet был достаточно зрелым для того, чтобы выпускать его “на волю”. Сейчас мы на 100% уверены, что группы Stuxnet и Flame работали вместе».

Хотя случаи применения Stuxnet, Flame и других образцов кибероружия, связанных с США и Израилем, являются самыми сложными из инициированных какими-либо государствами примерами военных действий в виртуальном пространстве, правительства других стран мира также используют различные методы ведения кибервойны. Эти атаки не обязательно связаны с какими-то важными геополитическими целями — иногда достаточно желания задеть соперника.

На фоне дипломатических баталий, развернувшихся в 2007 году после заявления правительства Эстонии о планах убрать советский мемориал, посвященный Великой Отечественной войне, последовала неожиданная DDoS-атака (атака типа «отказ в обслуживании») на множество известных эстонских сайтов, в том числе банков, газет и государственных органов. Эстонию часто называют самой цифровой страной на земле, поскольку практически все повседневные задачи государства (и почти всех его граждан) решаются при помощи онлайн-сервисов, включая интернет-правительство, интернет-выборы, интернет-банкинг и мобильный паркинг (последнее означает, что водители могут оплатить парковку при помощи мобильного устройства). И вот страна, давшая миру Skype, внезапно оказалась парализованной группой хакеров. Затем все заработало, и эстонцы немедленно заподозрили своего соседа Россию. Министр иностранных дел Эстонии Урмас Паэт прямо обвинил во всем Кремль, но доказательств не было. Эксперты НАТО и Евросоюза не смогли найти

свидетельства причастности к инциденту российских властей (которые, в свою очередь, отвергли все обвинения).

Возникшие вопросы: было ли это актом кибервойны? возможно ли, что Кремль не отдавал прямых приказов на эти действия, но «благословил» сделавших это хакеров? — остаются без ответа. Поскольку не удается установить источник, жертвы кибератак мало что могут предпринять, а преступники остаются безнаказанными даже в случае очень обоснованных подозрений.

Через год после нападения на Эстонию при помощи DDoS-атак были выведены из строя сайты министерства обороны и правительства Грузии, и в этом снова обвинили — вы угадали! — Россию. В следующем году хакеры из России выбрали в качестве мишени киргизских интернет-провайдеров, на несколько дней отключив 80% абонентов широкополосного доступа страны. Кто-то считает, что целью атаки было ослабление позиций киргизской оппозиционной партии, которая довольно активно вела себя в интернете, кто-то — что причиной стала сорвавшаяся инвестиционная сделка, в рамках которой Россия пыталась заставить Киргизию закрыть расположенную на ее территории американскую военную базу. Можно вспомнить происходившие в последние несколько лет китайские кибератаки на Google и другие американские компании. Электронный промышленный шпионаж превратился в бурно развивающуюся подкатегорию кибероружия. Это сравнительно новое явление в будущем окажет серьезное влияние на отношения между странами, а также на национальные экономики. В Google часто замечают атаки на системы компании со стороны неизвестных киберпротивников, поэтому компания тратит много времени и энергии на создание самой безопасной сети и организацию максимальной защиты своих пользователей.

В конце 2009 года специалисты Google обнаружили подозрительный трафик в своей сети и начали наблюдать за происходящим. (Как и в случае большинства кибератак, специалистам по компьютерной безопасности гораздо правильнее на какое-то время оставить открытым взломанный канал, с тем чтобы проследить за взломщиками, нежели немедленно его закрыть.) Оказалось, что речь идет об

очень изобретательном и профессиональном нападении на интеллектуальную собственность Google из Китая.

В ходе проведенного компанией расследования было собрано достаточно доказательств того, что за атакой на Google стоит правительство Китая или его агенты. Помимо технических подсказок, аргументом явилось то, что одной из целей нападавших был доступ к аккаунтам электронной почты Gmail китайских правозащитников, а также американских и европейских защитников прав человека в Китае (в целом им это не удалось). Именно эта атака, задевшая не только Google, но и десятки других компаний, акции которых обращаются на бирже, оказалась одним из основных факторов, побудивших Google принять решение об изменении своего подхода к бизнесу в Китае: компания прекратила свою деятельность в этой стране, перестала заниматься самоцензурой контента в китайском сегменте интернета и начала перенаправлять все поисковые запросы на свой гонконгский сайт.

Сегодня возможности проведения крупномасштабных кибератак есть у очень небольшого количества стран (остальных сдерживает отсутствие быстрых каналов связи и технических талантов), но в будущем в эти действия окажутся втянутыми десятки новых участников, как нападающих, так и обороняющихся. Многие специалисты считают, что положено начало новой гонке вооружений, в ходе которой США, Китай, Россия, Израиль, Иран и другие страны активно инвестируют в наращивание своих технологических возможностей и поддержание высокой конкурентоспособности. В 2009 году, примерно в то же время, когда Пентагон выпустил директиву о создании Кибернетического командования США (USCybercom), министр обороны Роберт Гейтс провозгласил киберпространство «пятой областью» военных операций наряду с сушей, морем, воздухом и космосом. Возможно, в будущем в армии появится виртуальный аналог элитного спецподразделения «Дельта», а в состав новой администрации войдет министерство кибервойн. Если это кажется вам слишком сильной натяжкой, вспомните о создании министерства национальной безопасности в качестве реакции на теракты 11 сентября. Все, что нужно, — это один серьезный случай национального масштаба, и в распоряжении правительства окажутся огромные ресурсы и мандат на все необходимые действия. Помните, как в результате террористических актов ирландских сепаратистов в каждом уголке Лондона появились камеры видеонаблюдения, что

одобрила большая часть его жителей? Конечно, были люди, недовольные тем, что каждый их шаг на улице будет записан и сохранен, но в моменты, когда нация в опасности, мнение «ястребов» всегда превалирует над мнением «голубей». Посткризисные меры безопасности традиционно обходятся чрезвычайно дорого, поскольку власти вынуждены действовать быстро и совершать дополнительные усилия, чтобы ослабить тревогу населения. Некоторые эксперты оценивают годовой бюджет нового «киберпромышленного комплекса» в диапазоне $80–150 млрд.

Государства с мощным технологическим сектором экономики, вроде США, обладают достаточным человеческим капиталом для создания своего виртуального оружия «на месте». Но что делать тем странам, чей технический потенциал недостаточен? Мы уже упоминали о сделках типа «сырье в обмен на технологии» — это инструмент правящих режимов, стремящихся построить государства тотального контроля. Есть все причины полагать, что такого типа обмен будет эффективным и в случае, когда внимание таких государств переключится на внешних врагов. Страны Африки, Латинской Америки и Центральной Азии подберут себе партнеров, чьи инвестиции в развитие технологий смогут дополнить их недостаточно развитую инфраструктуру. Крупнейшими поставщиками станут Китай и США, но, разумеется, не они одни: за возможность предложить странам-покупателям товары и услуги будут конкурировать правительственные агентства и частные компании всего мира. Большинство сделок такого рода будут заключаться без ведома населения обеих стран, что позднее, когда партнерство распадется, приведет к некоторым неудобным для властей вопросам. После разгрома здания египетской службы государственной безопасности в ходе революции 2011 года достоянием гласности стали множество скандальных контрактов с частными поставщиками, в том числе загадочной британской компанией, продававшей режиму Мубарака шпионское программное обеспечение.

Странам, которые стремятся обладать возможностями для ведения кибервойн, нужно принять важное решение о выборе страны-поставщика, а также согласиться с тем, что придется оказаться в ее «сфере онлайн-влияния». А страны-поставщики будут жестко

настаивать на получении плацдармов в развивающихся странах, поскольку инвестиции всегда обмениваются на влияние. Чрезвычайно успешно ведет себя в деле завоевания плацдарма в Африке Китай, обменивая техническую помощь и реализацию крупных инфраструктурных проектов на доступ к ресурсам и потребительским рынкам, в немалой степени благодаря китайской позиции невмешательства и низким ценам. К кому же в таком случае обратятся эти страны, когда решат приступить к созданию своих киберарсеналов?

И действительно, мы уже видим признаки таких инвестиций под «прикрытием» проектов научно-технического развития. Одним из крупнейших получателей прямой иностранной помощи из Китая является Танзания, бывшая социалистическая страна.

> В 2007 году китайскую телекоммуникационную компанию привлекли к прокладке около 10 000 километров оптоволоконного кабеля. Несколько лет спустя китайская горнорудная компания Sichuan Hongda объявила о заключении с Танзанией контракта на добычу угля и железной руды в южных районах страны, объем сделки составил $3 млрд. Вскоре после этого представитель правительства Танзании заявил о том, что подписано соглашение с Китаем на сумму $1 млрд о предоставлении кредита на строительство газопровода для природного газа. Подобный симбиоз возникает во всех частях континента: правительства африканских стран налаживают отношения с крупными китайскими компаниями, большинство которых принадлежат государству. (На долю государственных компаний в Китае приходится 80% капитализации фондового рынка.) Кредит в размере $150 млн на создание проекта «электронного правительства» Ганы с участием китайской компании Huawei, исследовательский госпиталь в Кении, «Африканский техноград» в Хартуме — все это делается в рамках Форума китайско-африканского сотрудничества (FOCAC), организации, учрежденной в 2000 году с целью развития партнерства между Китаем и африканскими странами.

В будущем сверхдержавы — поставщики высокотехнологичной продукции будут стремиться к формированию собственных сфер онлайн-влияния на базе уникальных протоколов и продуктов. Эти технологии сформируют электронный «скелет» общества страны-покупателя, в результате чего она окажется зависимой от критически важной инфраструктуры, которую строит, обслуживает и контролирует исключительно эта сверхдержава. Сегодня в мире существует четыре

основных производителя телекоммуникационного оборудования: шведская Ericsson, китайская Huawei, французская Alcatel-Lucent и американская Cisco. Естественно, что Китай получает выгоду от использования значительной частью мира его оборудования и программного обеспечения, ведь именно китайское правительство определяет деятельность национальных компаний. Там, где получает долю рынка Huawei, растут влияние и глубина проникновения самого Китая. Ericsson и Cisco в меньшей степени контролируются властями их стран, но со временем их коммерческие и национальные интересы также будут согласованы и противопоставлены китайским (скажем, за исключением торговли с авторитарными режимами), и эти компании начнут координировать свои действия со своими правительствами и на дипломатическом, и на техническом уровне.

По своей природе эти сферы онлайн-влияния будут одновременно и техническими, и дипломатическими. Хотя в практическом плане отношения на столь высоком уровне не затрагивают повседневную жизнь людей, используемая в стране технология и то, к чьей сфере влияния она относится, могут иметь значение в случае каких-либо серьезных событий (например, восстания, организованного в том числе с помощью мобильных телефонов). Технологические компании вместе со своими продуктами экспортируют и свои ценности, поэтому-то столь исключительно важно, кто именно закладывает фундамент сетевой инфраструктуры. В мире существуют различные подходы к открытым и закрытым системам, разногласия по поводу роли правительства, разные подходы к его подотчетности перед обществом. Если власти какой-то страны, являющейся «клиентом» Китая, используют приобретенную у него технологию для преследования меньшинств на своей территории, США мало что смогут сделать: правовые нормы окажутся бессильными. Так что у этой коммерческой битвы возможны серьезные последствия с точки зрения безопасности.

Новая холодная война

Логическим следствием того, что все больше стран выходят в виртуальное пространство, создают или приобретают средства для

проведения кибератак и действуют в условиях существования конкурирующих сфер онлайн-влияния, станут постоянные, никогда не прекращающиеся боевые действия в ходе кибервойн низкой интенсивности. Крупные страны атакуют другие крупные страны, сами или через посредников; развивающиеся государства используют свои новые возможности для мести за старые обиды; мелкие страны попытаются добиться непропорционально большого влияния, не опасаясь возмездия, поскольку проследить источник их атак будет невозможно. Поскольку большинство таких атак представляют собой незаметный и неторопливый сбор информации, они не предполагают силовых ответных действий. Благодаря этому конфликты могут тлеть годами. А сверхдержавы создадут виртуальные армии, «размещая» их в сферах своего влияния и при необходимости используя посредников, чтобы дистанцироваться от них и без помех создавать червей, вирусы, изощренные средства взлома и другие инструменты онлайн-шпионажа для получения коммерческой и политической выгоды.

Это уже называют «новой холодной войной», в ходе которой крупнейшие страны мира окажутся вовлеченными в медленно кипящий конфликт в одном из измерений, в то время как в другом они будут как ни в чем не бывало успешно развивать экономические и политические взаимоотношения. Но в отличие от своей предшественницы холодная кибервойна не ограничится двусторонним противостоянием — скорее, речь будет идти о многополярном конфликте с участием высокоразвитых в техническом смысле государств, включая Иран, Израиль и Россию. Четкие идеологические линии раздела — это отношение к свободе самовыражения, открытости данных и либерализму. Как уже было отмечено, такое противостояние почти не отразится на отношениях между государствами в реальном мире, поскольку никто из его участников не захочет их ухудшения.

В ходе холодной кибервойны будут использоваться некоторые классические атрибуты ее исторического предшественника, в частности шпионаж, поскольку правительства считают свое кибероружие дополнением к спецслужбам. На смену «жучкам», шпионским тайникам и прочим средствам из арсенала профессиональных разведчиков придут компьютерные черви,

«клавиатурные шпионы», программы для отслеживания местоположения объекта и прочее шпионское программное обеспечение. Возможно, поскольку информацию будут добывать не у людей, а с жестких дисков, и снизятся риски для традиционных активов и их владельцев, но при этом к старым проблемам добавятся новые: целенаправленное распространение дезинформации и легкость, с которой даже самые сложные компьютеры делятся секретами, превосходя в этом людей.

В новую цифровую эпоху возродится еще один атрибут холодной войны — действия через посредников. С одной стороны, это может проявляться в виде альянсов между различными государствами, созданных с позитивными целями, например для борьбы с опасными незаконными группами, когда невозможность установить авторство атакующего позволяет обеспечить его политическое прикрытие. Скажем, США могут скрытно финансировать подготовку или инструктировать специалистов из латиноамериканских стран, которые по заданию своих правительств совершают электронные атаки на компьютерные сети наркокартелей. С другой стороны, ведение войны через посредников способно привести к еще большей неразберихе и ложным обвинениям, которые отдельные страны будут использовать в своих политических или экономических интересах.

Как и в случае с первой холодной войной, которая практически никак не влияла на жизнь среднего человека: о ней не знали, прямого вреда от нее не чувствовали; незаметность холодной кибервойны пагубно повлияет на то, как страны оценивают риски своих действий. Правительства с большими амбициями и недостаточным опытом обращения с кибероружием могут зайти слишком далеко и невольно начать конфликт, который нанесет ущерб населению их стран. Не исключено, что снова сложится доктрина гарантированного взаимного уничтожения, которая стабилизирует ситуацию, но из-за многополярности политического пейзажа некоторая неустойчивость системы будет сохраняться всегда.

Еще важнее то, что в условиях новой холодной войны возрастает вероятность ошибки. Пока ее участники научатся использовать оказавшиеся в их распоряжении новые мощные инструменты, с новой силой проявятся и характерные для эпохи холодной войны ошибки

восприятия, выбора правильного направления и последовательности шагов. А учитывая, что в случае кибератак ситуация еще более запутана, чем обычно, закончиться все может даже плачевнее, чем во времена холодной войны — вплоть до изменения курса боевых ракет. Ошибки могут делать власти страны, решая, кого атаковать и как; жертвы нападения, нанося в панике или в ярости ответный удар по невиновному; инженеры в процессе разработки чрезвычайно сложных компьютерных программ.

Учитывая столь высокую техническую сложность нового оружия, не будет преувеличением предположить, что какой-нибудь негодяй сознательно оставит в программе лазейку, с помощью которой можно обойти защитные механизмы и дистанционно управлять ею, и эта лазейка останется незамеченной до тех пор, пока он не решит воспользоваться ею. Или, скажем, некий пользователь компьютера, зараженного сложным вирусом, нечаянно использует вредоносную программу не так, как предполагали ее разработчики, и, вместо того чтобы красть информацию о фондовой бирже страны, вирус полностью блокирует ее работу. Или будет выявлена опасная программа, в код которой внедрены ложные «флажки» (цифровые аналоги приманки), и страна, ставшая мишенью атаки, примет решение нанести ответный удар по мнимому агрессору.

Уже известны примеры того, как невозможность установления авторства кибератак приводит к ошибкам на государственном уровне. В 2009 году в результате трех волн DDoS-атак были выведены из строя крупные правительственные сайты в США и Южной Корее. Когда специалисты по компьютерной безопасности изучили ситуацию, то обнаружили файлы на корейском языке и другие признаки, явно свидетельствующие о том, что сеть участвовавших в атаке компьютеров, или ботнетов, была родом из Северной Кореи. В Сеуле официальные лица явно обвинили в произошедшем Пхеньян, история получила соответствующее освещение в американских СМИ, а один видный республиканский конгрессмен потребовал от Барака Обамы «наказать» северокорейцев.

На самом деле *доказать*, откуда была совершена атака, не смог никто. Спустя год аналитики пришли к выводу, что никаких признаков причастности к нападению правительства Северной Кореи или любой другой страны найти не удалось. Один из вьетнамских специалистов заявил, что атака началась в Великобритании, хотя в Южной Корее продолжали настаивать на виновности северокорейского министерства связи. Некоторые наблюдатели даже считают,

что весь эпизод срежиссирован южнокорейскими властями или политическими активистами, попытавшимися спровоцировать США на силовые действия против Северной Кореи.

Те атаки оказались по большому счету неэффективными и довольно простыми: какие-либо данные потеряны не были, а сам DDoS-метод считается примитивным инструментом. Этим отчасти и объясняется отсутствие эскалации конфликта. Но что будет, когда все большее количество стран смогут создавать компьютерных червей вроде Stuxnet или еще более сложное кибероружие? В какой момент кибератака превратится в военные действия? И как реагировать жертве, если агрессор практически всегда скрывает свои следы? На все эти вопросы придется ответить политикам всего мира — и быстрее, чем они предполагают. Какие-то решения этих проблем уже известны, но большинство вариантов, например заключение международных соглашений о борьбе с кибератаками, потребуют выделения значительных инвестиций и честного диалога о том, что мы можем, а чего не можем контролировать.

Вряд ли поводом для этого диалога станет применение кибероружия против другого государства. Вероятнее, это будет корпоративный шпионаж при поддержке на государственном уровне. Власти могут скрывать негативные последствия атак на правительственные корпоративные сети, но, если мишенями нападения окажутся компании, особенно в случае несанкционированного доступа к персональным данным пользователей или клиентов, нападение привлечет больше внимания и затронет интересы большего количества людей. Кроме того, глобализация делает электронный корпоративный шпионаж гораздо более плодотворным предприятием. Сейчас компании стремятся выйти на новые рынки, и инсайдерская информация о деятельности и планах конкурентов помогает их местным подразделениям обеспечить себе преимущество и получить выгодные контракты. Чтобы понять, что это значит для будущего, нам снова придется посмотреть на Китай.

Именно Китай проводит наиболее изощренные и многочисленные кибератаки против иностранных компаний, хотя, естественно, он не одинок в этом. Готовность властей Китая заниматься корпоративным

шпионажем и поощрение к этому же национальных компаний привели к резко возросшей уязвимости иностранных корпораций, причем не только тех, которые хотят работать в Китае. Уже упоминавшаяся китайская кибератака на Google и десятки других в 2009 году не отдельные случаи: только за последние несколько лет в ходе кампании промышленного шпионажа жертвами китайских агентов стали американские компании, производящие все: от полупроводников и автомобилей до реактивных технологий. (Конечно, корпоративный шпионаж — явление не новое. В XIX веке английская Ост-Индская компания наняла одного шотландского ботаника для того, чтобы тот, притворившись китайским торговцем, тайно вывез из Китая в Индию саженцы и выяснил секреты ухода за ними, с чем он успешно справился, положив тем самым конец чайной монополии Китая.)

В цифровую эпоху значительная часть операций по промышленному шпионажу может быть проведена дистанционно и практически анонимно. Скоро мы перейдем к автоматизированным войнам — критически важному технологическому новшеству, которое повлияет на многие аспекты нашего будущего мира. Мы живем во времена экспансии, и, поскольку Китай и другие потенциальные сверхдержавы стремятся расширить свое экономическое присутствие по всему миру, электронный корпоративный шпионаж серьезно повышает возможности для их роста. Взлом электронной почты и компьютерных сетей конкурентов — неважно, официально спонсируемый государством или просто поощряемый им, — несомненно, обеспечит незаслуженные рыночные преимущества. Несколько руководителей крупных американских корпораций на условиях конфиденциальности рассказывали нам о неудавшихся сделках в Африке и на других развивающихся рынках, причем они обвиняли в этом китайских шпионов, укравших конфиденциальную информацию (которая затем использовалась для того, чтобы расстроить договоренности или перехватить выгодные контракты).

Анализ инцидентов корпоративного шпионажа Китая против США показывает, что в настоящее время чаще всего речь идет об использовании его властями услуг разных авантюристов, а не о прямом участии государства. Так, одна китайская супружеская пара из Мичигана украла коммерческую информацию, имеющую отношение к

исследованиям General Motors в области гибридных автомобилей (стоившую, по оценкам компании, $40 млн), а затем попыталась продать ее Chery Automobile, китайскому конкуренту GM. Еще один китаец, сотрудник ведущего производителя красок и облицовочных материалов Valspar Corporation, нелегально скачал секретные формулы стоимостью $20 млн с намерением продать их в Китай; ученый-химик из DuPont похитил информацию об органических светоизлучающих диодах и планировал передать их одному китайскому университету. Никто из них не был непосредственно связан с китайскими властями — это обычные люди, попытавшиеся заработать на доступе к коммерческой тайне. Но нам также известно, что в Китае, где большинство крупных компаний или принадлежат государству, или сильно зависят от него, правительство провело или санкционировало множество кибератак против американских компаний, направленных на сбор информации. Так что можно не сомневаться: те нападения, о которых мы знаем, представляют собой незначительную долю предпринятых попыток, как успешных, так и неудачных.

Соединенные Штаты не пойдут той же дорогой электронного промышленного шпионажа, поскольку их законы намного строже (и лучше исполняются) и поскольку незаконная конкуренция противоречит американскому принципу честной игры. Это не столько разница в законах, сколько в ценностях: мы уже говорили о том, что Китай пока не очень высоко ценит право интеллектуальной собственности. Но такая диспропорция между американскими и китайскими компаниями и используемыми ими тактиками ставит как правительство, так и бизнес США в невыгодное положение. Чтобы остаться конкурентоспособными, американским компаниям придется яростно защищать свою информацию и охранять границы своих корпоративных сетей, а также отслеживать широкий диапазон внутренних угроз (все участники упомянутых инцидентов официально работали в пострадавших компаниях).

В ближайшие десятилетия сохранится противостояние как между США и Китаем, так и между другими странами, которые получают доступ к новым техническим возможностям и видят обеспечиваемые ими конкурентные преимущества, так что нынешняя волна экономического шпионажа на убыль не пойдет. Но драматического

обострения ситуации не случится по тем же причинам, по которым будет продолжаться непрекращающаяся, но относительно стабильная новая холодная война: невозможность установить инициатора кибератак. И китайские власти смогут поощрять любое количество нападений на иностранные компании и правозащитные организации (и даже принимать в них участие), пока их причастность не будет убедительно доказана[27]. Впрочем, существуют стратегии, которые можно использовать для смягчения ущерба от кибератак, помимо ослабления атакующих. Одна из идей принадлежит Крейгу Манди из Microsoft: виртуальный карантин. Мы уже говорили о том, что сегодня многие кибернападения проводятся в форме распределенных (DDoS) и обычных (DoS) атак типа «отказ в обслуживании». Для этого нужен один «открытый», то есть незащищенный компьютер в сети, который хакер может использовать в качестве базы для создания своей армии компьютеров-«зомби». (DoS-атаки проводятся посредством небольшого количества гиперактивных машин, а DDoS-атаки — крупной *распределенной* сетью атакующих машин, часто состоящей из взломанных компьютеров, чьи владельцы даже не подозревают о том, что стали объектом манипуляции.) Базой для хакера может стать всего одно забытое или незащищенное устройство в сети: никогда не использующийся ноутбук в научной лаборатории, личный компьютер, принесенный сотрудником в офис, — и вот уже взломана вся система[28].

Механизм карантина гасит такую атаку благодаря тому, что интернет-провайдер имеет возможность отключить инфицированный компьютер сразу же, как только идентифицирует его, в одностороннем порядке, без какого-либо дополнительного разрешения его владельца. «Основное условие: если ваша сеть заражена, нужно найти способ замедлить распространение вируса, — объясняет Манди. — Людей в таком случае помещают в карантин автоматически, а вот правильно ли вводить карантин в виртуальном пространстве, мы еще не решили». Когда у какой-либо машины обнаруживают признаки заражения вирусом или взлома, ее нужно «изолировать, проверить и вылечить до того, как под угрозой окажутся здоровые устройства», — добавил он. А поскольку пользователи зачастую не знают, что их компьютеры

инфицированы, ситуацию можно разрешить намного быстрее, если позволить интернет-провайдерам помещать их в карантин. В зависимости от того, как работает этот механизм, и от типа нападения атакующий может узнать о том, что инфицированное устройство находится в режиме офлайн, а может и не узнать, но пользователь в любом случае обнаружит, что у него пропало соединение с интернетом, отключенное его провайдером. Поскольку это лишает хакеров возможности проникнуть в систему посредством зараженного компьютера, ущерб, который он мог бы причинить, значительно снижается.

Манди считает, что должна быть создана независимая международная организация, интернет-провайдеры которой могли бы сообщать IP-адреса инфицированных компьютеров. Тогда и провайдеры, и все страны мира получили бы возможность отказывать устройствам с такими адресами в доступе к их онлайн-пространству, сокращая масштаб кибератак. Тем временем специалисты по компьютерной безопасности издалека следили бы за происходящим (ничем не обнаруживая, что интересующий хакеров компьютер попал в карантин) и собирали информацию, необходимую для выявления источника атаки. Исключать IP-адрес из карантина можно было бы лишь после того, как владелец компьютера очистил его при помощи лицензированного антивирусного программного обеспечения. Можно не только создать международную организацию, отвечающую за механизм автоматического отключения компьютеров, но и подписать международный договор, регулирующий его условия. Такое соглашение, позволяющее быстро реагировать на случаи заражения сетей, стало бы большим шагом вперед в деле борьбы с кибератаками. А страны, не желающие подписывать такой договор, рисковали бы оказаться в карантине целиком, что означало бы их недоступность для большинства пользователей мира.

Но карантин может и не потребоваться: шансы потенциальных жертв повышаются, если их сеть надежно защищена. Одна из основных проблем компьютерной безопасности заключается в том, что обычно на создание защиты требуется гораздо больше усилий, чем на ее преодоление: программа для обеспечения безопасности конфиденциальных данных может состоять из 10 млн строк кода, а

обойти ее в случае нападения удается при помощи всего лишь 125 строк. Некоторое время назад за кибербезопасность американского правительства отвечала Регина Даган, тогдашний директор DARPA (Агентство передовых оборонных исследовательских проектов, США), а ныне старший вице-президент Google. По ее словам, для того чтобы устранить этот дисбаланс, приходилось выступать «за технологические изменения». Как и Манди, Даган и DAPRA обратились для этого к биологии, собрав объединенную команду из специалистов по компьютерной безопасности и ученых-биологов, занимающихся изучением инфекционных болезней, результатом чего стала программа CRASH по разработке принципиально новых отказоустойчивых адаптивных защищенных серверов.

В основе программы CRASH лежит тот факт, что человеческие организмы генетически разнообразны и имеют иммунную систему для защиты от попадающих в них вирусов. Компьютеры устроены очень похоже, и это делает возможным их массовое заражение с помощью вредоносного программного обеспечения. «Мы пришли к выводу, что для обеспечения кибербезопасности нам нужно включить в архитектуру компьютерной защиты эквивалент адаптивной иммунной системы», — говорит Даган. Компьютеры будут выглядеть и действовать одинаково, но в их поведении станут проявляться уникальные различия, способные их защищать. «А это значит, что злоумышленникам теперь придется писать по 125 строчек кода для каждого из *миллионов* компьютеров — вот так мы и устраним дисбаланс». Полученный урок, несомненно, применим не только в области компьютерной безопасности, считает Даган: «Если при первом рассмотрении вы видите, что ситуация проигрышная, вам нужно что-то принципиально иное, и это само по себе означает новые возможности». То есть, если не можете выиграть в игре, измените ее правила.

И все же, несмотря на появление некоторых средств для отражения кибератак, невозможность установить авторство в виртуальном мире останется серьезной проблемой компьютерной и сетевой безопасности. В соответствии с общим правилом при наличии достаточного количества «анонимизирующих» слоев между двумя узлами интернета проследить источник переданных пакетов данных

невозможно. Это реальная проблема, но надо помнить, что интернет создавался не преступниками. Изначально он основывался на доверии. В онлайн-пространстве трудно определить, с кем вы имеете дело. Специалисты по кибербезопасности с каждым днем все надежнее защищают пользователей, компьютерные системы и информацию. Однако так же быстро растут навыки криминальных и анархически настроенных элементов. Эта игра в кошки-мышки будет продолжаться столько, сколько просуществует сам интернет. На уровне сети в целом полезно публиковать информацию о кибератаках и подробностях вредоносного программного обеспечения: если бы были распакованы и преданы гласности компоненты червя Stuxnet, можно было бы устранить уязвимости программ, которые он использовал, а специалисты занялись бы разработкой защиты от него. Могли бы помочь и другие стратегии, такие как универсальная регистрация, но нам придется пройти еще долгий путь, пока интернет-безопасность станет эффективной хотя бы настолько, чтобы отражать простые кибератаки. Это проявление дуализма виртуального мира: анонимность позволяет творить как добро, так и зло кому бы то ни было: и обычному пользователю, и государству, и корпорации. В конце концов, лишь от людей зависит, каким окажется наше будущее.

Подведем итоги. Те времена, когда государствам приходилось заниматься внутренней и внешней политикой лишь в физическом мире, миновали. Если бы можно было просто воспроизвести ту же политику в мире виртуальном, будущее государственного строительства не было бы столь сложным. Но главам стран придется смириться с тем, что отныне управлять населением и оказывать влияние за рубежом станет гораздо труднее. Им придется применять наиболее мощные из имеющихся в их распоряжении инструментов, в том числе устанавливать контроль за национальным интернетом, меняя привычные способы работы в сети своих граждан и объединяясь с союзниками со сходной идеологией, чтобы расширить свое присутствие в виртуальном пространстве. Такой дисбаланс между силой в реальном и виртуальном мирах означает возможности для некоторых новых, но недооцененных пока игроков, в том числе для небольших амбициозных стран, а также для самых смелых из непризнанных государств.

Государствам, стремящимся разобраться в поведении друг друга, ученым, изучающим международные отношения, неправительственным организациям и корпорациям, действующим на территории суверенных стран, придется по-разному оценивать ситуацию в реальном и виртуальном мирах, чтобы понять, как то или иное событие в одном из них скажется на другом, и сориентироваться в противоречиях, которые могут существовать между реальной и виртуальной политикой властей — как внешней, так и внутренней. Справиться с этим нелегко даже в реальном мире, так что в новую цифровую эпоху сталкиваться с ошибками и просчетами нам придется гораздо чаще. На международной арене это приведет к эскалации киберконфликтов и войн нового типа, а также, как мы сейчас увидим, к новым революциям.

Примечания к главе 3

ГЛАВА 4

Будущее революций

Всем известна история «арабской весны», но мы пока не знаем, где она повторится. Нет сомнений, что в ближайшем будущем нас ожидает расцвет революционного движения, ведь благодаря телекоммуникациям возникают новые связи и больше возможностей для самовыражения. Поскольку во многих странах уровень проникновения мобильной связи и интернета растет, все легче становится делать какие-то тактические шаги: заниматься мобилизацией сторонников или распространять агитационные материалы.

Однако, несмотря на множество попыток революций, немногие из них приведут к радикальным результатам — полноценным революциям с коренной и прогрессивной сменой государственного строя. Препятствовать глубоким изменениям, сравнимым по масштабу с арабскими революциями, начавшимися в конце 2010 года, будут недостаток ярких лидеров и более изобретательная реакция властей. История показывает, что уровень технологического развития общества действительно обусловливает революционные процессы и влияет на их характер. На фундаментальном же уровне у всех успешных революций есть общие элементы, в частности институциональная структура, поддержка извне и культурное единство. Отсутствие одного или нескольких таких элементов может вести к неудаче, что подтверждается событиями прошлого, начиная с русского революционного движения до 1917 года и заканчивая шиитским восстанием 1991 года в Ираке и иранской «зеленой революцией» 2009 года. Современные технологии, какими бы они мощными ни были, не могут сотворить чуда, хотя и способны значительно повысить шансы на успех.

Учитывая, какое количество людей будут иметь доступ в сеть в столь разных местах, можно сделать вывод, что в будущем на земле

сложится самое активное, открытое и глобализированное гражданское общество из всех, которые когда-либо знал мир. В начале развития революционного движения присущая виртуальному миру информационная «зашумленность» помешает спецслужбам отслеживать и пресекать революционную активность, тем самым позволяя революции начаться. Но после этого возникнет другая проблема: лидерам протеста может не хватить опыта или способностей для работы в реальном мире — с парламентами, конституциями и электоральными политиками.

Легче начать...

По мере распространения интернета и подключения к нему все новых уголков мира по сети будут распространяться ростки революции, причем все более внезапно и чаще, чем когда-либо раньше. Пользуясь недавно обретенным доступом к виртуальному пространству и его технологиям, постараются не упустить своего различные группы людей. Движимые давними или новыми обидами, они станут действовать упорно и убежденно. Многие лидеры, возглавившие такие движения, будут молоды, и не только потому, что невероятно молодо население многих государств, недавно получивших доступ в сеть (примерами стран, большинство жителей которых младше 35 лет, могут быть Эфиопия, Пакистан и Филиппины), но и потому, что именно для молодых людей характерно сочетание активности и высокомерия. Они уже убеждены, что знают, как сделать правильно, так что не преминут воспользоваться представившейся им возможностью.

В будущем все страны, включая давно знакомые с интернет-технологиями, столкнутся с теми или иными формами протеста, причем инструментом его организации, мобилизации и вовлечения международного сообщества будут служить телекоммуникации. Те платформы, которыми сегодня пользуются протестующие — Facebook, Twitter, YouTube и тому подобные, — станут еще действеннее, поскольку разработчики из разных уголков планеты найдут новые способы применения видеороликов, изображений и сообщений в своих целях. Мир узнает еще больше «цифровых» активистов, ставших

героями своих сообществ в результате сознательной работы в этом направлении. В странах, где еще не было крупных протестных движений, они вспыхнут, причем в мировом масштабе: весь мир будет следить за ними и, вполне вероятно, их поддерживать. Для демократических обществ более характерны протесты, вызванные социальной несправедливостью и экономическим неравенством, в то время как жители государств с репрессивными режимами будут выступать против проблем иного рода: нечестных выборов, коррупции и жестокости полиции. Вряд ли появятся принципиально новые причины для протестов — скорее, вырастет количество их участников и возникнут новые формы мобилизации сторонников.

Когда-то инициатива восстания была прерогативой определенного круга хорошо обученных и вооруженных людей, пользующихся поддержкой из-за рубежа. Этому пришел конец: телекоммуникационные технологии устранили все возрастные, половые и общественно-экономические барьеры, которые прежде ограничивали круг активистов. Больше не нужно терпеть несправедливость в изоляции и одиночестве, и возможность получить глобальную обратную связь, то есть комментарии и реакцию людей со всего мира, позволит жителям многих стран встать во весь рост и заявить о том, что они чувствуют. Как показала «арабская весна», стоит только людям преодолеть так называемый «барьер страха» и понять уязвимость правительства, как к революции без колебаний присоединяются даже прежде вполне лояльные и тихие граждане. Одним из позитивных последствий участия в арабских революциях социальных СМИ стала более активная роль женщин, у которых появился выбор. Они могли выражать себя в социальных сетях даже тогда, когда на улицу выходить было слишком рискованно (хотя многие женщины шли и на физический риск!). В некоторых странах люди будут время от времени устраивать ежедневные протесты онлайн или на улицах просто потому, что могут это делать. Мы видели это в Ливии в 2012 году. На встрече с министрами переходного правительства в Триполи кто-то из них невзначай обронил, что небольшие группы протестующих собираются практически каждое утро. «Беспокоит ли вас это?» — спросили мы. Большинство

присутствующих отрицательно покачали головами: нам с усмешками заявили, что это нормальная реакция после сорока лет репрессий.

В виртуальном пространстве постоянно возникают новые возможности для проявления несогласия и участия в протестных действиях, а также появляются новые средства защиты потенциальных революционеров. Скорее всего, большинство диссидентов почувствуют, что их мир благодаря массовому распространению коммуникационных технологий стал более безопасным, несмотря на то что физические риски остались прежними. (Но не всех активистов новые технологии защищают одинаково: в странах с технически «продвинутыми» властями диссиденты в интернете могут оставаться столь же уязвимыми, как и на улицах.) Аресты, преследования, пытки и физические расправы не исчезнут, но в целом анонимность интернета и сетевая мощь коммуникационных технологий обеспечат активистам и потенциальным участникам протестов дополнительный «изолирующий слой», поощряя их продолжать свою деятельность.

Некоторые достижения высоких технологий окажутся особенно полезными для активистов и диссидентов. Высокопроизводительное программное обеспечение для видеотрансляций в режиме реального времени позволяет держать в курсе пользователей за рубежом. Надежные средства доступа к внешней информации и связи с диаспорами помогают противостоять деструктивным действиям государства и заметно увеличивать базу поддержки оппозиции. А безопасные электронные платформы для перевода денежных средств и передачи данных еще теснее связывают участников протестов с иностранными источниками помощи, не раскрывая при этом местонахождения получателей.

В этих новых революционных движениях будет больше анонимных активистов и активистов «по совместительству», чем сегодня, просто потому, что у людей появится свобода выбора, когда и как им протестовать. Когда-то быть революционером означало полностью посвятить себя революции. Сегодня, а в еще большей мере в будущем универсальные технологические платформы позволят кому-то участвовать в ней постоянно, а кому-то вносить посильный вклад во время обеденного перерыва. Активистам поможет коллективное знание других активистов и обычных пользователей со всего мира,

особенно когда речь идет о средствах защиты: протоколах безопасности, инструментах шифрования и прочих электронных системах, которые станут гораздо более доступными и понятными. Большинство тех, кто в следующем десятилетии получат доступ в сеть, живут в странах с авторитарными или полуавторитарными правительствами, а история учит нас, что в эпоху свободного распространения информации режимы теократии, культа личности и диктатуры поддерживать все сложнее (достаточно вспомнить, какую роль в крахе Советского Союза сыграла политика гласности). В итоге возникнет новая модель поведения в мире, при которой народы, имеющие доступ к новой информации в виртуальном пространстве и недовольные своим репрессивным или недостаточно прозрачным правительством, будут участвовать в непрерывных онлайн-акциях протеста, фактически постоянно поддерживая состояние революционного напряжения.

Всеобщий доступ в сеть изменит наши взгляды на оппозицию. В странах продолжат действовать «реальные» общественные организации и партии, но появление на виртуальной центральной площади огромного количества новых участников драматически преобразует пейзаж политической активности. Большинство людей будет волновать не конкретная проблема — они скорее присоединятся к движению, выступающему за решение целого спектра проблем и действующему на территории нескольких стран. Для организаторов кампаний здесь есть и плюсы, и минусы: это позволит легко оценивать и визуализировать размер сети сторонников, однако усложнит понимание степени их заинтересованности в общем деле и преданности ему. В странах, где свобода собраний ограничена или вовсе отсутствует, возможность общаться и планировать действия в виртуальном пространстве кажется манной небесной независимо от состава участников. А вообще именно лидеры, принимающие стратегические решения, должны будут разобраться, действительно ли у их движения есть массовая поддержка, или оно представляет собой огромную эхо-камеру.

Оппозиционным силам виртуальный мир позволяет по-новому решать критически важные задачи сбора средств и создания собственного бренда. Некоторые из них будут по-разному

позиционировать себя в различных частях интернета для того, чтобы добиться внимания нужных целевых групп. Так, оппозиционная организация из Центральной Азии может приглушить свои религиозные обертоны на платформе с англоговорящими пользователями из западных стран, а в рамках сетей своего региона повести себя противоположным образом. Уже сегодня нечто подобное делают «Братья-мусульмане» и другие исламистские партии; именно так отличаются по тону и подбору тем независимые друг от друга редакции канала «Аль-Джазира», которые вещают на английском и арабском языках. (К примеру, в день проведения одной из первых акций протеста в Сирии в 2011 году в сообщении «Аль-Джазира» на английском языке были приведены данные о множестве погибших демонстрантов. Та же «Аль-Джазира» на арабском, как ни странно, вместо этого рассказала о какой-то незначительной инициативе Башара Асада, относящейся к проблеме курдского меньшинства страны. По мнению некоторых аналитиков, этот дисбаланс отражает политическую зависимость катарского телеканала от Ирана, союзника Сирии и соседа Катара.)

Одновременно с тем, что у оппозиционных групп становится все больше возможностей для создания своего бренда, меняется традиционная модель их организации: сегодня у оппозиции вместо офисов — сайты, вместо сотрудников — фолловеры и члены сообщества; они используют бесплатные и открытые платформы, позволяющие сократить накладные расходы. В будущем «цифровых оппозиционеров» будет так много, что им придется яростно конкурировать за внимание публики.

В результате появления в интернете такого изобилия новых голосов и шума, который они будут производить, потребуется точнее определить само понятие «диссидент». В конце концов, диссидентом может называться не каждый, кто выражает в интернете свое мнение: так делают практически все, кто имеет к нему доступ. Лидерами следующей волны диссидентского движения станут лишь люди, способные вести за собой других и с помощью краудсорсинга обеспечивать себе поддержку в сети, имеющие навыки использования цифровых инструментов продвижения и, что самое главное, готовые подвергнуть себя физической опасности. Активность исключительно в

сети, особенно удаленная или анонимная, снижает привлекательность диссидента в глазах потенциальных последователей, поэтому истинные лидеры будут рисковать в реальной жизни в отличие от их виртуальных сторонников. Так что больше шансов остаться позади окажется не у тех, кто плохо знаком с механизмами проведения конституционных реформ, строительства общественных институтов и государственного управления, а у тех, кто не обладает техническими навыками других активистов: таким людям труднее возглавить виртуальную толпу и сравниться с другими, молодыми лидерами (молодежь может просто не понять истинную значимость их опыта).

Как отмечалось, будущие революционные движения окажутся транснациональными и более массовыми, чем многие (хотя и не все) революции прошлого, выходя далеко за пределы традиционных национальных, этнических, языковых, половых и религиозных границ. Во время нашей поездки в Тунис в 2011 году мы встретились с активистами «жасминовой революции» — это было примерно через год после их успешного выступления. На наш вопрос о том, почему их революция вызвала настоящую цепную реакцию восстаний, они вначале упомянули об одинаковых проблемах, ставших их первопричиной, а затем рассказали о региональной сети контактов. Оказалось, что им легко удается налаживать отношения с любыми иностранцами, говорящими по-арабски и живущими на Ближнем Востоке, причем не только благодаря общности языка и культуры, но и потому, что часто у них есть общие друзья. Обширные социальные контакты, возникшие еще до начала революции, активизировали и ускорили распространение революционных настроений по региону, позволили обмениваться стратегиями и инструментами, обеспечивать финансовую и моральную поддержку.

Однако даже у этих крупных сетей существовали пределы, соответствующие границам арабского мира. В будущем все изменится. Благодаря продвинутым программам-переводчикам, способным учитывать региональные особенности языков и переводить в режиме реального времени, говорящий по-арабски активист из Марокко сможет координировать действия другого активиста, скажем, в Бангкоке, не знающего никакого иного языка, кроме тайского. Инновационные голосовые переводчики, интерфейсы управления

жестами и в конечном счете голографические проекции позволят сформировать виртуальные сети гораздо более обширные, чем существующие. У разных народов невероятно много общих культурных черт, плохо изученных из-за языкового барьера и связанных с этим проблем коммуникации. В ходе будущих революций благодаря, казалось бы, почти случайным связям между находящимися очень далеко друг от друга сообществами и отдельными пользователями будут возможны обмен знаниями, аутсорсинг некоторых задач и новые неожиданные способы распространения идей.

Кому-то телекоммуникационные технологии позволят участвовать в борьбе, не подвергая себя риску, и чувствовать себя активистом, не прилагая особых усилий. Ведь сделать ретвит антиправительственного лозунга или поделиться видеороликом о жестоких действиях полиции, находясь в безопасности, довольно легко, особенно по сравнению с риском, на который шел тот, кто его снимал. Даже не участвующие непосредственно в оппозиционном движении люди могут испытать ощущение всемогущества, делая *хоть что-то*, и онлайн-платформы предоставляют им возможность подключиться и почувствовать свою ценность — пусть то, что они делают, мало на что влияет. Впрочем, если для жителей стран, власти которых обладают определенными техническими навыками, и есть шанс быть пойманными, виртуальная храбрость практически не несет никаких рисков.

Внести значительный вклад в какую-либо кампанию в другой части света может любой тинейджер из Чикаго или Токио. После того как режимом Мубарака была отрезана связь Египта с внешним миром, многие наблюдатели в поисках достоверной информации переключились на аккаунт в Twitter, созданный старшекурсником из Лос-Анджелеса Джоном Скоттом-Рэйлтоном, который размещал там последние известия, полученные из египетских источников по телефону. Некоторое время его аккаунт @Jan25voices был основным источником информации о восстании, несмотря на то что он не был журналистом и не говорил свободно по-арабски. Однако, хотя Скотт-Рэйлтон и смог привлечь к своим твитам некоторое внимание общественности, возможности таких людей ограниченны. В любом случае влиятельными фигурами им не стать.

Более показателен пример Энди Карвина. Он курировал один из самых заметных источников информации о египетской и ливийской революциях с десятками тысяч подписчиков, в том числе огромным количеством журналистов. Последние знали, что Карвин придерживается профессиональных

журналистских стандартов, и поэтому его твиты и ретвиты содержат только достоверные сведения. Он стал чрезвычайно авторитетным источником, отбирая и проверяя всю поступавшую к нему информацию.

Тем не менее, сколь бы талантливыми ни были люди, подобные Энди Карвину и Джону Скотту-Рэйлтону, тяжелая работа революции делается «на земле», жителями страны, которые готовы выйти на улицу. Вы не сможете взять штурмом здание министерства внутренних дел при помощи мобильного телефона.

А вот инструменты, которые позволяют проявлять виртуальную храбрость, будут влиять и на поведение протестующих на улицах. Благодаря глобальным социальным сетям потенциальные активисты и диссиденты могут поверить в то, что их многие поддерживают, независимо от того, так ли это. Иногда организации переоценивают степень своей онлайн-поддержки и в результате пренебрегают другими возможностями, которые действительно обеспечили бы им преимущество (скажем, переманивание в свой лагерь видных представителей правящего режима). Наличие большой виртуальной сети последователей может подвигнуть какую-нибудь оппозиционную группу пойти на больший риск, причем не в самый удачный момент. И вот ее руководители, преисполненные уверенности и окрыленные успехом в виртуальном мире, уже развязывают кампанию, плохо подготовленную и обреченную на поражение — неизбежное следствие пренебрежения контрольными механизмами революционных движений. И до тех пор, пока оппозиционеры не научатся эффективно использовать «виртуальное» воодушевление как лидеров, так и их последователей, такая тенденция сохранится.

Скорее всего, возросшая информированность общества о революциях и кампаниях протеста во всем мире приведет к возникновению культуры революционных «помощников». Их будет много: и полезных, и не очень, и даже откровенно опасных. Мы увидим талантливых инженеров, которые разрабатывают приложения и средства защиты для диссидентов, и успешных интернет-агрегаторов, которые используют голоса множества людей для давления на власть и привлечения внимания к своим требованиям. Обязательно появятся те, кто разрабатывает специализированные

телефоны для дальнейшего тайного ввоза в страну, охваченную протестами. Такие телефоны, благодаря предустановленным секретным приложениям, позволят пользователям размещать информацию (тексты, фотографии, видео), не оставляя никаких следов в памяти устройства. А если не будет следов, телефон не сможет стать уликой, попав в руки агентов спецслужб.

А еще мы увидим волну «революционеров-туристов» — людей, весь день прочесывающих интернет в поисках каких-нибудь протестных онлайн-кампаний и готовых присоединиться к ним просто для того, чтобы пощекотать себе нервы. Такие участники помогают движению набирать ход, поскольку распространяют информацию о нем. Однако если их не контролировать и не отфильтровывать, они способны исказить истинные масштабы поддержки и навредить тем, кто организует практическую работу и рискует по-настоящему. Ключевым для действительно эффективных лидеров оппозиции, понимающих, как много требуется для проведения успешной революции, станет вопрос: как привлекать новых сторонников, не теряя контроля над их качественным составом и эффективно управляя ожиданиями?

...Но труднее закончить

Стремительное распространение революционных движений в странах, недавно получивших доступ к интернету, в конечном счете окажется не столь опасным для их властей, как предсказывают некоторые наблюдатели. Ведь несмотря на то, что с развитием телекоммуникационных технологий баланс силы действительно смещается в пользу граждан, помогая революции, существуют критически важные факторы перемен, над которыми технические средства не властны. И главный из них — появление первоклассных лидеров, то есть людей, способных провести оппозицию сквозь трудные времена, вести переговоры с властями в случае их готовности начать реформы или бороться за власть, победить и дать людям то, что они хотят, после бегства диктатора. Если человек не обладает чертами, необходимыми для управления государством, то ему не помогут никакие технологии.

В последние годы мы видели, что множество молодых людей, «вооруженных» всего лишь мобильными телефонами, могут стремительно разжигать революции, бросая вызов десятилетиям авторитарного правления и тотального контроля, — а ведь прежде на это требовались годы. Теперь понятно, что высокотехнологичные платформы в умелых руках помогают свергать диктаторов. Но если учесть диапазон возможных последствий: жестокие репрессии, смену режима, гражданские войны, переход к демократии, — становится очевидным, что решают судьбы революций люди, а не инструменты, которые они используют. Когда на виртуальные площади выплеснутся онлайн-толпы, традиционные компоненты гражданского общества окажутся особенно важными: в то время как некоторые из новых участников революционного движения (вроде активистов-организаторов) проявят себя как адекватные и влиятельные фигуры, многие другие — мы уже говорили об этом — на протяжении всего процесса останутся всего лишь генераторами и усилителями шума.

В ходе будущих революций многие люди станут знаменитыми, но эта особенность развития любого оппозиционного движения задержит появление истинных лидеров, способных довести дело до конца. Ведь технологии помогают отыскать людей с лидерскими качествами — мыслителей, интеллектуалов и т. п., но не способны создать их. Народные восстания могут смести диктаторов, однако успех зависит от того, есть ли у оппозиции план и возможности его реализовать. В противном случае результатом будет или восстановление прежнего режима, или скатывание к стране с недееспособным правительством. Создание странички в Facebook — это не план; истинные навыки управления — это когда революцию доводят до успешного завершения.

Для описания событий «арабской весны» и наблюдатели, и участники использовали эпитет «революция без лидеров», но это не совсем точно. Конечно, на этапе ежедневных демонстраций вполне возможно сохранение децентрализованной структуры управления: так безопаснее, поскольку у режима нет возможности парализовать протест, просто схватив его лидеров. Однако со временем должно возникнуть централизованное руководство движением, если оно развивается в каком-то определенном направлении.

Мятежники, которые многие месяцы противостояли Муаммару Каддафи, не были единой армией, но к 27 февраля 2011 года, через две недели после начала публичных протестов в Ливии, в Бенгази был сформирован Переходный национальный совет (ПНС). В него вошли известные оппозиционеры, видные члены правительства, перешедшие на сторону восставших, бывшие военные, ученые, юристы, политики и бизнесмены, а его исполнительный комитет действовал как оппозиционное правительство и вел переговоры с представителями иностранных государств и НАТО об их участии в борьбе с диктатором. Председатель ПНС Махмуд Джибрил исполнял обязанности временного премьер-министра страны до конца октября 2011 года, когда был схвачен и убит Муаммар Каддафи.

А вот в Тунисе революция развивалась так быстро, что времени на формирование оппозиционного правительства, аналога ливийского ПНС, не было. Когда из страны бежал тогдашний президент Зин эль-Абидин Бен Али, государственный строй Туниса остался прежним. Население не прекращало протесты, пока из правительства не ушли последние члены президентской Конституционно-демократической партии, на смену которым пришли устроившие оппозицию фигуры. Но, отреагируй руководители на требования народа иначе, начни они репрессии вместо того, чтобы пересмотреть свою позицию, Тунис мог бы пойти по другому, гораздо менее стабильному пути. (Интересно, что многие лидеры, победившие на выборах в октябре 2011 года, оказались бывшими политзаключенными, к которым у жителей страны был иной, вероятно, более высокий уровень доверия, чем к тем, кто вернулся из-за границы.) Премьер-министр Туниса Хамади Джебали, сам бывший политзаключенный, рассказывал нам, что, с его точки зрения, первый министр внутренних дел после падения режима Бен Али должен был быть «жертвой министерства внутренних дел». И поэтому он назначил на этот пост Али Лараеда, который провел 14 лет в тюрьме, причем большую часть времени — в одиночке.

Недостаток такого ускоренного роста оппозиционных движений состоит в том, что у организаций и их идей, стратегий и лидеров очень мало времени на «созревание». История показывает нам, что оппозиционным движениям нужно время на полноценное развитие и что в результате такого развития они набирают силу, а их лидеры лучше понимают нужды населения, которое собираются увлечь за собой. Возьмем Африканский национальный конгресс (АНК) в ЮАР. За несколько десятилетий борьбы с системой апартеида организация прибрела опыт, а у тех, кто потом становился президентом ЮАР (Нельсон Мандела, Табо Мбеки и Джейкоб Зума), было время заработать репутацию, заслужить доверие и выстроить связи,

одновременно оттачивая управленческие навыки. То же самое можно сказать и о Лехе Валенсе и его польском профсоюзе «Солидарность»: прошло десять лет, прежде чем лидеры «Солидарности» смогли завоевать места в парламенте и их победа подготовила почву для падения коммунизма.

У большинства оппозиционных групп на организацию, согласование позиций и подготовку лидеров уходят многие годы. Мы спросили бывшего госсекретаря США Генри Киссинджера, который встречался практически со всеми ведущими революционными лидерами последних сорока лет, что теряется в случае развития по ускоренному графику. «Трудно представить, чтобы де Голль или Черчилль могли появиться в эпоху Facebook, — считает он, замечая: — Я не вижу людей, готовых выдержать давление и выступить в одиночку» в наше время гиперсвязанности всех со всеми. Вместо этого миром будет править «бездумное единодушие», и открыто противостоять ему смогут лишь очень немногие. А это именно тот риск, на который должен был готов идти любой лидер. «Уникальные лидерские качества — исключительно индивидуальная черта, она не вырабатывается в социальных сетях», — сказал Киссинджер.

Если руководители революционного движения не проявляют себя как сильные лидеры и не обладают качествами, необходимыми для управления страной, у них может не получиться удержать власть, и в результате возникает риск замены одного авторитарного режима на другой. По словам Киссинджера, «обладающие влиянием люди знают, как вывести сограждан на площадь, но не знают, что делать *после* этого. И еще меньше понимают, что делать с ними после победы». Он объясняет, что такие люди быстро становятся маргиналами, ведь их стратегии теряют эффективность: «Вы не можете выводить людей на площадь двадцать раз в год. Эта фаза объективно ограниченна, а какова следующая — неясно». Но без ясной следующей фазы движение будет двигаться по инерции, которая непременно ослабнет.

Множество уличных активистов, хотя и критикуют состоявшиеся в их странах революции и их последствия, все же не согласились бы с точкой зрения Генри Киссинджера. Один из них — Махмуд Салем, египетский блогер, своего рода рупор революции 2011 года в его стране. Салем активно критикует сограждан за то, что они неспособны

планировать дальше отстранения от власти Мубарака и не стремятся к созданию открытой конкурентной политической системы. Но критикует он лишь египтян, а не революционную модель новой цифровой эпохи как таковую. Он писал в июне 2012 года, сразу после первых свободных президентских выборов: «Если вы революционеры, покажите нам, на что способны. Начните что-нибудь делать. Создайте партию. Выстройте организацию. Решите реальную проблему. Сделайте что-нибудь, кроме вечного круговорота от демонстраций к маршам, от маршей к сидячим забастовкам. Это не уличная работа: настоящая уличная работа — это когда вы двигаете улицу, а не двигаетесь по ней. Настоящая уличная работа — это когда улица вас знает и вам доверяет и готова за вами идти». Он убеждал уличных активистов принимать участие в управлении страной и в изменении культуры коррупции, против которой они выступали. Это означает, что нужно пристегивать ремни безопасности, соблюдать правила движения, поступать в полицейскую академию, участвовать в парламентских выборах и делать так, чтобы местные власти отвечали за свои действия перед избирателями.

Тому, чего может добиться толпа, посвящена книга Тины Розенберг «Вступите в клуб: как мнение группы может изменить мир»[29]. Рассматривая важность человеческих взаимоотношений с точки зрения их влияния на поведение индивидуума и основные социальные тенденции, она утверждает, что настоящие революционеры способны управлять давлением со стороны членов группы, к которой принадлежит человек, на то, чтобы подтолкнуть к нужным поступкам и его, и группу в целом. Возможно, самая убедительная иллюстрация того, что Розенберг называет «социальным лекарством», — деятельность сербской оппозиционной группы «Отпор», сыгравшей ключевую роль в падении режима Слободана Милошевича. Она описывает, как для разрушения культуры страха и безнадежности группа использовала веселые и яркие уличные представления, розыгрыши, концерты, лозунги и акции мирного гражданского неповиновения. В борьбе с группой режим вел себя одновременно жестоко и глупо, так что поддержка «Отпора» постоянно росла.

Однако важнее то, что роль, которую играли в прошлом группы вроде «Отпора», в будущем смогут играть их лидеры. Как показывает Розенберг на примере бывших сербских активистов, обучающих своих молодых коллег по всему миру, успешные революционеры должны разрабатывать разные стратегии для действий в виртуальном и реальном мире. В противном случае заметные фигуры появятся в избытке, а лидеров, которым можно доверять, так и не найдется. Исторически с известными людьми ассоциируется определенное доверие общества: за исключением таких пользующихся дурной славой политиков, как командиры вооруженных формирований и руководители военной хунты, известность высокопоставленных лиц коррелирует с количеством их сторонников. Но в будущем левая и правая части этого уравнения поменяются местами: известность будет приходить легко и быстро, после чего ее обладателю придется завоевать значительную поддержку, доверие и наработать опыт.

Мы уже сталкивались с этим в сбывающихся пророчествах независимых кандидатов в президенты США. Во время президентской кампании 2012 года очень заметной фигурой стал Херман Кейн, до этого сравнительно мало известный за пределами делового мира. Некоторые наблюдатели считали его серьезным претендентом, несмотря на то что как политик он был совершенно не готов занять пост президента, что и выяснилось по прошествии нескольких недель (хотя могло стать понятным мгновенно, если бы его кандидатуру выдвигала какая-либо партия в ходе открытой дискуссии). В революционных движениях будущего встретится множество таких персонажей, как Кейн, ведь харизматичные однодневки, популярные в сети, гораздо быстрее взбираются наверх. Но непривычные к политической «жаре» революционеры-знаменитости обладают слишком «тонкой кожей» и быстро «сгорают».

То, как оппозиция будет решать проблему поиска подходящих лидеров, зависит от страны и имеющихся в распоряжении движения ресурсов. В странах с неразвитым революционным движением, находящимся под пристальным вниманием правящего режима, просеивать толпу в поисках подлинного лидера очень непросто. Там же, где ресурсов достаточно, а движения обладают известной автономностью, вполне возможно при помощи специалистов-

консультантов идентифицировать прирожденных вожаков, помогая им в дальнейшем развивать необходимые навыки и налаживать контакты. В отличие от сегодняшних консультантов специалисты высокотехнологичного завтра будут иметь дипломы в области инжиниринга и когнитивной психологии, обладать техническими знаниями и гораздо лучше понимать, как нужно создавать и корректировать имидж политической фигуры в каждом конкретном случае. Работая с перспективным кандидатом, чья известность превышает кредит доверия общества, они смогут измерять его политический потенциал с помощью различных инструментов: «поручая» тексты его выступлений сложным программным средствам для выделения их основных характеристик[30] и анализа тенденций; составляя карту функций его мозга, чтобы определить, как он справляется со страхом или искушением, и проводя всестороннюю диагностику его политических установок для оценки их слабых сторон.

* * *

Многие группы активистов и политические организации станут создавать виртуальные фронты, намного превосходящие их физические проекции. Представьте себе новую оппозиционную группу, сформированную спустя всего несколько дней после революции в Алжире, которая привлекает к сотрудничеству ярких интернет-маркетологов и дизайнеров из алжирской диаспоры Марселя. Костяк группы составляют всего пять недавних выпускников университета двадцати с небольшим лет, практически не имеющие политического опыта. У этой команды нет былых заслуг, но благодаря технически совершенной онлайн-платформе алжирцам кажется, что она компетентна, высокомотивирована и обладает огромной сетью сподвижников. В действительности это неорганизованная, лишенная видения и совершенно не готовая взять на себя хоть какую-то ответственность группа людей. Диссонанс между онлайн-презентацией и реальными возможностями таких организаций будет задерживать их развитие и вызывать трения между участниками. Вполне вероятно, что какие-то движения покажутся в виртуальном

мире серьезной угрозой режиму, но на деле это лишь результат отличного владения интернет-технологиями без какой-либо угрозы властям вообще. Но, создавая завышенные ожидания и порождая ложную надежду на успех движения, оппозиционные группы, не способные справиться со своей задачей, могут принести больше вреда, чем пользы, поскольку служат слишком дорогостоящим средством отвлечения внимания общества.

Несомненно, что организационные просчеты и ложные пророки — спутники всех революций прошлого, однако в будущем значение таких недостатков повысится, увеличивая риск разочарования членов оппозиционных групп. А если слишком много людей потеряют веру в набирающее силу движение и его перспективы, это может совершенно уничтожить шансы на перемены. Нестабильность руководства, а также диссонанс между физическими и виртуальными возможностями движения могут лишить его перспектив на поддержку и успех в стране. Следствием информированности граждан и наличия у них доступа в интернет станет их критическое и осторожное отношение не только к властям, но и к оппозиции.

Критическое отношение к потенциальной оппозиции скажется и на членах зарубежной диаспоры, и на тех, кто вернется из-за границы после бегства от репрессий. Обычно такие люди возвращаются с международной поддержкой, но плохо понимают нужды и желания населения страны. Этот отрыв от реальности проявляется в публичных скандалах (такими, как с участием Ахмеда Чалаби, какое-то время руководившего Ираком) и трудностях (например, с которыми столкнулся президент Афганистана Хамид Карзай). Расширение возможностей доступа в интернет, с одной стороны, сокращает разрыв между зарубежной диаспорой и населением страны, в результате чего политики, возвращающиеся из-за границы в надежде поучаствовать в революционном процессе, оказываются лучше подготовленными к взаимодействию с местными игроками. С другой стороны, конкуренты на родине будут знать о них больше (ведь их прошлое, вне всяких сомнений, можно изучить по следам, оставленным в интернете) и используют эти знания с выгодой для себя.

Представьте себе состоятельного члена эритрейской диаспоры, который занимается на Западе медийным бизнесом. У него много

сторонников в интернете и на родине, и за ее пределами, и таким образом сформировался обширный виртуальный электорат. Но может так получиться, что завоевать симпатии сравнимого по масштабам реального электората в Эритрее ему будет трудно, поскольку многие скептически отнесутся и к его прошлому, и к связям с международными СМИ. То, что казалось привлекательным аудитории на международном уровне или в интернете, может остаться пустым звуком для населения страны. И тогда, вернувшись домой в надежде, что ему открыт путь к высотам власти, политик столкнется с тем, что, несмотря на его многообещающий старт, соотечественники предпочли его местному сопернику, которому больше доверяют.

Добиться успеха смогут лидеры, которые имеют связи с зарубежной диаспорой и придерживаются некоей гибридной модели, то есть стремятся привлечь на свою сторону и виртуальный, и реальный электорат, обращаясь в равной степени к обоим и стараясь сбалансировать их масштабы. Завоевать симпатии сторонников обоих типов достаточно сложно, но жизненно важно для того, чтобы быть сильным лидером в цифровую эпоху.

После того как в будущем развернется серия неудачных революций, сторонники оппозиционеров потребуют от них не только видения, но и детального плана построения новой страны. Особенно это коснется новых малоизвестных оппозиционных групп, которым придется доказывать обществу свою добросовестность. Естественно, это совпадет с новейшими технологическими тенденциями: с большей прозрачностью и свободным доступом к информации. А их потенциальные сторонники станут все больше напоминать потребителей: их начнут привлекать не столько политические идеалы, сколько маркетинг и сам продукт. Появится больше возможностей для того, чтобы стать лидером (как минимум на словах), но, поскольку кандидатов в лидеры будет много, а людей, действительно способных двигаться вперед, мало, избиратели будут даровать и отнимать свою лояльность с бесстрастной расчетливостью. Однако для оппозиционных движений конкуренция так же полезна, как и для компаний.

Недовольные режимом и готовые выйти на улицу люди вправе рассчитывать на то, что у всех серьезных оппозиционных групп есть

онлайн-представительства, где они представят свое видение будущего правительства: кто займет кресла министров, как будет организован аппарат государственной безопасности, каким образом станут распределяться товары и услуги. Сегодня оппозиционные лидеры часто делают неопределенные заявления, предлагая верить им на слово (особенно в странах, где медленно растет доступность интернета), но хорошо информированное общество будущего потребует от них деталей. Поскольку оппозиция формируется задолго до начала революции (неважно, внутри страны или за границей), ей следует быть готовой к предстоящим событиям и представить обществу не формальные планы, а детально разработанные проекты, которые станут основой новой государственной системы. Если какая-то оппозиционная группа не может или не хочет продемонстрировать такие проекты или неспособна их выполнить, можно сколько угодно превозносить ее организационные способности, но доверие к лидерским и управленческим качествам ее руководителей наверняка окажется под вопросом.

Но даже когда у оппозиционного движения есть надежный план, а также сильные и способные лидеры, остается множество других, не поддающихся контролю переменных, которые способны привести к провалу революции. Во многих обществах глубоко укоренились племенные, религиозные и этнические трения, представляющие собой настоящее минное поле, опасное даже для самого осторожного политического деятеля. Безопасность могут поставить под угрозу внутренние и внешние силы: террористические группы, вооруженная милиция, мятежники, иностранные войска. Нередко причиной революции становятся плохое состояние экономики или неудачная фискальная политика, и даже незначительная корректировка экономического поведения властей (неважно, с каким конечным результатом) может охладить пыл протестующих и скорректировать баланс сил в стране.

Кроме того, неизбежен громадный разрыв между ожиданиями и действительностью. Даже если революция заканчивается «успешно» — к власти приходят новые действующие лица, оптимизм общества зашкаливает, — мало какому правительству удается соответствовать ожиданиям и желаниям своих сограждан. Следствием

широкомасштабных народных восстаний, в которых участвуют миллионы людей (не в последнюю очередь благодаря доступу в интернет), станет резкое разочарование многих из них после окончания революции, когда они почувствуют себя выключенными из политического процесса.

Мы столкнулись с этим в Ливии и в Тунисе, где встречались и с политическими активистами, и с министрами. Ни одна из групп не чувствовала ни полной удовлетворенности, ни признательности народа. После египетской революции столь многие были разочарованы действиями нового военного правительства страны, Высшего совета вооруженных сил, что площадь Тахрир — место, где началась революция, — демонстранты несколько раз оккупировали *снова*. А когда оказалось, что у египтян на первых после революции президентских выборах такой небогатый выбор: или Ахмед Шафик, символ армии, или Мохаммед Мурси, символ «Братьев-мусульман», разочарование и ощущение украденной победы только усилились. Из-за той степени вовлеченности, которую чувствуют люди благодаря доступу в сеть, ожидания оказываются слишком высокими.

Новые руководители постараются удовлетворить этот спрос на подотчетность и прозрачность власти путем реализации инициатив в рамках «открытого правительства», например начнут публиковать ежедневные планы министров и общаться с избирателями на онлайн-форумах, создадут систему максимально прямой связи с населением. Однако это удовлетворит не всех, и они станут основой онлайн-поддержки оставшихся не у дел представителей смещенной политической элиты. Самые разумные из лоялистов постараются воспользоваться разрывом между ожиданиями и действительностью, поддерживая отношения со своей аудиторией в интернете, подпитывая их обиды и готовя почву для попыток реставрации режима. В конечном счете они могут сформировать новое оппозиционное движение.

Виртуальные репрессии и виртуальное сдерживание

Сталкиваясь с самыми разными угрозами революции, власти будут искать быстрые решения этой проблемы. Им придется придумывать

нестандартные ходы. По мере того как интернет становится все доступнее, теряют эффективность традиционные методы — физические репрессии и отключение связи. Старые как мир авторитарные приемы подавления восстания с помощью насилия и ликвидации лидеров плохо работают в эпоху виртуальных протестов, онлайн-активистов и распространения информации в режиме реального времени. В истории очень мало примеров (исключениями стали события на площади Тяньаньмэнь в 1989 году и резня в сирийской Хаме, 1982 год), когда репрессии удавалось сфотографировать или снять на видеопленку, тем более передать эти свидетельства за пределы страны. Если режим контролирует все каналы связи, СМИ и границы, распространение информации становится практически невозможным.

Когда протестующим стали доступны мобильные телефоны и интернет, правящие режимы скорректировали свою стратегию. Теперь они отключают сети связи. Вначале показалось, что это работает (тому есть несколько примеров; особенно это помогло иранскому режиму в ходе протестов 2009 года, начавшихся после выборов: тогда почти полное отключение связи действительно остановило набиравшее силу оппозиционное движение). У египетского президента Хосни Мубарака были все основания полагать, что виртуальные репрессии в состоянии прекратить революционную агитацию на площади Тахрир, развернутую всего два года спустя после иранских событий. Однако эта стратегия уже стала контрпродуктивной.

> Ранним утром 28 января 2011 года руководство Египта, ожидая в этот день быстрый рост антиправительственной активности, отдало распоряжение отключить интернет и мобильную связь на всей территории страны. «Египет уходит из интернета» — гласил заголовок одного из первых постов в блоге, посвященных этому событию[31]. Доступ к социальным сетям и интернет-сервису BlackBerry был блокирован несколькими днями ранее, так что теперь отключение от глобальной сети стало полным[32]. Оно коснулось четырех основных национальных интернет-провайдеров: Link Egypt, Telecom Egypt, Etisalat Misr и Vodafone/Raya, а оказание услуг мобильной связи было приостановлено всеми тремя сотовыми операторами. Утром крупнейшая из телекоммуникационных компаний Vodafone Egypt выступила с заявлением: «Всем операторам сотовой связи было дано распоряжение прекратить оказание

услуг в некоторых районах. В соответствии с законодательством Египта власти имеют право издавать подобные распоряжения, а мы обязаны выполнять их».

Учитывая, что правительство Египта уже контролировало немногие физические каналы связи с внешним миром, в частности оптоволоконные кабели, размещенные в одном из каирских зданий, для полного отключения связи было достаточно обратиться к крупным операторам связи и объявить им требование властей. Как выяснилось позже, компаниям вроде Vodafone ясно дали понять, что, если они не выполнят распоряжение, государственная компания Telecom Egypt физически отрежет их от телекоммуникационной инфраструктуры страны (что сделало бы невозможным оказание услуг, а на последующее восстановление работы понадобилось бы длительное время). До этого власти активно поддерживали планы развития сетей по всему Египту, поэтому у интернет-провайдеров и сотовых операторов не было плана действий на случай чрезвычайных обстоятельств. Эта угроза застала их врасплох. Вообще такой шаг не имел прецедентов в истории: бывало, что власти мешали интернет-провайдерам оказывать услуги населению, но никогда еще не проводили такого скоординированного и полного отключения страны.

Этот шаг привел к противоположным результатам. Как потом отмечали многие египетские и иностранные обозреватели, именно отключение связи спровоцировало протестное движение, поскольку на улицу выплеснулось огромное количество возмущенных людей. С этим согласен CEO Vodafone Витторио Колао. «Правительство ударило по тому, что полагали важным 100% жителей страны: люди посчитали себя ограбленными, и их реакция оказалась гораздо более резкой и негативной, чем предполагали власти», — сказал он нам. Это же подтверждают и многие египетские активисты: «Мне Мубарак не нравился, но это была не моя борьба. А потом Мубарак отнял у меня интернет, и это стало моей борьбой. Поэтому я пошел на площадь Тахрир». В результате такого шага властей движение получило мощный дополнительный импульс. Не будь его — вполне вероятно, что события в Египте развивались бы совсем иначе.

По словам Колао, когда в Vodafone получили распоряжение об отключении сети, прежде всего «убедились, что мы имеем дело с юридически обоснованным требованием. Оно могло быть спорным, но обязано было быть законным». Все операторы связи должны были выполнять условия лицензий, выданных государством, и поэтому, когда в компании выяснили, что требование было законным, у них не

осталось выхода: «Оно могло нам не нравиться, но если бы мы его не выполнили, то нарушили бы закон».

Вскоре после того как в Египте были отключены интернет и мобильная связь, Vodafone пришлось пройти еще одно испытание: в компанию, как и к другим сотовым операторам страны, поступила просьба правительства централизованно разослать SMS всем своим абонентам. И тут, рассказывает Колао, Vodafone сыграла позитивную роль. Вначале, по его словам, тон правительства был вполне нейтральным: «Сегодня вводится комендантский час с шести до девяти». «Это была команда из тех, которые можешь выполнить», — считает Колао. Далее тон сообщений стал патриотическим: «Давайте будем дружить и любить свою страну». «Тоже прекрасно, — говорит Колао. — Но в какой-то момент сообщения стали чересчур политизированными, причем односторонними. Однако мы не могли сказать местным служащим Vodafone: “Не выполняйте требования египетских законов”. Мы обсудили этот вопрос с посольством Египта, с Хиллари Клинтон и правительством США, после чего Vodafone Group PLC, материнская компания, выступила с заявлением, в котором говорилось, что мы [отказываемся выполнять распоряжение властей]. После этого прекратилась передача SMS. Вообще голосовая связь не работала сутки, а передача SMS — четыре или пять дней. Они считали SMS угрозой».

Провал попытки отключить связь в Египте заставит и правительства, и операторов разных стран сделать нужные выводы. Это мобилизовало массы в самой стране и привело в ярость мировое сообщество. За несколько дней иностранные компании и активисты обеспечили египтян альтернативными способами связи, хотя и не во всех регионах. Французская неправительственная организация French Data Network организовала интернет-доступ по коммутируемым линиям (он был доступен всем, у кого имелся домашний телефон), а Google запустила услугу передачи твитов по телефону Speak2Tweet, которая позволяла, позвонив по одному из трех номеров, оставить голосовое сообщение, которое затем размещалось в Twitter.

Витторио Колао рассказал нам, что после событий в Египте руководители крупных операторов связи решили собраться и поговорить о том, как предотвратить повторение подобных случаев и

какую совместную позицию занять, если они все же произойдут. В конечном счете, говорит Колао, «мы решили, что это нужно обсудить в рамках Международного союза электросвязи — агентства ООН, занимающегося вопросами связи, — и четко установить правила поведения». В будущем власти других стран наверняка учтут прецедент с отключением связи в Египте и по-новому оценят свои шансы на выживание в случае, если вдруг решат лишить население возможности общаться. Кроме того, поскольку все большую популярность набирают пиринговые и другие платформы, работающие вне рамок обычных сетей, отключение связи окажется гораздо менее эффективным. Конечно, недальновидные или запаниковавшие представители властей могут планировать чрезвычайные меры в виде буквальной изоляции страны от остального мира: отсоединение оптоволоконных кабелей, уничтожение вышек сотовой связи. Но этот сценарий привел бы к настолько серьезному экономическому ущербу для страны (прекратили бы работу все финансовые и валютные рынки, а также компании, использующие внешние данные), что вероятность его реализации ничтожно мала, каким бы ни был режим.

Впрочем, у репрессивных режимов нет недостатка в других средствах и, столкнувшись с недовольством населения и ростом революционных настроений, они вполне способны отыскать лазейки и воспользоваться ими. Власти придумают иные методы, более тонкие и коварные. Известная стратегия «не можешь победить — возглавь» может быть использована следующим образом: не пытайтесь ограничить доступ в интернет, лучше используйте его. Мы уже писали, что в результате революции данных у правительств есть перед гражданами колоссальное преимущество: они имеют доступ к огромному объему информации о них. Если власти страны будут обеспокоены ростом оппозиционных настроений, их агенты активизируют усилия по прочесыванию социальных сетей в поисках активистов-агитаторов; станут выдавать себя за диссидентов, увлекая «сторонников» в ложном направлении; взламывать известные сайты, где происходит мобилизация оппозиционеров, и вбрасывать дезинформацию; дистанционно включать веб-камеры ноутбуков и планшетных компьютеров без ведома их владельцев, чтобы шпионить за диссидентами; следить за денежными потоками, проходящими через

электронные платежные системы, в надежде выявить иностранных спонсоров. Такое активное использование властями интернета на ранней стадии протестов может привести к тому, что они закончатся не национальным восстанием, а безобидными демонстрациями.

Но даже если изменится природа виртуального подавления оппозиции, набор физических карательных мер, входящих в арсенал спецслужб репрессивного государства, останется неизменным. На уличную жестокость технологии почти не влияют, как показывает страшный пример Сирии, где уже много лет не прекращаются силовые акции против инакомыслящих. Поначалу не верится, что международное сообщество *способно* стать бесчувственным к виду насилия, даже если с течением времени поток кошмарных видео- и фотоматериалов постоянно нарастает. Тем не менее для тех режимов, которые пытаются сохранить какое-то доверие к себе и отрицают свое участие в совершении подобных преступлений, проводить жестокие репрессии в цифровую эпоху — довольно рискованное дело. Благодаря глобальным онлайн-платформам прозрачность жизни повысилась. Это уже сегодня защищает людей, а будет, мы надеемся, защищать еще больше, когда удастся усовершенствовать такие инструменты, как средства распознавания лиц. Любой офицер правительственной армии постарается сдерживать себя или даже решится перейти на сторону восставших, зная, что всего лишь один сделанный чьим-то мобильным телефоном снимок поможет идентифицировать его и «прославить» на весь мир — или заставит власти отдать команду о его устранении. То же самое касается и членов подразделений неформальной «милиции», участвующей в акциях насилия на стороне правительства, таких как банды сторонников партии ЗАНУ-ПФ Роберта Мугабе, орудующие в Зимбабве.

Вместо активного использования интернета в своих целях (или по крайней мере вместе с ним) от властей некоторых стран можно ожидать действий в рамках стратегии, которую мы называем «виртуальным сдерживанием». Чтобы «сбросить пар» и успокоить возбужденное, хорошо информированное общество, они могут вместо полного отключения связи создать некую отдушину, которая позволит людям выплескивать свое недовольство в интернете. Но (и это важно!) только в строго определенных рамках. То есть репрессивные режимы

будущего могут позволить некоторое онлайн-инакомыслие или смягчив жесткие законы, или просто не применяя их, когда оппозиция высказывается, используя контролируемые властью информационные каналы, причем на ее условиях. В конце концов, если дать возможность боливийским защитникам окружающей среды публично предупреждать об опасности ликвидации лесов, это вряд ли станет серьезной угрозой правящему режиму.

На первый взгляд, создание виртуального инструмента для «выпускания пара» кажется выгодным всем: жители страны обретают новую степень свободы и чувствуют причастность к большой политике, а власти набирают очки за проведение реформ (при этом полностью снимая или как минимум снижая риск открытой конфронтации). Наверное, какие-то авторитарные правители действительно осознают ценность реформирования страны и решатся изменить свою политику. Однако в большинстве случаев создание оппозиционной площадки под эгидой властей будет не только неискренним жестом (потому что они не заинтересованы в обратной связи). Усилится опасность того, что с ее помощью спецслужбы будут собирать информацию. Репрессивные режимы уже понимают, насколько стратегически правильно разрешать онлайн-активность, которая может привести к арестам. Еще десять лет назад египетская полиция нравов использовала троллей в чатах и форумах, чтобы заманивать в ловушку гомосексуалистов: им назначали встречу в одном из каирских кафе McDonalds, где устраивали засаду и задерживали[33]. В 2011 году, после тунисской революции, несколько китайских оппозиционеров выступили с онлайн-призывом присоединиться к китайской версии акции протеста, которую планировалось провести у заведений известных американских сетей вроде Starbucks. Этот призыв распространялся по китайским социальным сетям и в микроблогах, поэтому о нем стало известно полиции. Когда активисты собрались в назначенном месте, то столкнулись с невероятным количеством полицейских, которые тут же начали задержания. А ведь если бы власти пресекли онлайн-активность, как только узнали о ней, полиция не смогла бы следить за

действиями диссидентов в виртуальном пространстве, чтобы затем задержать их в реальном.

Политика виртуального сдерживания предполагает, что государства делают шаги, вроде бы направленные на повышение прозрачности, но при этом раскрывают лишь крохи имеющейся у них информации, утаивая большую ее часть. Такие страны будут считаться информационно открытыми и даже признаются в каких-то давних преступлениях. Известные своей коррумпированностью режимы могут сделать вид, что начинают жить по-новому, и предадут огласке случаи взяточничества в судебной системе или в бывшем руководстве страны. Или, скажем, власти однопартийного государства обнародуют информацию, пусть и точную, но не особенно сенсационную или полезную, такую как бюджет министерства здравоохранения. Назначенный «стрелочником» чиновник возьмет на себя ответственность, на него изольется гнев общества, а сам режим останется прежним. В рамках политики псевдооткрытости, когда отсутствует противоречащая официальной точке зрения информация (например, в результате утечки оригинальных документов), несложно фабриковать правдоподобные документы и записи, ведь доказать их фиктивность почти невозможно.

В странах, где применяется стратегия виртуального сдерживания, особенно трудно будет отличать реальную оппозицию от искусственных структур, созданных для «выпускания пара». Для описания звука, пусть и громкого, но не содержащего полезного сигнала, в радиотехнике используется термин «шум». С его политической версией и столкнутся власти авторитарной страны, когда начнут поощрять свободные онлайн-дискуссии. В открытых обществах границы дозволенного для граждан определяют в том числе законы о свободе слова и о недопустимости разжигания ненависти. Там, где отсутствуют законные инструменты, которые позволяют определять, допустимо ли то или иное высказывание, правительству приходится действовать вслепую. А ему очень трудно разобраться в намерениях каждого отдельного пользователя интернета: если он не явный диссидент, не связан с оппозицией и вообще ничем особо не примечателен, как реагировать на его слова властям, которые еще недавно заявляли о своей приверженности открытому диалогу, чтобы

не зайти слишком далеко? Эта незаметность среднего пользователя и создает цифровой «шум», который заводит в тупик правительство, пытающееся вначале оценивать ситуацию и лишь потом реагировать на нее. Любая ошибка — и переоценка, и недооценка происходящего — может оказаться для властей смертельной. С пренебрежением отмахнетесь от онлайн-зыби — получите офлайн-шторм; обрушитесь со всей мощью на онлайн-остряка — подольете масла в огонь нарождающейся виртуальной оппозиции.

В наши дни слишком резкая реакция властей на материалы, которые появляются в интернете, встречается довольно часто, хотя революцию это пока ни разу не спровоцировало. И все же давайте на примере двух заметных событий, произошедших в Саудовской Аравии в 2011 году, рассмотрим типичную для будущего модель обострения ситуации.

В первом случае главную роль сыграла группа консервативных имамов, несогласных с решением саудовского короля разрешить женщинам голосовать на муниципальных выборах 2015 года. В качестве ответного удара они ополчились на участниц кампании «Женщины за право водить» (те открыто нарушили законы Саудовской Аравии и сели за руль). Имамы решили примерно наказать одну из них и приговорили к десяти ударам плетью. Когда стало известно об этом приговоре, рядовые жители страны вступились за нее в интернете, распространив новость далеко за пределы страны. Ответная реакция сотен тысяч людей как в самой Саудовской Аравии, так и за рубежом заставила правительство отменить свое решение меньше чем через сутки. Быстрая реакция короля позволила сбить поднимавшуюся волну, одновременно показав, насколько обеспокоены власти угрозой, которая может исходить от шумной онлайн-толпы.

Второй случай связан с запретом сатирического короткометражного фильма о рынке дорогого жилья Саудовской Аравии. Известно, что нет более верного способа разжечь общественный интерес к чему-нибудь, чем официальный запрет. Так было всегда, так произошло и в этот раз. Фильм под названием «Монополия» (Monopoly) появился на YouTube спустя час после наложения запрета на него и уже через несколько недель собрал более миллиона просмотров.

История с наказанием плетьми говорит о том, насколько важно для властей быстро исправлять свои ошибки. Второй случай наводит на мысль о том, что им необходимо аккуратнее выбирать объекты для атаки. Они никогда не смогут предугадать, что именно трансформирует виртуальное недовольство в реальные уличные

протесты, и каждое решение — реагировать или игнорировать — сродни игре в рулетку. Пока в Саудовской Аравии не было крупномасштабных публичных оппозиционных акций, но, поскольку население этой страны по интенсивности общения в социальных сетях занимает одно из самых высоких мест в регионе (а по количеству просмотров роликов на YouTube — в мире), мелких стычек, подобных описанным, точно будет все больше. Любой просчет правительства может привести к серьезным проблемам.

Последняя «весна»

Чем больше стран получают доступ в интернет, тем более пристально наблюдатели ищут признаки начала региональных революционных эпидемий. Кто-то считает, что следующей будет Латинская Америка с ее колоссальным экономическим неравенством, слабыми правительствами, стареющими лидерами и многочисленным населением, говорящим на двух родственных языках. Другие указывают на Африку: там самые хрупкие в мире государства, а стремительное распространение сотовой связи создает наиболее динамичный мобильный рынок на земле. А возможно, это будет Азия: в этом регионе самое большое население, которое живет в условиях авторитаризма, быстрый рост экономики и многочисленные социальные, экономические и политические проблемы. Уже сделаны первые попытки организовать массовые выступления во Вьетнаме, Таиланде, Малайзии и Сингапуре. С течением времени их количество, конечно же, будет расти.

Население этих регионов все активнее подключается к сети, все лучше информировано о событиях в мире и разделяет настроения людей других национальностей. Тем не менее вряд ли можно утверждать, что приближается еще одна волна протестов, характерная для «арабской весны». (Однако стоит заметить, что эскалации протестов и демонстраций добиться будет *легче*, как показала в сентябре 2012 года реакция на знаменитый фильм «Невинность мусульман» (Innocence of Muslims), охватившая несколько десятков стран.) Арабский мир имеет уникальную региональную идентичность, которую лишь упрочили исторические попытки объединения и

панарабские настроения, существующие уже десятки лет. И, конечно же, свой вклад внесли общие язык, культура и схожие политические системы. Мы уже отмечали, что современные коммуникационные технологии не создали связи между людьми, которыми воспользовались оппозиционеры и участники протестов на Ближнем Востоке, а лишь усилили их.

Кроме того, здесь возникли мощные религиозные сообщества. В отсутствие сильного гражданского общества, не сложившегося в рамках авторитарной модели управления, они по определению были наиболее организованными и часто наиболее полезными для людей неправительственными структурами. Все арабские лидеры, лишившиеся власти в результате волны революций (Бен Али в Тунисе, Мубарак в Египте, Каддафи в Ливии и Али Абдулла Салех в Йемене), создали в своих странах политические системы, которые душили развитие общественных институтов. В этих условиях религиозные организации зачастую заполняли образовавшиеся лакуны, вызывая ненависть диктаторов: самые известные объединения (например, «Братья-мусульмане» в Египте и исламская партия «Ан-Нахда» в Тунисе) или запрещались, или беспощадно преследовались властями, воспринимавшими их как угрозу. В ходе недавних революций участие имамов и других священников нередко придавало протестам определенную легитимность; кроме того, многие люди считают религиозную солидарность важной причиной для присоединения к оппозиции.

В других регионах эти составляющие отсутствуют. Африка, Латинская Америка и Азия гораздо менее однородны с точки зрения культуры, языка, религии и экономического развития, чтобы просто повторить арабскую модель. Там нет такой региональной идентичности, как на Ближнем Востоке, а социальные, деловые и политические связи локализованы сильнее.

Однако невозможно не заметить перемены во всех этих регионах. В каждой стране они могут быть своеобразными: разброс результатов окажется гораздо шире, нежели простая смена режима, но непреложно одно: преобразования будут очень глубокими и на политическом, и на психологическом уровне. Шансы на революционные перемены повысятся во всем мире, однако большая часть стран выдержит этот

шторм — в немалой степени потому, что у них появится возможность видеть чужие ошибки и учиться на них. Общими усилиями власти выработают набор оптимальных инструментов, с помощью которых смогут отражать атаки своих недавно получивших доступ к сети граждан. (У нас есть все основания предполагать это: недаром министры внутренних дел стран с репрессивными режимами встречаются друг с другом и обмениваются знаниями.) Такие проблемы, как неравенство доходов, безработица, высокие цены на продукты и жестокость полиции, существуют повсюду, и властям придется гораздо чаще, чем раньше, идти на упреждающие шаги, меняя свою политику в ответ на требования общества. Даже лидеры относительно стабильных стран чувствуют давление со стороны своих граждан, вооруженных доступом в интернет, и признают необходимость проведения реформ и приспособления к условиям новой цифровой эпохи, поскольку ни одно правительство не может считать себя неуязвимым перед лицом сгущающихся угроз.

Премьер-министр Сингапура Ли Сяньлун как никто другой понимает синергию политического давления и технологических вызовов, ведь этот региональный лидер получил образование в области вычислительной техники. «Интернет хорош как средство для “выпускания пара”, — сказал он нам, — но может использоваться и для разжигания новых пожаров. Опасность, с которой мы встретимся в будущем, состоит в том, что людям гораздо легче быть “против” чего-то, чем “за”». И пояснил, что в молодости все люди хотят быть частью какого-то классного движения и «эта социальная привычка всегда выступать против властей означает, что им больше не нужен план. Теперь ведь очень легко развить бурную онлайн-деятельность по поводу любой мелочи, чем и пользуются оппозиционные силы».

Ли привел в пример недавнее событие в его стране, известное как «карригейт». «Китайский эмигрант и сингапурец индийского происхождения поссорились из-за карри: его запах просачивался сквозь стены», — рассказал Ли. Китаец посчитал, что постоянное приготовление карри является со стороны индийца проявлением неуважения к соседям, и «в типично сингапурской манере» они отправились к посреднику, чья роль заключается в разрешении спора и примирении сторон. Им действительно удалось достичь согласия: индиец мог готовить карри только тогда, когда его соседа не было в городе. На этом бы все и закончилось, если бы

через год посредник не предал эту историю огласке. Мысль о том, что китайцы могут диктовать людям, когда готовить, а когда не готовить карри, привела в ярость индийское сообщество Сингапура, и ситуация стала быстро накаляться. По словам Ли, «то, что начиналось как провозглашение национального дня приготовления карри, привело к тысячам «лайков» и постов, а в конечном счете превратилось в быстро растущее движение, приковавшее внимание всей страны». К счастью для Ли, онлайн-возбуждение по поводу карри не привело к массовым уличным протестам, несмотря на звучавшие тогда весьма жесткие призывы.

Причиной протестов в Сингапуре было не столько карри, сколько растущее недовольство из-за эмигрантов (в основном из материкового Китая), приезжающих в страну и занимающих рабочие места. Неудивительно, что оппозиционеры с такой готовностью ухватились за «карригейт», чтобы снова поднять эту тему. Для Сингапура, который гордится своей стабильностью, эффективностью и властью закона, внезапный гнев, охвативший многих его граждан, стал показателем уязвимости системы. Оказывается, что даже в таком жестко контролируемом пространстве, как Сингапур, сила законодательных ограничений и социальных норм в виртуальном мире очень ограниченна. Для Ли этот эпизод стал первым предвестником грядущего прилива онлайн-активности, который, как признает сингапурский лидер, остановить будет невозможно. Но если даже власти Сингапура чувствуют жар от активно осваивающего интернет гражданского общества, только представьте себе, как должны нервничать менее устойчивые режимы в других частях планеты!

Мы спросили Ли, как, по его мнению, с этим переходом справится Китай, где в ближайшие десять лет доступ к интернету получит почти миллиард жителей этого жестко цензурируемого общества. «Происходящее в Китае полностью не контролирует никто, даже сами китайские власти, — ответил он. — Стране будет нелегко привыкнуть к появлению такого количества онлайн-голосов: сейчас выход в виртуальное пространство имеет меньшинство населения, а будет иметь большинство, и этот переход окажется довольно трудным для руководства Китая». По поводу руководства Ли высказался так: «Последовательно сменяющие друг друга поколения китайских лидеров постепенно утратят харизму и коммуникационные

возможности, необходимые для того, чтобы толкать страну вперед. В этом смысле виртуальный мир будет гораздо более приятным и адекватным китайскому обществу местом, чем мир реальный». И перемены, по его словам, вызовут не только действия «чужаков»: «Скорее, их инициируют люди, находящиеся внутри системы и принадлежащие китайскому истеблишменту, люди, которые испытывают влияние уличных настроений и сами скептически относятся к легитимности нынешнего правительства».

Мы согласны с мнением Ли и других специалистов по этому региону, что Китай не обязательно ждет безоблачное будущее. Некоторые эксперты указывают на снижение темпов экономического роста, старение населения и технологические изменения как признаки того, что вскоре китайскому государству в его нынешнем виде придется бороться за выживание. А их оппоненты убеждены, что грядущие вызовы в конечном счете стимулируют стремление к инновациям и умение решать типичные для китайцев проблемы. И все же нам очень трудно вообразить, как может, не изменившись, пережить переход в новую цифровую эпоху закрытая система с населением в 1,3 млрд человек, огромными социальными и экономическими проблемами, внутренними этническими конфликтами и жесткой цензурой. Всеобщий доступ в сеть умножает ожидания, запросы и стремление к подотчетности властей, и с этим не в состоянии справиться даже государства с самой мощной системой контроля над гражданами. И если правоохранительные органы зайдут слишком далеко или приближенные режима поведут себя слишком неосторожно, причинив физический вред кому-то из граждан, мы увидим более мощные всплески общественного возмущения с требованием призвать правительство к ответу. А поскольку министры терпеть не могут состояния растерянности, давление со стороны *вейбос*[34] и других онлайн-форумов может привести к аналогичному давлению и в конечном счете к переменам, исправляющим «перегибы» однопартийной системы управления страной.

Итак, пусть интернет и не превратит Китай в демократическую страну за одну ночь, но выросшая требовательность общества заставит власти страны активнее реагировать на справедливые запросы

граждан. А если темпы экономического роста снизятся заметно, это может вызвать революционные настроения у части китайского общества. Так что в том или ином виде революцию в ближайшие десятилетия Китай переживет, но вот насколько обширной и эффективной она будет, зависит от готовности населения идти на риск как в онлайн-пространстве, так и на улицах.

* * *

Революции будущего, где бы они ни свершились и какую бы форму ни приняли, могут привести к смене режима, однако это не означает, что страна станет демократической. Генри Киссинджер в разговоре с нами заметил: «История революций — это история долго копившегося недовольства, достигающего точки взрыва, а затем сметающего существующую систему управления. После этого или наступает хаос, или происходит реставрация прежней власти, в зависимости от степени ее разрушения». Иными словами, после успешной революции «чем сильнее разрушена прежняя власть, тем более авторитарная система управления приходит ей на смену», — считает Киссинджер. Более сорока лет он наблюдал за революциями — и успешными, и неудачными — и глубоко разбирается в их устройстве и характере. По его мнению, только в США и Восточной Европе была создана истинная демократия после разрушения существующей системы. «В Восточной Европе революции достигли успеха потому, что опыт жизни при диктатуре был ужасным, а еще потому, что эти страны помнили о своей принадлежности к Западу и сохранили демократические традиции, хотя и не были никогда подлинными демократиями», — объясняет Киссинджер.

Хотя точка зрения Генри Киссинджера на отличительные особенности Восточной Европы хорошо понятна, мы не можем отрицать роли стимулов, которую они играют в успехе революций. Было бы ошибкой забыть о таком важном стимуле, как возможность вступить в Европейский союз (ЕС). Не будь доступно членство в ЕС — в качестве политического мотива для либеральных элит и населения в целом, а также стабилизирующего фактора, — мы бы, скорее всего, увидели много стран, откатывающихся на старые позиции или

охваченные контрреволюцией. Вот почему западным державам пришлось расширять НАТО *и* предлагать членство в ЕС.

Отсутствие демократической культуры стало одной из причин, по которым падение диктаторов в ходе «арабской весны» привело, по мнению некоторых наблюдателей, скорее к разбавленной версии автократии, чем к подлинной демократии Джефферсона[35]. Или, как сказал Киссинджер, «на смену власти, сконцентрированной в руках одного диктатора, пришла система множества партий, как светских, так и религиозных, но в конечном счете оказалось, что доминирующей силой является всего одна мусульманская партия, создавшая формально коалиционное правительство». Создание этого коалиционного правительства «в New York Times назвали проявлением истинной демократии», смеется Киссинджер, но на самом деле «в конечном счете выяснилось, что это правительство без оппозиции, пусть и появившееся в результате выборов».

Киссинджер предсказывает, что в результате цифровых революций, ожидаемых в ближайшие десятилетия, часто будут создаваться склонные к авторитаризму коалиционные правительства, и дело здесь не столько в технологиях, сколько в отсутствии сильных, самостоятельных лидеров. Такие правительства без доминирующего лидера и единого видения становятся способом разделить власть на всех, примирить всех участников революции, но всегда остается риск того, что они не дистанцируются от прежнего режима и старшего поколения политических деятелей.

Однако революции — это не просто проявление недовольства. Они так прочно заняли место в нашем сознании потому, что окружены ореолом романтики и ассоциируются со свободой, независимостью и самоопределением. С развитием технологий появляется все больше сюжетов, способных захватить наше воображение и обеспечить броские заголовки новостей. Даже революционеры-неудачники занимают свое место в коллективной истории и вызывают невольное уважение. Все это стало важным компонентом политического развития человечества, центральным элементом нашего понимания гражданства и социальных контрактов, и приход нового поколения технологий не сможет этого изменить.

Если революции представляют собой результат чьего-то стремления к изменению системы или выражения несогласия с существующим положением вещей, всегда найдутся одиночки и группы людей, которые преследуют те же цели, но посредством наиболее разрушительных, насильственных действий. Террористы и экстремисты останутся такой же частью нашего будущего, какой являются в настоящем. В следующей главе мы рассмотрим очаги радикализма будущего, возникающие как в виртуальном, так и в реальном мире; поговорим о резком расширении поля битвы, которое изменит природу терроризма, и об имеющихся в нашем распоряжении инструментах для борьбы с ним.

Примечания к главе 4

ГЛАВА 5

Будущее терроризма

Мы уже говорили о том, что высокие технологии — это мощный инструмент, который позволяет людям достигать желаемых целей, иногда поразительно конструктивных, а порой на редкость разрушительных. Террористы и экстремисты тоже пользуются связью и интернетом в своих интересах. Это неизбежно, и по мере продвижения технологий растут и риски. Деятельность террористов будет иметь физические и виртуальные аспекты, от подбора исполнителей до проведения терактов. Террористические организации продолжат ежегодно убивать тысячи людей. Это очень плохие новости и для населения, и для властей, которые уже сейчас с трудом обеспечивают защиту своих стран в реальном мире, и для компаний, которые станут еще более уязвимыми.

По-прежнему нельзя исключать страшную вероятность того, что одна из террористических группировок получит в свое распоряжение ядерное, химическое или биологическое оружие. Растет зависимость развивающихся стран от доступа в сеть (к ней так или иначе подключены все компьютерные системы, которыми мы пользуемся), а с ней — уязвимость перед кибертерроризмом в самых разных его формах. Это же относится и к странам с низким проникновением интернета, в которых сегодня отмечено большинство террористических атак. Экстремисты усовершенствуют свои технические навыки и разработают стратегии подбора исполнителей, их обучения и совершения терактов в виртуальном пространстве, отлично понимая, что благодаря все более широкому распространению социальных сетей их атаки вызовут гораздо более сильный резонанс, чем раньше.

Однако развитие коммуникационных технологий принесет террористам не только плюсы, но и минусы, сделав их намного более уязвимыми. Несмотря на все преимущества виртуального мира,

которые они используют (например, возможность создавать повсюду небольшие ячейки, деструктивную деятельность которых сложнее отследить), им все же по-прежнему приходится жить в мире реальном (питаться, находить укрытие, откуда-то звонить и выходить в интернет). Именно это и повышает их уязвимость в новую цифровую эпоху. Посмотрим, как террористам удастся совмещать виртуальный и реальный миры и почему, невзирая на все вновь обретенные преимущества, они обречены на то, чтобы совершать больше ошибок и общаться с большим количеством людей, что в итоге сильно осложнит им жизнь.

Новые рубежи, новые риски

В интернете много опасной информации, доступ к которой могут получить потенциальные преступники и экстремисты. Не совсем ясно только, к чему это приведет в глобальном масштабе. В последние десять лет к сети подключились жители неспокойных регионов с ограниченными экономическими возможностями и длительной историей внутренних и внешних конфликтов. Там наступление новой цифровой эпохи повлечет за собой рост насилия, подпитываемого доступностью высоких технологий. Явным признаком начала этого процесса стало широкое распространение самодельных взрывных устройств (СВУ) профессионального уровня.

Во время поездки в Ирак в 2009 году нас поразило, как легко быть террористом. Один капитан рассказал нам, что американские патрули больше всего боятся самодельных бомб, установленных у обочины дороги. В начале войны они обходились дорого, поскольку сложно было найти компоненты для их изготовления, но со временем и компоненты, и все необходимые инструкции стали доступными любому потенциальному террористу. СВУ образца 2009 года были дешевле и совершеннее своих предшественников, а их устройство предполагало возможность простых переделок, что позволяло преодолеть все известные на тот момент меры предосторожности. К бомбе прикреплялся мобильный телефон, установленный на виброрежим, и взорвать ее можно было на расстоянии, просто позвонив на этот номер. (Вскоре американцы стали применять

ответную тактику — блокирование сигналов сотовой связи, впрочем, с переменным успехом.) Теракты, когда-то казавшиеся сложными и неоправданно дорогими (они обходились боевикам в тысячи долларов), стали обыденным делом: их вызывались совершить за сигареты.

Если решить задачу по сборке самодельного взрывного устройства, детонирующего от мобильного телефона, способен даже старшеклассник, что это означает для будущего? Такие «проекты» стали печальным следствием явления, которое создатель Android Энди Рубин назвал «феноменом творца», восхищающего многих, пока дело не касается терроризма. «Людям будет гораздо проще самим становиться “производителями”, собирая из существующих продуктов нечто новое, что раньше обычному человеку было бы сложно построить», — объяснил нам свой термин Рубин. Возникающая на наших глазах «культура творца» создает невероятное количество оригинальных вещей (3D-принтеры — только начало), но, как всегда в случае технического прогресса, у инноваций есть и оборотная сторона.

Скорее всего, оружием террористов будущего станет некая комбинация бытового беспилотного летательного аппарата («дрона») и мобильного СВУ. Такой дрон можно будет купить через интернет или в любом магазине игрушек. На рынке уже сейчас есть простые вертолеты с дистанционным управлением. Накануне Рождества 2011–2012 годов одним из самых популярных подарков оказался игрушечный квадролет AR.Drone компании Parrot. Он снабжен видеокамерой, а управляется при помощи смартфона. Представьте его более сложную версию: с генерируемой «на борту» сетью Wi-Fi, вооруженной самодельной бомбой... Речь идет о совершенно новом уровне локального терроризма, причем он уже не за горами. В ближайшем будущем практически каждому будут доступны знания, ресурсы и технические навыки, необходимые для сборки такого аппарата. Благодаря системам автономной навигации, о которых мы уже говорили (а купить их можно будет повсеместно), террористам и преступникам станет легче проводить атаки с помощью дронов, находящих цель без вмешательства человека. Однако новые способы совершения разрушительных терактов — это лишь одно из следствий развития технологий, оказывающих влияние на международный

терроризм. Другое — это, конечно же, кибертерроризм (термин появился еще в 1980-х годах), который становится все более серьезной угрозой. В рамках нашей книги мы определим кибертерроризм как «политически или идеологически мотивированную атаку на информацию, данные пользователей или компьютерные системы с намерением причинить разрушительные последствия». (Кибертеррористы и обычные хакеры используют общие тактические средства, но обычно имеют различные мотивы.)

Трудно себе представить группу экстремистов, планирующих кибератаку из афганских пещер Тора Бора, но по мере распространения интернета по миру даже в самых удаленных уголках планеты можно выйти в сеть на приемлемой скорости и раздобыть сложные мобильные устройства. Придется также принять то, что такие группы будут обладать достаточными техническими навыками для проведения кибератак. Все эти перемены, а также тот факт, что наша зависимость от сети создает экстремистам множество потенциальных мишеней, наводят на довольно мрачные размышления.

Возьмем самую простую ситуацию. Если кибертеррористам удастся успешно взломать систему безопасности компьютерной сети банка, окажутся под угрозой все данные *и* деньги его клиентов. (В определенных обстоятельствах даже возможность такой атаки может вызвать массовое бегство вкладчиков.) А если мишенью кибератаки станут транспортная система, полиция, фондовая биржа или электрические сети, террористам удастся нарушить нормальный ход жизни в городе.

Конечно, системы безопасности, имеющиеся у некоторых организаций и в крупных городах, могут предотвратить подобные нападения, но такая защита есть не везде. Нигерия, страдающая от терроризма и отличающаяся слабыми государственными институтами, уже стала мировым лидером онлайн-мошенничества. Когда доступ в сеть помимо жителей Лагоса и Абуджи получит население менее спокойного крестьянского севера страны, где процветает экстремизм, многие потенциальные кибермошенники легко могут оказаться под знаменами радикальной исламистской секты «Боко Харам» (нигерийской версии «Талибана»). И тогда всего лишь несколько новых членов смогут превратить «Боко Харам» из самой опасной

террористической организации Западной Африки в самую мощную кибертеррористическую группировку.

Целями кибератак окажутся не только компьютерные системы. Наркотеррористы, наркокартели и прочие преступники из Латинской Америки уже лидируют в мире по числу похищений людей, однако в будущем традиционные похищения станут более рискованным делом, учитывая современные возможности, в частности использование точной геолокации в мобильных телефонах. (Даже если похитители уничтожат телефон жертвы, ее последнее местонахождение зафиксируется где-то в «облаке». Жители стран, в которых распространен киднепинг, в целях безопасности смогут использовать какие-то портативные устройства (скажем, с булавочную головку), передающие их координаты в режиме реального времени. А те, кто относится к группе особого риска, получат возможность применять средства дополненной реальности, о которых мы писали ранее.) С другой стороны, обычным делом станут виртуальные похищения, то есть кража онлайн-личности состоятельных людей — от банковских реквизитов до аккаунтов социальных сетей, чтобы получить выкуп за эту информацию. Вместо того чтобы удерживать похищенных в джунглях, партизаны из колумбийской леворадикальной повстанческой группировки ФАРК и им подобных предпочтут не брать на себя лишний риск и ответственность и начнут захватывать «виртуальных заложников».

С точки зрения экстремистов, у кибератак множество преимуществ: почти или совсем отсутствует физический риск для исполнителя, требуются минимальные ресурсы, и при этом имеется возможность нанести ощутимый ущерб. Такие нападения дезориентируют жертву, поскольку выследить преступников и определить их местонахождение очень трудно[36]. При этом они вызывают страх у огромного числа потенциальных жертв (а это почти все пользователи интернета). Мы считаем, что наряду с операциями в реальном мире террористы станут все активнее переносить свою деятельность в виртуальное пространство. Пока что доминирует страх перед оружием массового уничтожения (из-за проницаемости границ ничего не стоит доставить в любую страну бомбу, помещающуюся в чемодан). Однако при

следующем теракте, сравнимом по масштабам с терактом 11 сентября 2001 года, террористы могут устроить не захват самолетов или взрывы бомб, а скоординированные атаки в виртуальном и реальном мире, направленные в наиболее уязвимые места инфраструктуры.

> Нападение на Америку может начаться с виртуальной диверсии, возможно, крупномасштабного взлома системы контроля авиационного транспорта, в результате чего множество самолетов получат команду занять неверную высоту или лечь на встречные курсы. Когда начнется паника, вторая кибератака приведет к отключению питания башен авиадиспетчеров в нескольких крупных аэропортах, окончательно приковав все внимание к небесам и вызвав ощущение того, что именно этого все опасались. Тем временем настоящая угроза придет с земли: три мощные бомбы, доставленные через Канаду, взорвутся одновременно в Нью-Йорке, Чикаго и Сан-Франциско. Пока жители остальной части страны будут внимать первым комментаторам, пытающимся оценить ущерб, начнется следующая волна заградительных кибератак, парализующая полицию, пожарных и систему оповещения в этих городах. Чтобы стало еще страшнее, предположим, что, пока спасатели пытаются хоть что-то сделать в условиях масштабных разрушений и огромных человеческих жертв, начинается новая скоординированная компьютерная атака национального масштаба на диспетчерские системы управления и сбора данных (SCADA-системы), обеспечивающие функционирование таких жизненно важных объектов, как системы водо- и электроснабжения, а также газо- и нефтепроводы. Получив контроль над SCADA-системами, террористы смогут делать все что угодно: отключать подачу электроэнергии и водоочистные сооружения, системы тепловизионного контроля атомных электростанций. (Когда в 2012 году компьютерный червь Stuxnet напал на иранский ядерный объект, ему удалось взломать контур управления работой газовых центрифуг.) Будьте уверены, что провести атаку такого уровня чрезвычайно сложно, практически невозможно: только управление SCADA-системами требует детального знания их внутренней архитектуры, многих месяцев для написания кода и очень четкого планирования. Но в том или ином виде координация физических и кибертеракт появится обязательно.

В ближайшие десятилетия лишь у немногих террористических организаций хватит навыков и решимости на проведение терактов такого масштаба. На самом деле технический прогресс усиливает уязвимость лидеров террористов, поэтому их число будет снижаться. Но зато оставшиеся станут еще опаснее. В будущем фору террористическим организациям обеспечит не готовность их членов умереть за свою идею, а хорошее знание высоких технологий.

Так, например, экстремистские группы будут использовать различные онлайн-платформы для планирования, мобилизации

ресурсов, исполнения терактов и, что немаловажно, вербовки новых членов. В интернете, может быть, и не так много сайтов, где творятся мерзкие дела, в том числе размещаются детская порнография и чаты террористов, но они никуда не денутся и в будущем. Террористы создадут собственные безопасные и технически сложные социальные платформы, которые станут выполнять роль виртуальных лагерей боевой подготовки. Такие сайты позволят доносить информацию до потенциальных новых членов организации, обмениваться данными между ячейками преступной сети и формировать онлайн-сообщество единомышленников. Эти своего рода виртуальные конспиративные квартиры будут иметь особую ценность для экстремистов (конечно, при условии, что там не окажется двойных агентов, а система шифрования будет достаточно надежной). Естественно, подразделения по борьбе с терроризмом, правоохранительные органы и независимые активисты попытаются отключить такие сайты или взломать их, но, скорее всего, безуспешно. Ведь в безграничном виртуальном пространстве так просто перенести данные или изменить ключи шифрования и сохранить работоспособность платформы.

Особую важность для будущих международных террористов приобретут медийные навыки: помимо прочего, именно на них станет строиться вербовка новых членов. Большинство террористических организаций уже «пробуют на зуб» медийный маркетинг, и то, что пока выглядит фарсом — сайт «Аль-Каиды», перегруженный спецэффектами, или твиттер сомалийской повстанческой группировки «Аль-Шабааб», — скоро станет новой реальностью.

Ярким подтверждением является недавнее убийство Анвара аль-Авлаки, радикального американского проповедника, связанного с йеменской ячейкой «Аль-Каиды». Известность он во многом приобрел в результате самопродвижения, при помощи вирусных видеороликов и социальных сетей распространяя свои харизматичные проповеди по всему миру. Аль-Авлаки, несомненно, был первой террористической «звездой» YouTube. Его влияние бесспорно, ведь многие и состоявшиеся, и потенциальные террористы называли его своим вдохновителем. Кроме того, именно популярность сделала его первым номером американского списка лиц, подлежащих немедленной

ликвидации. Он был убит в результате удара беспилотного бомбардировщика в сентябре 2011 года.

Мастерское владение аль-Авлаки социальными СМИ произвело большое впечатление на саудовского принца аль-Валида бин Талала аль-Сауда, миллиардера и реформатора, который считал это проявлением более широкой тенденции, характерной для всего региона. «Почти все, даже наиболее нетерпимо настроенные к Западу, религиозные деятели Саудовской Аравии сегодня пользуются высокотехнологичными устройствами, — сказал он нам и добавил: — Многие даже имеют мобильные телефоны и распространяют через социальные сети *фетвы*» (фетвы — это мусульманские указы). Специалисты по Ближнему Востоку понимают, что это говорит о глубоких изменениях, особенно в Саудовской Аравии, где религиозная верхушка особенно активно сопротивляется новым технологиям. И такая тенденция сохранится.

Учитывая важность виртуального маркетинга для будущих террористов, мы предполагаем, что они постараются проникнуть в компании-операторы сотовой связи и интернет-компании. Некоторые исламистские группы уже предпринимали такие попытки. Мааджид Наваз, бывший лидер «Хизб ут-Тахрир» (ХТ) — международной экстремистской организации, ставящей своей целью свержение правительств в странах, где большинство жителей исповедуют ислам, и создание всемирной исламистской супердержавы, — рассказал нам, что эта организация практиковала политику вербовки сотрудников операторов сотовой связи. «Мы разместили пропагандистские материалы у офисов Motorola в Пакистане, а затем привлекли в свои ряды нескольких служащих компании, которые смогли узнать и сообщить нам номера телефонов редакторов пакистанских национальных газет», — сказал он. А потом члены ХТ начали атаковать этих редакторов SMS с пропагандистскими сообщениями, вопросами и даже угрозами. Этим помощь ХТ со стороны служащих Motorola не ограничилась: по словам Наваза, они изменяли персональные данные членов организации, заключивших контракты на мобильную связь, что позволяло тем действовать под чужими именами.

Даже если экстремистские группы и не сделают мобильные компании своими мишенями напрямую, то найдут возможности влиять на эти мощные платформы. Группам вроде «Хамас» или «Хезболла» удается обеспечить поддержку населения за счет того, что они оказывают людям услуги, которые не могут или не хотят в полной мере оказывать официальные власти. Благодаря таким услугам, а также материальной и моральной помощи террористические организации завоевывают доверие и упрочивают лояльность жителей. Поэтому специалисты «Хамас» могли бы разработать серию приложений для недорогих и широко распространенных смартфонов, предлагая пользователям все, что угодно, от медицинской информации и мобильной валютной биржи до детских игр. Такая платформа принесет «Хамас» огромную пользу, а создать ее можно силами членов организации и сочувствующих им энтузиастов. И даже если Apple блокирует приложения по распоряжению правительства США или вступят в действие соответствующие санкции ООН, приложения можно разрабатывать без какой-либо официальной привязки к «Хамас», а затем продвигать их при помощи «сарафанного радио». Влияние такой тактики на молодое поколение было бы огромным.

Поскольку глобальное распространение мобильной связи и интернета делает экстремистские группы все более опасными и сильными, традиционные методы борьбы с ними теряют эффективность. Обычное заключение террористов в тюрьму практически не поможет ослабить их влияние. Они смогут контролировать свои организации и отдавать команды прямо из-за тюремных стен, при помощи тайно пронесенных сотовых телефонов. Конфисковать их или иным образом ограничить их использование будет все труднее, ведь основные элементы смартфонов — процессоры, SIM-карты (на которых можно переносить данные с одного аппарата на другой) и все остальное — становятся все компактнее и мощнее.

Такая практика уже существует, и иногда доходит до комичных ситуаций.

В 2011 году внимание охранников одной из колумбийских тюрем в Медельине привлекла одиннадцатилетняя девочка, которая пришла на свидание к родственнику-заключенному: им показался странным ее свитер. В результате

они обнаружили 74 мобильных телефона и револьвер, закрепленные на ее спине. В Бразилии заключенные выдрессировали почтовых голубей, научив их прилетать в тюрьму с деталями телефонов, а один местный бандит заплатил какому-то подростку, чтобы тот доставлял телефоны за тюремные стены при помощи лука и стрел. (Его поймали, когда одна из выпущенных стрел попала в офицера.)

Это характерно не только для развивающихся стран. Бывший член лос-анджелесской банды рассказал нам, что сегодня в американских тюрьмах стоимость контрабандного смартфона доходит до $1000. За соответствующую цену вы купите даже планшет. Используя эти устройства и популярные социальные сети, можно управлять своим незаконным бизнесом прямо из камеры. Когда в 2010 году заключенные как минимум шести тюрем в американском штате Джорджия одновременно устроили забастовку, протестуя против условий содержания, эта акция была организована почти исключительно при помощи мобильных телефонов, контрабандой доставленных за решетку.

Хорошим примером успешной деятельности заключенных является Афганистан, где уровень проникновения связи один из самых низких в мире. В пригородах Кабула находится крупнейшая в стране печально известная тюрьма «Пуль-э-Чархи». Ее строительство было начато в 1970-х и закончено во время советской оккупации. В те времена там ежегодно гибли десятки тысяч политзаключенных, еще больше людей подвергались пыткам за антикоммунистические настроения. После ввода американских войск тюрьма превратилась в «нервный центр» афганских террористов. В 2008 году в Третьем блоке произошел бунт заключенных, и только тогда власти страны выяснили, что там действовала полноценная террористическая ячейка. Имелся и узел связи, который заключенные использовали для организации терактов за пределами тюрьмы. Дверь запасного выхода была опутана проводами под напряжением, которые, словно вены, проходили между прутьями решетки и освещали коридор мягким красным светом, а на стенах были нарисованы мечи и написаны цитаты из Корана. Оказалось, что Третий блок был взят под контроль членами движения «Талибан» и «Аль-Каиды» еще несколько лет назад. Наладив контрабандную доставку мобильных телефонов и радиоприемников, вербовку сообщников среди заключенных и угрожая охранникам и их семьям, они превратили его в «тюрьму без стен» — безопасное укрытие, которому не страшны удары американских беспилотников. Это позволяло им развивать свою организацию, заниматься вымогательством и координировать теракты в городе, расположенном в двадцати милях от них. Террористы пользовались услугами мелких воров, наркоманов и заключенных-христиан (статус парий в афганском обществе делал их легкой добычей для радикалов), кого-то привлекая за деньги, кого-то заставляя угрозами.

В 2008 году казалось, что для ликвидации или как минимум серьезного ограничения возможностей этой террористической сети достаточно перевести заключенных в разные тюремные блоки. Однако спустя два года, после серии масштабных терактов в Кабуле, тюремные власти официально признали практически мгновенное восстановление террористической сети в «Пуль-э-Чархи». Попытки подавить ее деятельность путем глушения сигналов сотовой связи (чтобы блокировать контрабандные телефоны) ни к чему не привели. В тюрьме содержалось много заключенных высокого ранга, и, хотя охраняла ее афганская армия при поддержке американских инструкторов, похоже, контролировать мобильные сети не мог никто. Когда Джаред приехал в Кабул вместе со специальным представителем в Афганистане Ричардом Холбруком, он посетил тюрьму и встретился с одним из бывших главарей Третьего блока, лидером экстремистов по имени Мулла Акбар Аджи, чтобы оценить, насколько в «Пуль-э-Чархи» изменились условия после подавления бунта 2008 года. В ответ на шутливую просьбу дать номер телефона Аджи опустил руку в карман робы и достал модный смартфон последней модели. А потом гордо вывел на клочке бумаги свое имя и номер: 070-703-1073.

Уроки «Пуль-э-Чархи» говорят о том, что в цифровую эпоху становится опасным содержать в одной тюрьме гангстеров, религиозных экстремистов, наркоторговцев и мелких преступников. Конечно, на свободе эти группы тоже пересекаются и пользуются одними и теми же техническими средствами. Но когда их представители тесно общаются между собой внутри тюремных стен, да еще имеют возможность пользоваться запрещенными устройствами связи, они становятся очень опасной силой. Скажем, банда мексиканских наркоторговцев в обмен на деньги или помощь в выходе на новый рынок поделится с исламистскими экстремистами ценной информацией о возможностях контрабанды оружия. И когда стороны придут к соглашению, каждый может позвонить кому-то из членов своей организации и рассказать о новом партнере. Очень сложно не допустить сделок, которые заключаются в тюрьме, а затем исполняются за ее пределами. Для этого нужно или помещать всех заключенных в одиночные камеры (что нереально), или пресекать контрабандную торговлю (так же нереально, несмотря на огромные

усилия), и поэтому администрации тюрем вряд ли добьются видимых успехов в предотвращении случаев, подобных этому.

Как не допустить осуществления сценария «Пуль-э-Чархи» во всем мире, если мы считаем, что система контрабандных поставок товаров в тюрьмы всегда будет сильнее тех, кто пытается ее уничтожить, а мобильные телефоны продолжат пользоваться таким высоким спросом среди заключенных? Самое очевидное решение — ограничить доступ, глушить сети, чтобы незаконно оказавшиеся в камерах телефоны превратились в дорогие устройства для игры в Tetris. Однако есть все основания полагать, что кто-нибудь найдет возможность обойти и эту проблему. Ее не решат почтовые голуби, а вот небольшие беспилотники, выглядящие как голуби и действующие как мобильные точки доступа сети Wi-Fi, точно смогут.

Правоохранительные органы могут отслеживать и перехватывать разговоры и сообщения заключенных. Полученная таким образом оперативная информация могла бы пролить свет на то, как работают незаконные сети. Еще более радикальное решение — использовать в своих интересах контрабандные поставки товаров в тюрьму и передать в руки заключенных мобильные устройства, снабженные «ловушками для информации». Такие телефоны с загруженным в них программным обеспечением позволили бы тайно отслеживать все, что делается с его помощью. Это эффективнее, чем использовать информаторов, да и безопаснее.

В некоторых странах будет сделано все, чтобы человек, оказавшись за решеткой, совсем исчез из интернета. Его виртуальная личность будет заморожена в соответствии с приговором суда, с его профилем будет запрещено вступать в контакт, обмениваться информацией и даже размещать в нем рекламу, а на испытательный срок придется передать представителю закона все права доступа к своим аккаунтам. В цифровую эпоху эквивалентом ножных кандалов станет специальное программное обеспечение для мониторинга и ограничения онлайн-активности, необходимое не только в очевидных случаях вроде покушения на растление малолетних (иногда судья ограничивает таким лицам доступ в интернет), но и для всех осужденных по уголовным статьям на период их испытательного срока[37]. Человеку,

признанному виновным в инсайдерской торговле, могут временно запретить заключать онлайн-сделки любого рода: никакой торговли, онлайн-
банкинга и даже простой покупки товаров через интернет. А если в отношении кого-то выпущен запретительный судебный приказ, его могут ограничить в посещении страниц в социальных сетях, принадлежащих тем, кого этот человек преследовал, и их друзьям, возможно, даже запретят делать поисковые запросы по их именам и фамилиям.

К сожалению, в век кибертерроризма многие решения подобного рода можно будет обойти, поскольку все больше преступников учатся действовать в интернете скрытно.

Активизация террористов-хакеров

То, насколько серьезно люди воспринимают угрозу кибертерроризма, похоже, зависит от их отношения к хакерам. Некоторых забавляет образ подростка, взламывающего защиту офисной АТС ради забавы. Однако за последние десять лет хакеры сильно изменились, а взлом систем превратился из хобби в довольно обыденное, хотя и неоднозначное занятие. Появление «хактивистов» (политически или социально мотивированных хакеров) и хакерских групп вроде Anonymous говорит о зрелости как идей, так и методов и позволяет представить, что нас ждет в ближайшие годы. Хакеры начнут все чаще объединяться вокруг какой-то общей задачи. Они будут тщательно планировать атаки на тех, кого сочтут подходящей целью, а затем активно делиться информацией о своих успехах. Эти группы окажутся в зоне постоянного внимания со стороны органов власти и институтов, становящихся объектами их атак. Их угрозы придется воспринимать гораздо серьезнее, чем можно судить по сегодняшней их деятельности, которая часто кажется простым хулиганством. Ярким примером этого может быть история WikiLeaks — сайта, на котором публикуются секретные материалы (мы уже говорили об этом), и симпатизирующих ему хакеров.

> Арест основателя WikiLeaks Джулиана Ассанжа в декабре 2010 года вызвал возмущение во всем мире, особенно у политических активистов, хакеров и

специалистов-компьютерщиков, уверенных, что обвинения в изнасиловании имеют политическую подоплеку. Вскоре после этого последовала серия хакерских атак, в частности против компании Amazon, которая отказала WikiLeaks в праве использования своих серверов, и MasterCard и PayPal, прекративших обработку пожертвований в ее пользу.

Эту операцию, официально названную «Месть за Ассанжа», координировала группа Anonymous — объединение хакеров и их сторонников, уже бравшее на себя ответственность за серию шумных DDoS-атак против Церкви сайентологии и других организаций. В ходе операции группа призывала отомстить всем, кто встал на пути WikiLeaks: «Хотя мы не связаны с WikiLeaks, нас объединяют одни цели. Мы выступаем за прозрачность и боремся с цензурой. Попытки заставить WikiLeaks замолчать быстро приближают нас к миру, в котором мы не сможем говорить что думаем, выражать свои мнения и идеи. Мы не можем этого допустить... Вот почему мы намерены использовать имеющиеся у нас ресурсы для информирования общества, атакуя тех, кто мешает вести наш мир к свободе и демократии, и поддерживая тех, кто способствует этому». В течение нескольких часов корпоративные сайты снова заработали, но их отключение вызвало большой резонанс, поскольку потенциально затрагивало миллионы пользователей, большинство которых понятия не имели об уязвимости этих сайтов. Иными словами, хактивисты добились своего. Началось международное расследование, в ходе которого были арестованы десятки подозреваемых в Голландии, Турции, США, Испании, Швейцарии и других странах.

Ни WikiLeaks, ни Anonymous не являются террористическими организациями, хотя кто-то может заявить, что хакеры, крадущие и публикующие персональные данные и секретную информацию, вполне могут считаться террористами. Публикации WikiLeaks создали угрозу множеству жизней и нанесли серьезный ущерб дипломатическим отношениям[38]. Дело в том, что после терактов 9 сентября 2001 года становится все сложнее проводить водораздел между безобидными и опасными хакерами (или в нашем случае между хакерами и кибертеррористами). Такие децентрализованные коллективы, как группа Anonymous, явно демонстрируют, как легко могут организоваться и какое влияние на виртуальное пространство оказывать несколько целеустремленных людей, совершенно не знакомых друг с другом и никогда не встречавшихся лично. Речь даже не идет о какой-то критической массе, ведь выдвинуть свои требования может любой технически подкованный человек (скажем, инженер-компьютерщик), способный управлять тысячами компьютеров. Что будет, когда появится больше таких групп? Все ли

они будут выступать за свободу слова? Недавние события говорят о том, что стоит подготовиться и к другим вариантам.

В 2011 году мир узнал о хакере Comodohaker — двадцатилетнем иранском программисте, по всей видимости, жителе Тегерана. Он отличался от других хактивистов, обычно борющихся с попытками контроля над интернетом со стороны правительства. Как стало известно из его электронного письма в New York Times, наоборот, он считал, что его страна «должна контролировать Google, Skype, Yahoo! и так далее». Comodohaker дал понять, что сознательно мешает работе диссидентов в Иране. «Я взламываю все алгоритмы шифрования, чтобы моя страна могла держать их под контролем», — заявил он.

Если отбросить хвастовство, то Comodohaker действительно смог подделать 500 сертификатов интернет-безопасности, благодаря чему обошел проверку на подлинность сайта и украл конфиденциальную или персональную информацию у ничего не подозревавших жертв. По некоторым оценкам, всего за одно лето в результате его действий была взломана переписка ни много ни мало 300 тысяч иранцев. В качестве своих мишеней Comodohaker выбирал те компании, продуктами которых, как известно, пользуются несогласные с политикой правительства иранцы (Google и Skype), а также те, которым он придавал особое, символическое значение. По его словам, он атаковал голландскую компанию DigiNotar только потому, что в 1995 году в Сребренице голландские миротворцы не смогли защитить боснийских мусульман.

Всего несколько месяцев спустя появился еще один идеологический хактивист с Ближнего Востока. Он называл себя OxOmar, говорил, что живет в Эр-Рияде, столице Саудовской Аравии, и заявлял, что «ненавидит Израиль» и «прикончит Израиль электронным способом». В январе 2012 года он взломал широко известный израильский спортивный сайт и перенаправил его посетителей на другой сайт, где они могли скачать файл с данными о 400 тысячах кредитных карт (по большей части они дублировали друг друга, и общее количество уникальных украденных номеров приближалось к 20 000). OxOmar утверждал, что входит в группировку хакеров-ваххабитов Group-XP, и написал в своем заявлении: «Можно будет повеселиться, увидев 400 000 израильтян, которые выстроились в очередь к банкам и офисам компаний-эмитентов кредитных карт... и услышали о том, что израильские карты не принимают во всем мире, как будто они нигерийские». Через несколько недель, когда из-за DDoS-атак была нарушена работа израильской авиакомпании El Al и фондовой биржи, OxOmar сказал журналисту, что эту атаку он провел совместно с пропалестинской группой хакеров Nightmare и что она будет приостановлена, если Израиль извинится за «геноцид» против палестинцев. Заместитель министра иностранных дел Израиля Дэнни Аялон считает, что «удостоился чести стать

мишенью кибертеррористов». Позднее он подтвердил атаку на свою страницу в Facebook, но добавил, что «хакеры не заставят нас сдаться — ни в интернете, ни где бы то ни было еще».

Действительно ли Comodohacker — молодой иранский программист? Правда ли, что OxOmar проводил свои атаки совместно с другой группировкой? Скрываются ли за этими никами конкретные люди или коллективы хакеров? А вдруг кто-то из этих взломщиков — или они оба — выдуманный персонаж, призванный прикрывать какое-то государство? Любой из сценариев может оказаться правдой — в этом-то и заключается проблема кибертерроризма будущего. Поскольку доказать, откуда началась кибератака, крайне трудно, в распоряжении жертвы нападения имеется весьма ограниченный набор ответных мер независимо от того, кто берет на себя ответственность за него. Такая неопределенность добавляет новое измерение для проведения кампаний дезинформации, и не приходится сомневаться в том, что и государства, и отдельные индивидуумы воспользуются этим преимуществом. И будет труднее понять, с кем или с чем мы имеем дело.

* * *

Внезапно обретенный доступ к высоким технологиям не превращает автоматически людей с радикальными взглядами в кибертеррористов. Существует барьер в виде необходимых для этого технических навыков, который до настоящего времени препятствовал взрывному росту количества хакеров-террористов. Но мы предполагаем, что этот барьер будет играть все меньшую роль по мере того, как распространение сотовой связи и доступа в интернет, а также недорогих мобильных устройств достигнет таких удаленных уголков планеты, как район афгано-пакистанской границы, африканский Сахель или область в месте пересечения границ трех латиноамериканских стран (Парагвая, Аргентины и Бразилии). Хакерами в развивающихся странах, как правило, становятся самоучки, и если предположить, что молодые люди со склонностью к решению технических задач распределены по миру равномерно, то при наличии времени и доступа в сеть потенциальные хакеры способны получить всю необходимую информацию для того, чтобы

отточить свои навыки. Одним из результатов этого станет появление класса виртуальных новобранцев, вполне созревших для вербовки.

В то время как сегодня мы слышим о мусульманах — выходцах из среднего класса, которые живут в Европе и ездят в афганские лагеря подготовки террористов, в будущем может возникнуть обратное движение. Афганцы и пакистанцы будут ездить в Европу, чтобы учиться на кибертеррористов. В отличие от лагерей подготовки террористов с оружейными комнатами, гимнастическими снарядами и полосой препятствий, инженерные лагеря подготовки будут представлять собой несколько ничем не примечательных комнат где-нибудь в Париже или Лондоне, в которых напряженно работают на своих ноутбуках новобранцы — студенты технических факультетов. Полевые лагеря часто видны со спутника; лагеря для подготовки кибертеррористов не отличишь от интернет-кафе.

И террористические группировки, и правительства попытаются привлекать на свою сторону хакеров. Понимая, насколько опытный в техническом смысле персонал повышает их деструктивную мощь, они станут все активнее отбирать инженеров, студентов, программистов и специалистов-компьютерщиков, выращивая следующее поколение воинов киберджихада. Убедить человека стать террористом нелегко, учитывая возможные физические и юридические последствия, поэтому в процессе вербовки по-прежнему важную роль будут играть идеология, деньги и шантаж. В отличие от правительства террористические группировки могут разыграть карту недовольства властью, что усилит их позиции в среде молодых, настроенных против истеблишмента хакеров. Кроме того, решение стать кибертеррористом почти всегда означает меньшую угрозу для здоровья, нежели согласие на мученическую участь террориста-смертника.

Важную роль в том, где именно в мире возникнут кластеры кибертерроризма, сыграет культура. Традиционно самой плодородной почвой для вербовки террористов являлись глубоко религиозные общества с явными элементами радикализма. Так же будет и при подготовке кибертеррористов, особенно после того, как в виртуальном пространстве появятся представители пока не имеющих доступа в сеть регионов. Поведение пользователей в интернете в значительной степени определяется их связями и ближайшим окружением. Мы не

думаем, что в обществе произойдут радикальные социальные изменения исключительно из-за появления мобильной связи и интернета. Зато точно появятся новые каналы коммуникации, больше возможностей для сотрудничества, а также больше виртуальных злодеев.

Конечно же, найдутся государства — спонсоры терроризма, которые пожелают проводить кибератаки. Сегодня наиболее известным спонсором террористических группировок является Иран, снабжающий оружием, деньгами и продуктами такие организации, как «Хезболла», «Хамас», «Палестинский исламский джихад», «Бригады мучеников аль-Аксы» и многочисленные вооруженные формирования в Ираке. Поскольку кибертерроризм кажется все более выгодным занятием, Иран постарается в той же степени развивать и виртуальные возможности своих протеже. Это означает поставки компьютеров и сетевого оборудования, необходимого программного обеспечения, в том числе систем компьютерной безопасности, а также обучение персонала. Вполне возможно, что иранские технические университеты начнут приглашать из Ливана программистов-шиитов с конкретной целью — интегрировать их затем в создаваемую киберармию «Хезболлы». Или передавать им самые дорогие средства шифрования. Или финансировать технические медресе в таких оплотах «Хезболлы», как Миние-Дахие, Баальбек и юг Ливана, создавая там «инкубаторы», в которых талантливых инженеров научат тому, как совершать кибератаки на Израиль. Возможно, вместо передачи шиитским предпринимателям из Бразилии денежных средств, чтобы те начали свое дело (известная тактика иранского режима), власти этой страны будет поставлять им планшетные компьютеры и мобильные устройства с заранее установленным специализированным программным обеспечением.

В вербовке хакеров для любого правящего режима или террористической группировки есть определенный риск. Юных окажется довольно много, и не только по демографическим причинам. Психологи давно пришли к выводу, что тинейджеры удивительно восприимчивы к идее радикализма. (Однако по-прежнему продолжаются споры о том, какие именно факторы отвечают за это: одни считают, что дело в химических процессах, происходящих в

мозге, другие уверены, что причина кроется в социологических параметрах общества.) Так что вербовщикам предстоит не только организовать хакеров, до этого момента явно сопротивлявшихся попыткам любой формальной организации, — им придется иметь дело с подростками. Мы поговорим далее о том, что участие в виртуальной террористической сети потребует высочайшей дисциплины, а это не самая характерная для подростков черта. Большинство молодых людей жаждут одного и того же: внимания, приключений, самоутверждения, ощущения принадлежности и статуса. И при этом всего одна ошибка или брошенное вскользь хвастливое замечание юного хакера (или его знакомого) может привести к провалу всей террористической сети.

Как сегодняшние контртеррористические операции основаны на обмене разведданными и военном сотрудничестве (например, США и их союзников в Южной Азии), так и в будущем двусторонняя поддержка будет обязательно включать виртуальный компонент. Поскольку многие страны с наиболее радикальными режимами совсем недавно получили доступ в интернет, им понадобится иностранная поддержка для обучения тому, как отслеживать деятельность онлайн-террористов и как пользоваться недавно поступившими в их распоряжение средствами. Сегодня крупные поставщики зарабатывают целые состояния на продаже оружия иностранным государствам, соответственно, по мере того как взаимный обмен начнет включать и элементы кибербезопасности, выгоду от этого получат и новые, и давно существующие на рынке компании, специализирующиеся на компьютерной защите.

В ответ на угрозу, которую несет кибертерроризм, изменится и военная политика. Сегодня большинство террористических организаций базируются в несостоятельных странах со слабым правительством или в никем не управляемых регионах. В будущем в таких местах появится мобильная связь и интернет, что позволит террористам заниматься своими грязными делами в виртуальном пространстве, совершенно не опасаясь возмездия. Однако если разведка получит данные о том, что кибертеррористы планируют что-то действительно опасное, придется рассматривать возможность применения чрезвычайных мер вроде ударов беспилотных бомбардировщиков.

* * *

Правительства западных стран также постараются привлечь способных хакеров на свою сторону. На самом деле в США хакеры и государственные агентства уже сотрудничают, по крайней мере в вопросах кибербезопасности. На протяжении многих лет различные ведомства, подобные Агентству передовых оборонных исследовательских проектов США (DARPA) и Агентству национальной безопасности (NSA), набирают талантливых специалистов в ходе таких мероприятий, как серия конференций по компьютерной безопасности Black Hat и съезд хакеров Def Con. В 2011 году DARPA объявило о запуске новой программы Cyber Fast Track (CFT), созданной бывшим хакером, а ныне менеджером проектов в DARPA. Она была направлена на углубление и упорядочение сотрудничества с этими сообществами. В рамках CFT агентство привлекает отдельных специалистов и небольшие компании к работе над краткосрочными целевыми проектами в области сетевой безопасности. Эта инициатива направлена на работу с мелкими игроками, и ее отличает возможность быстро одобрять выделение грантов. В течение первых двух месяцев после запуска программы DARPA одобрило заключение восьми контрактов — иными словами, оно работает со скоростью света по сравнению с нормальными для государственных ведомств темпами. Это позволяет опытным специалистам, которые иначе вряд ли согласились бы работать на правительство, внести свой вклад в важное дело укрепления кибербезопасности, причем легко и в те временные рамки, которые соответствуют срочности задачи. Программа CFT стала одним из признаков сдвига агентства в сторону «демократических инноваций с использованием краудсорсинга», провозглашенного Региной Даган.

Мы спросили Даган о мотивах столь необычного подхода: в конце концов, решение пустить хакеров «в дом» и доверить им серьезные вопросы безопасности вызвало немало удивления. «Многие считают, что хакеры и члены группы Anonymous — все как один злодеи, — говорит Даган. — Но мы пытаемся донести до других то, что поняли сами: слово “хакер” представляет собой описание набора талантов. Те, кого называют хакерами (даже если они сами себя так называют),

должны внести какой-то значительный вклад в дело кибербезопасности, учитывая их подходы к решению проблем, график их решения и способности этих людей бороться с трудностями и добиваться своего». Успех Cyber Fast Track, по ее словам, стал подтверждением жизнеспособности модели. «Не думаю, что нужно пользоваться только этой моделью, но она точно должна входить в наш инструментарий», — сказала Даган.

В ближайшее время следует активнее работать с хакерами и другими независимыми специалистами-компьютерщиками, и мы рассчитываем на то, что правительства западных стран продолжат сотрудничать с ними — или открыто, с помощью программ, аналогичных CFT, или скрытно, по линии разведки. Власти постараются найти за рубежом виртуальных партнеров, чтобы расширить сеть своих тайных агентов и информаторов в реальном мире, вербовать хакеров и других технических экспертов для получения информации и удаленной работы с ними по защищенным онлайн-каналам. Однако у виртуальных партнеров есть очевидные недостатки. Разведчики веками полагаются на личное общение, чтобы удостовериться в том, можно ли доверять источнику, а в данном случае это невозможно. Личное общение не заменишь видеочатом, так что спецслужбам придется придумать эффективный способ проверки своих новых агентов. Завербовать их, возможно, будет легче, чем начать им доверять.

Ахиллесова пята террористов

Террористы будущего быстро убедятся, что высокие технологии необходимы, но использовать их рискованно. Гибель Осамы бен Ладена в 2011 году стала завершением эры пещерного терроризма, полностью изолированного от современной технологической инфраструктуры. Как минимум пять лет бен Ладен прятался на своей вилле в Абботтабаде (Пакистан) без мобильного телефона и интернета. Чтобы оставаться в живых, ему приходилось жить в офлайне. Неспособность постоянно быть на связи значительно уменьшала его возможности и влияние в «Аль-Каиде». Но, по иронии судьбы, именно отсутствие интернета на его вилле помогло сотрудникам спецслужб —

место, где скрывался бен Ладен, им указал один из курьеров, которых был вынужден использовать террорист.

Но, несмотря на то что бен Ладен, скрываясь от преследования, избегал интернета, он все же получал информацию на «флешках», жестких дисках и DVD. Эти средства позволяли ему оставаться в курсе международной деятельности «Аль-Каиды», а его курьерам — передавать большие объемы информации между ним и различными террористическими ячейками по всему миру. Пока он находился «в бегах», эта информация оставалась в безопасности: ее невозможно было получить. Но когда бойцы шестого отряда «морских котиков» захватили дом бен Ладена, они забрали все его устройства, то есть добрались и до самого разыскиваемого преступника в мире, и до сведений о тех, с кем он поддерживал связь.

Наиболее вероятный сценарий террористической атаки новой цифровой эпохи, скорее всего, напомнит теракт в Мумбаи, совершенный в 2008 году, когда десять человек в масках, захватив заложников, выдержали трехдневную осаду, в результате чего было убито 174 и ранено более 300 человек. Для координации и проведения своей операции террористы полагались на базовые общедоступные технологии BlackBerry, Google Earth и VoIP, с помощью которых связывались с командным пунктом в Пакистане, где их командиры следили за освещением событий по спутниковому телевидению и просматривали новости, чтобы в режиме реального времени корректировать свою тактику. Использование высоких технологий сделало этот теракт гораздо более кровавым, чем могло бы быть, но зато, когда был захвачен последний (и единственный выживший) террорист, информация, которую следователи получили от него и, что более важно, из принадлежавших его товарищам устройств, позволила по «электронным следам» обнаружить соучастников и места, где они скрывались в Пакистане. В противном случае на поиски ушли бы месяцы, если вообще удалось бы найти.

Утешает лишь то, что для кибертеррористов цена ошибки всегда будет выше. У обычного пользователя гораздо меньше причин для беспокойства, ведь его свобода и жизнь не зависят от того, насколько тщательно ему удалось скрыть следы в интернете. Конечно, кибертеррористы обладают очень высокими техническими навыками,

но как насчет их друзей? Как насчет родственников, с которыми они переписываются? Нереально ожидать от каждого террориста идеально дисциплинированного поведения в сети.

> Возьмем не связанный с терроризмом пример Джона Макафи, миллионера и пионера в области создания антивирусных программ, которого объявили в международный розыск после того, как он бежал из Белиза, своей новой родины, где его должны были допросить по подозрению в убийстве соседа. Пригласив в свое тайное убежище журналистов из онлайн-журнала Vice для интервью, Макафи разрешил главному редактору сфотографировать себя при помощи iPhone 4S. Ни Макафи, ни его интервьюер не знали, что публикация этой фотографии немедленно выдаст его местоположение, поскольку многие смартфоны (в том числе iPhone 4S) вставляют в фотоснимок метаданные с координатами GPS. И всего-то нужно было, чтобы один из пользователей Twitter заметил эти метаданные — и вот уже власти, да и весь мир знали, что Макафи находится в Гватемале, недалеко от бассейна у ресторана Ranchon Mary. Журналистам из Vice следовало бы об этом знать (о метаданных с координатами известно уже много лет), но по мере того, как смартфоны становятся все сложнее, количество мелких деталей, о которых нужно помнить, растет угрожающе быстро.

По мере того как профессиональная и личная жизнь все заметнее смещается в киберпространство, резко усиливается взаимосвязь различных видов онлайн-деятельности. Компьютеры прекрасно справляются с распознаванием моделей и решением проблем типа поиска иголки в стогу сена, то есть с ростом объема данных возрастает точность их прогнозов. И делают они это быстрее, чем человек. Представьте себе марокканского террориста во Франции, который изо всех сил старается сохранить анонимность своего смартфона в сотовой сети. Он отключил геолокацию и обмен данными, а еще периодически вынимает SIM-карту на случай, если кто-то захочет ее отследить. В качестве последней меры предосторожности он даже выработал привычку вынимать из телефона аккумуляторную батарею, поскольку знает, что даже при выключенном телефоне ему хватает энергии для приема и передачи сигналов. Смартфон у него самый обычный, таких тысячи, засечь его невозможно. Но в полиции знают, что он страстный игрок и постоянно делает ставки на скачках, и знают также четыре места в городе, где действует подпольный тотализатор. Используя эти данные, полицейские сузят список интересующих их телефонных номеров, часто появляющихся в районе этих тотализаторов, от многих

тысяч до сотни или около того. Далее предположим, что кто-то из его приятелей, известных полиции, не так тщательно уничтожает свои следы, как он, и сопоставим имеющийся список из сотни номеров с теми местами, где бывает этот приятель. Этого может быть достаточно, чтобы вычислить номер террориста. Когда-то анализ таких огромных массивов данных казался немыслимым, а сегодня это сделать проще простого — это еще один пример распределения обязанностей между человеком и компьютером в зависимости от сильных сторон каждого из них. Наши действия как в онлайн-, так и в офлайн-среде (а также действия наших друзей, родственников и знакомых) оставляют достаточно следов для того, чтобы компьютер мог нас отыскать.

Чтобы выдать всю террористическую сеть, достаточно всего одной ошибки или почти незаметной связи. Мы как-то разговаривали с бойцом шестого отряда «морских котиков», и он рассказал нам об одном из высокопоставленных руководителей «Аль-Каиды», который чрезвычайно осторожно относился к технологиям, часто менял телефоны и никогда не разговаривал подолгу. Но при всей осторожности в профессиональных делах он вел себя достаточно беспечно в личной жизни. Однажды он позвонил двоюродной сестре в Афганистан и сообщил, что планирует приехать на ее свадьбу. Всего один неверный шаг — и в распоряжении властей оказалась информация, достаточная для того, чтобы найти и задержать его. Если это не террорист-одиночка (что встречается редко) и он не ведет себя в сети идеально дисциплинированно (что бывает еще реже), довольно много шансов, что он выдаст себя еще до теракта. Вероятность совершить ошибку и позволить раскрыть себя так велика, что это внушает оптимизм по поводу будущего контртеррористических операций.

Конечно, среди умных и технически грамотных террористов будет много и достаточно недалеких. Пока продолжается период быстрого распространения интернета, многие действуют методом проб и ошибок, и мы столкнемся со множеством проявлений неопытности, которая может показаться смешной тем, кто вырос в эпоху интернета. Через три года после того, как в Сомали была похищена канадская журналистка Аманда Линдаут (экстремисты из группировки «Аль-

Шабааб» удерживали ее пятнадцать месяцев, пока не получили серьезный выкуп), похитители связались с ней в Facebook, угрожая и требуя еще денег. Некоторые из аккаунтов оказались пустыми, созданными исключительно с целью оказывать на нее давление, а другие — персональными страницами вполне реальных людей. Похоже, что террористы не понимали, какой угрозе себя подвергали, выдав не только свои имена и профили, но и тех, с кем они связаны, все, что когда-то писали на своих и чужих страницах в Facebook, ссылки на какие сайты размещали и так далее. Конечно, на всех подобных случаях будут учиться другие экстремисты, что позволит им избежать таких ошибок в будущем.

По некоторым оценкам, 90% обладателей мобильных телефонов во всем мире круглые сутки держат их на расстоянии не больше метра от себя. В большинстве случаев экстремисты ведут себя точно так же. Они могут повысить бдительность, например периодически вынимать батареи из телефонов, но не смогут отказаться от них совсем. Это значит, что антитеррористические рейды военных и спецслужб будут приводить к лучшим результатам: схватишь террориста — выявишь и всю его сеть. Конечно, не потеряет свою важность допрос после поимки, но настоящая золотая жила — это устройства, которыми пользовался террорист: мобильные телефоны, внешние диски, ноутбуки и фото- и видеокамеры. Управляя захваченными у террориста устройствами от его имени, можно заставить выдать важную информацию или раскрыть свое местоположение его ничего не подозревающих сообщников. Кроме того, такие устройства часто содержат материалы, которые позволят доказать лицемерность публичного имиджа террориста, что сделали американские спецслужбы, рассказав о том, что в компьютере, принадлежавшем Усаме бен Ладену, нашли большое количество порнофильмов. Конечно, слабые места наиболее разумные террористы постараются ликвидировать, например станут пользоваться многими устройствами одновременно. А еще можно направить правоохранительные органы по ложному пути, если подбросить им телефон или компьютер с персональными данными конкурентов или врагов.

Никаких людей-невидимок

Террористы будут придумывать что-то новое, подразделения по борьбе с террористами — разрабатывать контрмеры. Для ликвидации террористической сети может оказаться недостаточным заключить в тюрьму ее участников. Власти, предположим, решат, что слишком опасно допустить, чтобы кто-то из жителей страны находился «вне доступа», то есть не был подключен к технологической инфраструктуре. Понятно, что в будущем, как и сегодня, некоторые люди не захотят пользоваться современными технологиями, онлайн-системами и смартфонами, иметь виртуальные профили. Власти могут решить, что им есть что скрывать, и в качестве контртеррористической меры создать своего рода реестр таких «людей-невидимок». И если у вас нет ни одного зарегистрированного аккаунта социальных сетей и номера сотовой связи и почти невозможно найти ссылки на вас в интернете, вас могут посчитать кандидатом на включение в такой реестр. А попав в него, вы станете объектом отдельного регулирования, включая более тщательный досмотр в аэропортах или даже ограничения на перемещения по миру.

После терактов 9 сентября 2001 года даже страны с исторически сложившейся традицией гражданских свобод все чаще пренебрегают защитой граждан в пользу системы, повышающей безопасность и устойчивость государства. И эта тенденция будет усиливаться. После нескольких успешных атак кибертеррористов намного легче убедить людей пожертвовать чем-то, в частности согласиться, чтобы власти имели возможность более жестко контролировать нашу активность в интернете, ради спокойствия, которое принесут эти новые меры. Побочным эффектом такого сценария помимо гонений на небольшое количество безвредных отшельников будет опасность роста числа злоупотреблений или судебных ошибок, которые допускают представители власти. Это еще одна причина продолжить борьбу за безопасность и сохранение тайны частной жизни.

В ближайшие годы привычное для цифровой эпохи «перетягивание каната» между приватностью и безопасностью станет особенно заметным. Ведомствам, которые отвечают за поиск, выслеживание и поимку опасных лиц, потребуются для этого очень сложные системы

управления данными. Несмотря на все меры, которые принимают для защиты тайны частной жизни пользователи, компании и неправительственные организации, эти системы неизбежно будут получать информацию о людях, не имеющих к терроризму никакого отношения. Вопрос лишь в том, как много и из каких источников. Пока большая часть сведений, которые правительство собирает о населении — адреса, номера паспортов, история правонарушений, данные операторов сотовой связи, — хранится в разных местах (а в некоторых странах до сих пор даже не оцифрована). Отдельное хранение повышает уровень приватности для граждан, но резко снижает эффективность работы правоохранительных органов.

Это та самая «большая проблема данных», с которой столкнулись власти во всем мире: как спецслужбам, армии и правоохранительным органам интегрировать все свои базы данных в единую централизованную систему, чтобы можно было сопоставлять информацию, не нарушая права граждан на частную жизнь? Так, в США ФБР, Госдепартамент, ЦРУ и другие ведомства пользуются разными базами. Компьютеры определяют зависимости, аномалии и прочие значимые факторы намного эффективнее, чем люди, но объединение различных информационных систем (с паспортными данными, отпечатками пальцев, движением по банковским счетам, результатами прослушки телефонных разговоров, данными авиакомпаний) и создание алгоритмов для эффективной установки перекрестных ссылок, удаления избыточной информации и обнаружения сигналов тревоги является невероятно трудной задачей, требующей огромных затрат времени.

Однако «трудная» не значит «невозможная». Все говорит о том, что в современных богатых странах подобные всеобъемлющие информационные системы станут нормой. Нам представилась возможность посетить центр управления мексиканской национальной базой данных о преступниках Plataforma Mexico — впечатляющим, возможно, лучшим образцом интегрированной информационной системы на сегодняшней день. Она размещена в подземном бункере под комплексом зданий Секретариата общественной безопасности в Мехико и объединяет базы данных разведки и полиции, а также информацию с камер видеонаблюдения и других источников,

поступающую в режиме реального времени из всех частей страны. Созданы специальные алгоритмы, которые позволяют выделить паттерны, строить социальные графы и следить за неспокойными районами на случай вспышек насилия, совершения преступлений или природных катастроф, а также других чрезвычайных происшествий. Уровень контроля и технологическая сложность Plataforma Mexico нам показались невероятно высокими (впрочем, как и уровень проблем, с которыми имеют дело мексиканские власти). Да, Мексика — идеальное место для такого пилотного проекта, так как в стране остро стоит проблема безопасности. Однако когда модель будет опробована, что остановит другие страны, пусть и с менее очевидной мотивацией, создать что-либо подобное? В этом и заключается вызов, на который нам придется ответить. Конечно же, любое правительство способно разыграть карту «повышения безопасности» и настоять на необходимости создания столь же сложной платформы. Кто ему сможет помешать?

В начале 2000-х годов, сразу после теракта 11 сентября, нечто подобное предлагалось и в Соединенных Штатах. В министерстве обороны был создан департамент информационного наблюдения и начата работа над программой «Тотальное информационное наблюдение» (TIA). Эта программа продвигалась как главный механизм обеспечения безопасности и обнаружения террористической деятельности. Идея заключалась в том, чтобы собрать все «транзакционные» данные, в том числе о движении денежных средств на банковских счетах, об операциях с использованием банковских карт, о медицинских расходах, и объединить их с прочей информацией о жителях страны в централизованную систему, предназначенную для правоохранительных и контртеррористических ведомств. Предполагалось разработать сложные технологии глубинного анализа данных для поиска паттернов и связей, а также для определения «подписей», оставленных преступниками, которые позволят вовремя обнаружить их и предотвратить новые атаки.

Когда подробности программы TIA просочились наружу, со всех сторон зазвучали предупреждения о потенциальных угрозах для гражданских свобод, тайны частной жизни и безопасности страны в долгосрочной перспективе. Критики программы говорили о

возможных злоупотреблениях столь масштабной информационной системой и называли программу «оруэлловской» по тематике. Развернутая в Конгрессе кампания по прекращению программы TIA вылилась в законопроект о полном исключении расходов на ее реализацию в оборонном бюджете на 2004 год. Департамент информационного наблюдения был ликвидирован, хотя некоторые его проекты нашли пристанище в различных агентствах процветающего блока ведомств, отвечающих за безопасность.

Борьба за сохранение тайны частной жизни будет долгой и трудной. Возможно, несколько первых битв мы уже выиграли, но война далека от завершения. В целом логика обеспечения безопасности всегда оказывается выше соображений приватности. «Ястребам» нужно просто дождаться какого-то серьезного инцидента, который получит широкую огласку, чтобы появились и политическая воля, и общественная поддержка реализации их требований, несмотря на здравые возражения «голубей», — и вот уже отсутствие тайны частной жизни становится нормальным явлением. Прежде чем разрабатывать такие интегрированные информационные платформы, необходимо создать адекватные защитные механизмы для людей и их гражданских свобод, потому что, если возникнет серьезная угроза безопасности, можно зайти слишком далеко. В конечном счете власти, контролирующие систему информационного наблюдения, наверняка выйдут за рамки наложенных на нее законом или судом ограничений, но в демократических государствах с работающей судебной системой и активным гражданским обществом такие ошибки будут исправлены, а виновные понесут наказание.

Ответственные правительства должны признать, что вопросы остаются, и довольно серьезные. Пугающе высок риск неправомерного использования этой мощи, не говоря уже об опасностях, связанных с человеческими ошибками, неверными выводами по результатам анализа данных и простым любопытством. Возможно, полностью интегрированная информационная система, которая получает данные всеми возможными способами и оснащена программным обеспечением, способным интерпретировать и прогнозировать поведение людей, и при этом управляется человеком, обладает слишком большой мощью, чтобы кто-то мог взять на себя

ответственность за нее? Более того, однажды созданная, такая система никогда не будет уничтожена. Даже если когда-нибудь вопрос безопасности станет менее острым, разве правительство откажется по своей воле от столь мощного средства поддержания общественного порядка? Но что будет, если *другое* правительство окажется менее осторожным или более безответственным по отношению к информации, которой располагает? Такие полностью интегрированные информационные системы пока находятся в зачаточном состоянии. Конечно же, предстоит преодолеть некоторые недочеты (такие как нестабильность сбора данных), ограничивающие их эффективность. Постепенно такие системы будут развиваться и, вероятно, вскоре получат повсеместное распространение. А единственным лекарством от потенциальной электронной тирании остается укрепление правового поля и развитие гражданского общества, которое должно быть активным и не допускать злоупотребления этой огромной властью.

* * *

И еще одно замечание — о цифровом контенте и его использовании в будущем. Поскольку объем данных в виртуальном пространстве постоянно растет, а пользователи получают возможность самостоятельно производить, загружать в сеть и транслировать бесконечное количество уникального контента, серьезной проблемой становится его верификация. В последние несколько лет крупные новостные телеканалы перестали использовать только профессиональные видеоматериалы и стали включать в свои передачи материалы, снятые пользователями, например ролики, выложенные на YouTube. Обычно они делают оговорку, что видео не проверено независимым экспертом, но сам факт появления ролика в эфире, в сущности, является неявным подтверждением его подлинности. Кто-то может заявить, что видео смонтировано или сфальсифицировано, но на эти возражения мало кто обращает внимания, часто они просто игнорируются. Такая тенденция доверять непроверенному контенту в конце концов породит движение за более строгую, технически надежную проверку.

Повышается важность проверки во многих аспектах жизни. Мы уже говорили о том, как необходимость в верификации повлияет на наше поведение в сети, о том, что ввиду возможной кражи персональных данных нужно усиливать их защиту, и о том, как повлияют на безопасность биометрические данные. Проверка необходима и для того, чтобы понять, какие из угроз террористов не являются блефом. Чтобы избежать идентификации, большинство экстремистов станут использовать копии SIM-карт и чужих виртуальных личностей, а также целый набор отвлекающих средств для сокрытия своих следов. Правоохранительным органам придется решать трудную задачу: как не утонуть в этом море информации и не потратить время впустую, двигаясь в ложном направлении. Наличие реестров «людей-невидимок» упростит эту задачу, но не снимет ее.

Поскольку основная масса пользователей оценит преимущества использования верифицированных виртуальных личностей, будет больше доверять им, зависеть от их мнения и даже настаивать на верификации, террористам также придется использовать верифицированные каналы, чтобы озвучивать свои требования. Появится множество новых способов проверить подлинность видеороликов, фотографий и телефонных звонков экстремистов. Практика передачи фотографии заложников со свежей газетой в руках как доказательство того, когда она была сделана, уйдет в прошлое. С помощью методов судебной экспертизы, например проверки цифровых водяных знаков, специалисты по информационным технологиям смогут выяснить не только когда, но также где и как был сделан фотоснимок.

Желание общества удостовериться в подлинности контента означает, что экстремистам придется выполнять свои угрозы. Ведь если кто-то из известных террористов этого не сделает, потеря доверия к нему навредит и его собственной репутации, и репутации всей его группировки. Если, скажем, «Аль-Каида» заявит, что один из лидеров организации выжил во время удара беспилотного бомбардировщика, и обнародует якобы подтверждающую это аудиозапись, а компьютерный эксперт-криминалист при помощи программы распознавания голоса докажет, что на пленке записан чужой голос, это ослабит позиции «Аль-Каиды» и сыграет на руку ее критикам. Каждый такой случай

будет подрывать имидж непобедимых, на который рассчитывают многие экстремистские группы при поиске финансирования, вербовке новых членов и запугивании общества. Таким образом, верификация станет важнейшим средством борьбы с насильственным экстремизмом.

Битва за умы и сердца перемещается в интернет. Умелые хакеры и компьютерные эксперты повысят возможности террористических группировок, это правда, однако основную массу их новых членов будут по-прежнему составлять рядовые «пешки». Это молодые, плохо образованные люди, чью неудовлетворенность жизнью экстремисты станут использовать в своих интересах. Мы считаем, что в будущем главное внимание нужно уделять не подготовке налетов и мобильной слежке, а устранению социальных проблем тех, кто рискует попасть в преступные сети при помощи высоких технологий.

По оценкам специалистов, 52% населения Земли моложе 30 лет, и подавляющее большинство этих людей относится к так называемой социально-экономической группе риска, поскольку живут в трущобах или плохо интегрированных в новое общество иммигрантских сообществах, в странах, где плохо исполняются законы, а экономические возможности ограниченны. Бедность, отчужденность, унижение, отсутствие возможностей и недостаток мобильности, да и просто скука делают этих молодых людей легкой добычей. Они выросли в обстановке репрессий и принадлежат к субкультуре, поощряющей экстремизм; они испытывают обиду, которая подталкивает их к радикализму. Это касается и необразованных детей трущоб, и студентов университетов, которые не видят возможностей найти работу после получения диплома.

В нашем центре Google Ideas мы изучали радикализацию населения в разных уголках планеты, в частности с точки зрения роли, которую в борьбе с ней могут сыграть коммуникационные технологии[39]. Оказалось, что процесс радикализации террористов ненамного отличается от радикализации городских банд и других насильственных группировок, например сторонников идеи превосходства белой расы. На нашем «Саммите против насильственного экстремизма», состоявшемся в июне 2011 года, мы собрали больше 80 бывших

экстремистов для того, чтобы обсудить, как люди попадают в исповедующие насилие организации и как их покидают. В ходе открытого диалога участников, среди которых оказались бывшие религиозные экстремисты, националисты, члены городских банд, ультраправые фашисты и сторонники джихада, выяснилось, что все эти группы объединяют одни и те же мотивы и что религия или идеология играют гораздо меньшую роль, чем думает большинство людей. Причины, по которым люди становятся членами экстремистских группировок, сложны; часто это сочетание таких мотивов, как отчуждение от общества, желание принадлежать к группе, стремление к протесту, поиск защиты или жажда опасности и приключений.

Такие настроения разделяют слишком много молодых людей. Новизна заключается лишь в том, что многие из них станут проявлять свое недовольство в сети, сознательно или нечаянно привлекая внимание вербовщиков из террористических организаций. То, что склонная к радикализму молодежь ищет в интернете, есть следствие их опыта в реальной жизни: следствие заброшенности, отторжения, изоляции, одиночества и жестокости. Можно многое для них сделать в виртуальном мире, но чтобы излечить их от радикализма, понадобятся групповые встречи, поддержка, медицинская помощь и значимые альтернативы в реальной жизни.

В битве за умы и сердца молодежи мало одних призывов. Силой тоже ничего не решить. Власти неплохо справляются с поимкой и уничтожением террористов, но пресечь поток новобранцев им не удается. Как сказал в 2010 году в интервью Der Spiegel генерал Стэнли Маккристал, бывший командующий силами США и НАТО в Афганистане, «по-настоящему победить терроризм смогут только две вещи. Первое: власть закона, второе: возможности в жизни. Если вы так управляете страной, что в ней верховенство принадлежит закону, у вас сложится среда, в которой террористом быть очень трудно. А если вы при этом создаете людям возможности в жизни — сюда входит образование и шанс найти работу, — то устраняете главную причину терроризма. То есть на самом деле терроризм не победить военными ударами, это вопрос базовых условий».

Слова Маккристала означают, что перед энтузиастами и компаниями из технологических отраслей открывается широкое поле деятельности. Что может быть лучше с точки зрения повышения качества жизни людей, чем доступ в интернет и возможность связываться друг с другом? В результате развития коммуникаций общество получает такие выгоды, как новые экономические возможности, масса развлечений, свободный доступ к информации, прозрачность и подконтрольность власти. Все это вносит свой вклад в снижение уровня радикализма. Когда выход в сеть получит большая часть населения, можно постараться мобилизовать местное виртуальное сообщество, убедив его сказать «нет» террористам, и потребовать таких же решительных действий от властей. В любом случае противников экстремизма всегда будет больше, и, хотя развитие технологий расширяет возможности фанатиков, им не удастся навязывать единственную точку зрения без того, чтобы не встретить некоторого противодействия. Все, что присуще активной виртуальной среде — больше споров, больше точек зрения, больше противоположных версий событий, — породит сомнения и будет способствовать развитию независимого мышления юной, податливой аудитории. И, конечно, почва будет подготовлена лучше, если благодаря доступу в интернет появятся новые рабочие места.

Самая действенная стратегия ослабления процесса радикализации общества — создание нового виртуального пространства, наполненного разнообразным контентом и способного привлечь молодых людей. Это пространство станет альтернативой прежде единственного их прибежища — экстремизма. Конечно, потребуются большие усилия со стороны многих участников: общественного сектора, частных компаний, местных и зарубежных активистов. Главную роль в этой кампании сыграют мобильные технологии, поскольку большинство людей, выходящих в сеть, будут делать это при помощи мобильных устройств. Телефоны — индивидуальные и мощные платформы, ставшие символом статуса; владельцы полагаются на них и очень их ценят. Установить контакт с враждебно настроенными молодыми людьми с помощью их мобильных телефонов — лучшая из целей, которую мы можем себе поставить.

Разработкой нового контента займутся не только западные компании и правительства. Наибольшего успеха достигнут ультралокальные решения, созданием и поддержанием которых занимаются представители местного сообщества, досконально знающие тему. Ведь просто запускать платформы в *надежде*, что они понравятся отчужденным от взрослого мира подросткам и будут популярными в их среде, все равно что разбрасывать пропагандистские листовки с самолета.

Чужакам не стоит создавать контент, им нужно всего лишь предоставить пространство. Обеспечьте в городе доступ в интернет и дайте горожанам простейшие устройства, а все остальное они сделают сами. Множество технологических компаний разработали инструменты для начинающих, с помощью которых пользователи могут создавать приложения на базе их платформ (среди прочих можно упомянуть Amazon Web Service и Google App Engine). Вообще это блестящая идея — предоставлять людям место для развития бизнеса, написания игр, разработки платформ и строительства организаций в соответствии с собственными представлениями, поскольку она означает, что продуктами компании пользуются (что укрепляет лояльность бренду), и при этом пользователи занимаются тем, чем *сами* хотят. Сомалийцы будут создавать приложения для связи с другими сомалийцами, и это станет эффективным средством против радикализации общества; то же самое сделают для своих соотечественников пакистанцы. У местных жителей появится больше возможностей, одновременно возникает и малый бизнес, и занятие для молодежи. Самое главное здесь — позволить людям адаптировать продукты под свои нужды и не требовать от них большого технического опыта.

Этот процесс станет возможным благодаря сотрудничеству государственного и частного секторов, а также участию активистов и лиц, обладающих влиянием в обществе. Компаниям также следует объединять усилия с местными сообществами и создавать контент совместно. В идеале должно появиться множество материалов, платформ и приложений, говорящих на языке конкретного сообщества, но на одной технологической или системной основе, позволяющей

воспроизводить их в других местах. Ведь если причины радикализации везде одинаковы, схожим должно быть и лекарство.

Технологические компании находятся в уникальном положении и могут возглавить эти усилия на международном уровне. Самые известные из них разделяют все ценности демократического общества и при этом менее ограничены в средствах, чем власти страны. Они могут пойти туда, куда не может пойти правительство, общаться с людьми, невидимыми на дипломатических «радарах», и говорить на нейтральном, универсальном языке технологий. Более того, именно в этой отрасли создаются видеоигры, социальные сети и мобильные телефоны; вероятно, именно здесь знают, как привлечь внимание молодежи и детей из социальных групп, наиболее восприимчивых к вербовке в террористические группировки. Возможно, эти компании не очень хорошо разбираются в тонкостях радикализации или в различиях между населением ключевых регионов — Йемена, Ирака, Сомали, но зато очень хорошо понимают психологию молодых людей и то, в какие игры они любят играть. Только завладев их вниманием, мы можем надеяться завоевать их умы и сердца.

Кроме того, поскольку технологические компании имеют отношение к угрозам безопасности — их продукты используются и террористами, — общество потребует, чтобы они вносили больший вклад в дело борьбы с экстремизмом. Это означает, что им придется не только постоянно совершенствовать свои продукты и ужесточать политику безопасности для защиты пользователей и их контента, но и занять ясную общественную позицию. Как и в случае с капитуляцией MasterCard и PayPal перед политическим давлением в саге WikiLeaks, которая убедила многих активистов, что компании сделали свой выбор, примкнув к противоположной стороне, кто-то посчитает непростительным и бездействие технологических корпораций. Справедливо это или нет, но компаниям придется нести ответственность за использование их продуктов в деструктивных целях. Их культура и ценности будут понятны по тому, каким образом они борются с новыми вызовами. Пустые слова не смогут успокоить хорошо информированную общественность.

Уже сделаны первые шаги в правильном направлении: некоторые компании делают по этому поводу ясные заявления в своих политиках.

Скажем, в YouTube есть проблема объема контента. Ежедневно просматривается более четырех миллиардов роликов (и шестьдесят часов видео загружается каждую минуту), поэтому компания не может изучить все эти материалы, чтобы отсеять те, что содержат неприемлемое содержание, в частности пропагандируют терроризм. Вместо этого YouTube полагается на процесс, в рамках которого сами пользователи помечают контент, который считают недопустимым, после чего видеоролик направляется на рассмотрение команды YouTube и снимается с показа, если нарушает политику компании. В конечном счете должны появиться единые отраслевые стандарты. Все цифровые платформы выработают общие подходы к опасным экстремистским видеоматериалам, размещаемым в сети, как им уже удалось договориться об одинаковой политике в отношении детской порнографии. Между безопасностью и цензурой — очень тонкая грань, и мы должны это учитывать, создавая систему защиты. Совместными усилиями участников отрасли удастся разработать программное обеспечение, способное более эффективно обнаруживать видео с террористическим содержанием. Какие-то компании пойдут так далеко, что станут применять программы распознавания речи, регистрирующие определенные последовательности ключевых слов, или распознавания лиц, чтобы идентифицировать известных террористов.

Конечно, терроризм будет существовать всегда, оказывая деструктивное влияние на общество. Но раз завтрашним террористам придется жить одновременно в реальном и виртуальном мире, их сегодняшняя модель обеспечения секретности и свободы действий окажется разрушенной. За ними будет следить больше электронных глаз; будет фиксироваться больше взаимодействий, и поэтому, какими бы осторожными ни были даже самые способные из террористов, они не смогут найти в виртуальном пространстве идеального укрытия для себя. Если они в виртуальном пространстве, их можно найти. А значит, раскрыть и всю сеть их помощников.

В этой главе мы рассматривали самые темные способы насильственного разрушения будущего мира. Однако, увы, конфликты и войны уже стали частью истории и неотъемлемым элементом жизни общества. Поэтому возникает вопрос: как используют эти

инструменты государства и политические движения для достижения своих целей? Попробуем найти ответ, представив, на что будут похожи конфликты, войны и интервенции в мире, где практически каждый имеет доступ в интернет.

Примечания к главе 5

ГЛАВА 6

Будущее конфликтов, войн и иностранного военного вмешательства

Прежде мы не знали о стольких конфликтах по всему миру. Благодаря обилию информации о жестокости, творящейся повсюду: рассказов, видеоматериалов, фотографий, твитов, — иногда кажется, что в наше время насилия особенно много. Просто, как говорят газетчики, «настоящие новости — плохие новости». Поэтому если что и изменилось в последнее время, так это информированность о конфликтах, а не их количество.

Вообще-то сейчас гораздо более мирное время, чем когда бы то ни было, а уровень насилия в обществе за последние несколько веков резко упал благодаря стабилизации власти государств (которые монополизировали право на насилие и установили верховенство закона), развитию торговли (выгоднее торговать, чем убивать) и расширению международных связей (непонятные и страшные «чужие» стали ближе). Психолог Стивен Пинкер в своем выдающемся масштабном исследовании «Лучшие стороны нашей натуры»[40] отмечает, что «проявление миролюбивых наклонностей», так же как эмпатия, способность отличать добро от зла, здравомыслие и самоконтроль, стимулирует некие внешние силы, которые «удерживают нас от насилия и заставляют сотрудничать с другими и проявлять альтруизм». Как только понимаешь эту взаимосвязь, замечает Пинкер, «мир начинает выглядеть иначе. Прошлое представляется менее безоблачным, а настоящее — менее мрачным».

Если бы это исследование было проведено на пятьдесят лет позже, то, конечно же, пункт «Доступ в сеть» попал бы в список Пинкера, поскольку во времена интернета преступникам скрыться намного труднее, а это ослабляет мотивы к совершению насилия и меняет

баланс сил: желание совершать преступления уходит, препятствовать им — растет.

Тем не менее конфликты, войны, приграничные перестрелки и массовые убийства останутся неотъемлемой частью человеческой истории в течение жизни многих поколений, даже если их характер изменится в условиях технологической эпохи. В этой главе мы поговорим о появлении новых возможностей и угроз и о том, как изменятся в ближайшие годы различные типы конфликтов: дискриминация меньшинств, вооруженные конфликты и иностранное военное вмешательство.

Меньше геноцида, больше дискриминации

Причины насильственных конфликтов столь сложны, что выделить какую-то одну невозможно. Но есть один всем известный фактор (и он изменится в цифровую эпоху): это систематическая дискриминация и преследование меньшинств, когда их представители, став жертвами насилия, начинают мстить своим обидчикам. Мы считаем, что в будущем такие масштабные убийства, которые можно было бы признать геноцидом, совершать будет все труднее, а вот дискриминация, скорее всего, усилится и будет проявляться в самых разных формах. И официальные ведомства, и неформальные группировки, цель которых — дискриминация, с помощью интернета и мобильной связи найдут новые способы маргинализации меньшинств и других сообществ-изгоев, которые сами невольно облегчают задачу своим преследователям тем, что также используют современные технические устройства.

К существующим способам дискриминации виртуальный мир добавит множество новых, и те, кто сумеет синхронизировать свои действия в реальном и виртуальном мире, особенно преуспеет. Если у населения страны есть доступ в интернет, то у властей найдется масса способов оказать давление на одну из социальных групп. Самый простой — это удалить информацию о меньшинстве из национального интернета. Особенно легко это сделать в странах, где существует жесткая система фильтрации контента. Для этого достаточно потребовать от интернет-провайдеров блокировать все запросы,

содержащие определенные ключевые слова, и отключать сайты с запретными материалами. Чтобы предотвратить расползание ссылок по сайтам вроде Facebook и YouTube, можно использовать активный подход к цензуре, аналогичный китайскому, когда цензоры автоматически отключают соединение, заметив запрещенное слово.

Китайские власти в качестве мишени могут выбрать уйгурское меньшинство, проживающее на западе страны. Представители этой этнической группы сконцентрированы в Синьцзян-Уйгурском автономном районе, имеют тюркское происхождение, исповедуют ислам, и у них давние трения с китайцами хань, составляющими большинство жителей Китая. Сепаратистские движения уйгуров несколько раз пытались поднять восстание, но все эти попытки закончились неудачей. Уйгурское население при всей своей немногочисленности представляет собой постоянную головную боль для Пекина, и не нужно обладать слишком развитым воображением, чтобы представить, как власти страны переходят от цензуры информации (вроде запрета материалов о волнениях в Урумчи в 2009 году) к удалению из интернета любого контента, касающегося уйгуров.

Кто-то может посчитать, что такие действия вызваны политической необходимостью, что можно попытаться устранить внутренние угрозы стабильности, просто «стерев» их. И тогда информации об этих группах внутри страны не останется, хотя, конечно, за пределами национального интернета она сохранится. Удаляя информацию, власть унижает меньшинство, как бы игнорируя сам факт его существования, и сильнее изолирует его от остального населения, тем самым получая возможность безнаказанного преследования. Кроме того, если достаточно жесткая цензура продержится долгое время, вырастут следующие поколения титульной нации, которые практически ничего не будут знать об этом меньшинстве и о его проблемах. Трудно заметить удаление контента, оценить потери и поднять тревогу, поскольку в материальном плане эффект от него минимален, зато оно имеет огромное символическое и психологическое значение для представителей меньшинства, глубоко оскорбляя их. Если же кто-то уличит правительство в том, что оно сознательно блокирует информацию, касающуюся меньшинств, официальные лица могут

оправдать свои действия соображениями безопасности или сослаться на компьютерный сбой или неполадки инфраструктуры.

Если же власти захотят не только контролировать всю информацию в рамках политики дискриминации, но и перейдут к полноценным виртуальным гонениям, то найдут способ полностью лишить представителей меньшинства доступа в интернет. Это может показаться несерьезным по сравнению с физическим притеснением, незаконными арестами, актами насилия и экономическим и политическим подавлением, с которыми сталкиваются сегодня во всем мире подвергающиеся гонениям сообщества. Но люди все больше привыкают к использованию сотовой связи и интернета. Мобильные устройства становятся жизненно важными для них, позволяя им раздвинуть свои рамки, получая информацию, работу, доступ к ресурсам и развлечениям, связываясь с другими людьми. Исключение представителей преследуемых меньшинств из виртуального пространства может ухудшить их положение, поскольку в определенном смысле их развитие затормозится и они упустят возможности для роста и процветания, которые, как мы видим, несут всему миру информационные технологии. Им будет сложнее воспользоваться своими деньгами, оплачивать покупки банковской картой и получить кредит.

В Румынии власти умышленно лишают примерно 2,2 млн этнических цыган тех возможностей, которые есть у остального населения страны. Эта политика проявляется в раздельном обучении и экономических притеснениях в виде дискриминации при приеме на работу и отсутствия равного доступа к медицинским услугам (не говоря уже о социальном клейме). Трудно сказать хоть что-то об уровне проникновения мобильной связи и интернета среди цыган: многие из них не указывают при опросах свою национальность из страха наказания. Однако когда они освоят виртуальное пространство, то найдут способы улучшить свое положение. Возможно, когда-нибудь в будущем цыгане даже задумают создать свое виртуальное государство.

Все эти потенциальные возможности будут блокированы, если румынское правительство решит распространить свою политику дискриминации цыган на интернет. Технологическое давление может

принимать различные формы в зависимости от возможностей влияния государства и степени его желания причинять страдания свои жертвам. Если от всех граждан потребуют зарегистрировать свои устройства и IP-адреса (во многих странах уже регистрируют мобильные телефоны и компьютеры) или будут вести реестры «людей-невидимок», то с помощью этих данных румынское правительство легко сможет блокировать доступ цыган к новостям, информации из-за рубежа и платформам, важным с экономической или социальной точки зрения. У пользователей будет или пропадать доступ к их персональным страницам в социальных сетях или услугам онлайн-банкинга и появляться сообщение об ошибке, или практически до нуля падать скорость соединения. Власти могут воспользоваться своим контролем над телекоммуникационной инфраструктурой страны и начать разрывать разговоры по мобильному телефону, глушить телефонную связь в определенных районах или время от времени прерывать соединение пользователей-цыган с интернетом. Возможно, даже договорятся с розничными дистрибьюторами и, действуя через посредников, организуют продажи цыганам неисправных или напичканных ошибками и троянами ноутбуков и смартфонов, чтобы впоследствии установить на них вредоносные программы.

Вместо того чтобы систематически прерывать доступ в интернет (такая тактика может привлечь нежелательное внимание), румынскому правительству было бы достаточно делать это эпизодически: настолько часто для того, чтобы это раздражало целевую группу, но с такими перерывами, чтобы отрицать наличие злого умысла. Конечно, цыгане смогут найти техническую возможность получить хотя бы базовый доступ к сети, но все же блокада окажется вполне действенной и нанесет им серьезный ущерб, ведь эпизодически доступный интернет — не то же самое, что полноценно работающий. Если такие действия будут практиковаться на протяжении достаточно долгого времени, они могут превратиться в политику виртуального апартеида, когда для различных групп в обществе будут установлены разные ограничения на использование мобильной связи и интернета.

Меньшинств, находящихся в «электронной» изоляции, будет становиться все больше, поскольку власти, с одной стороны, в этом заинтересованы, а с другой — у них есть для создания такой изоляции

вся необходимая информация. Инициативы такого рода изначально могут быть реализованы в очень мягкой форме и даже пользоваться поддержкой в обществе, но со временем, после смены власти, способны ужесточаться и приобретать репрессивный характер. Представьте, что ультраортодоксальные религиозные деятели Израиля лоббируют формирование рекомендательного списка проверенных сайтов, своего рода «кошерного интернета», и их просьба удовлетворяется: создание такого отдельного сегмента сети ничем не отличается от списка «безопасных» сайтов для детей[41]. Если после этого ультраортодоксы выиграют выборы и получат контроль над правительством, их первым решением может стать превращение всего израильского интернета в «кошерный». И тогда у них появится возможность еще больше ограничить доступ к сети всем меньшинствам страны.

Такая запретительная политика чревата тем, что ставит представителей меньшинств в положение крайней уязвимости, иногда буквально сокращая их жизнь. Ограниченный доступ к мобильной связи и интернету может быть предвестником физического преследования или силовых акций со стороны государства, а кроме того, лишает его жертв возможности сообщить об опасности и зафиксировать факты причинения вреда. Скоро будет считаться, что если что-то произошло вне медийного пространства, то этого как бы и не было вовсе.

В странах, где меньшинства ущемляются в правах, могут возникнуть явные или негласные договоренности, в рамках которых государство обеспечивает качественной связью только в обмен на согласие предоставлять требуемую информацию и подчиняться правилам. Тем, кто сотрудничает с властями, будут предоставлены более совершенные устройства, более быстрое соединение, шире выбор доступных сайтов и лучшая защита от виртуального преследования. Какой-нибудь житель Саудовской Аравии, представитель шиитского меньшинства, художник и отец шестерых детей, не имеющий никакого желания становиться информатором спецслужб или подписывать обязательство не участвовать в политических движениях, в конечном счете может все же решить, что

сотрудничество с властями имеет смысл: это означает более надежный доход для него или возможности дать более качественное образование его детям. Вообще стратегия привлечения на свою сторону представителей непокорных меньшинств возникла одновременно с самим понятием государства в его нынешнем виде, но для нашей цифровой эпохи характерна именно такая ее реинкарнация.

Ни один из этих механизмов — удаление контента и ограничение доступа — не будет прерогативой государства. Техническая возможность организовать виртуальную дискриминацию независимо от правительства есть у различных заинтересованных в этом группировок и даже отдельных индивидуумов. И первый в мире виртуальный геноцид может быть проведен не властями, а бандой фанатиков. Мы уже говорили о том, что экстремистские организации по мере приобретения нужных технических навыков будут все активнее переходить к деструктивной онлайн-деятельности, и часто это станет аналогом преследования жертв в реальном мире. То же касается и фанатиков-одиночек. Легко представить себе, как ненавидящий мусульман активист, хорошо разбирающийся в информационных технологиях, устраивает «охоту» на сайты, онлайн-платформы и электронные СМИ местной мусульманской общины, причиняя им серьезный ущерб. Это не что иное, как виртуальный аналог травли в реальном мире, когда у жертв отнимают дома, громят лавки, стреляют из-за угла. А если преступник обладает исключительно высокой квалификацией, он сможет ограничить доступ мусульман в интернет, дистанционно отключая определенные маршрутизаторы, глуша сигналы сотовой связи в мусульманских районах или создавая компьютерные вирусы, способные отрезать их от сети.

Более того, для некоторых экстремистов виртуальная дискриминация даже предпочтительнее нынешней тактики. Об этом нам рассказывал бывший лидер неонацистов, а теперь активист движения против пропаганды ненависти Кристиан Пиччолини. «Экстремистским группам и фанатикам-одиночкам запугивать своих жертв через интернет гораздо проще, поскольку он обеспечивает анонимность, устраняет человеческий аспект их взаимодействия и обеспечивает некоторую отстраненность, — объясняет он. — Наличие

интернета в качестве буфера позволяет экстремисту оскорблять жертвы, не боясь наказания и осуждения со стороны знакомых. В обществе расистская риторика справедливо несет на себе некоторое социальное табу, но в виртуальном мире можно высказаться, не раскрывая связи между словами и тем, кто их произносит». Пиччолини считает, что в ближайшие годы число случаев виртуальной агрессии со стороны экстремистов значительно вырастет, поскольку «в случае онлайн-запугивания агрессор меньше боится последствий, а это значит, что такие случаи будут происходить все чаще и становиться все серьезнее».

В обществах, где есть почва для конфликта между различными его группами, традиционно используется практика ограничения одной из них в физических или юридических правах. Мы убеждены, что виртуальные ограничения станут еще одним ее элементом (причем без ущерба для первых двух). Однако из истории мы знаем, что, когда условия для кого-то становятся невыносимыми, вспыхивает открытый конфликт.

Конфликт с участием нескольких сторон

Конфликты в обществе всегда сопровождаются дезинформацией и пропагандой. Свой знаменитый отчет о Галльской войне (58–50 гг. до н. э.) Юлий Цезарь щедро снабдил яркими описаниями порочных варварских племен, с которыми ему пришлось сражаться. Решить, кто «хороший», а кто «плохой», очень важно и очень трудно, учитывая противоположные версии событий. В новую цифровую эпоху эта задача еще более усложнится. Отношение к конфликту будет определяться исходом информационных войн между противоборствующими сторонами: у них есть доступ к электронным платформам, инструментам и устройствам, которые позволяют им убедительно изложить свой вариант истории и донести его до местной и международной аудитории.

> Это можно было наблюдать в ходе конфликта между Израилем и группировкой «Хамас», начавшегося в ноябре 2012 года, когда террористическая организация развязала информационную войну, наводнив виртуальный мир шокирующими фотографиями убитых женщин и детей. «Хамас», опору которого составляют

> униженные и деморализованные люди, смогла использовать в своих интересах многочисленные случаи гибели мирных жителей в секторе Газа. А Израиль сосредоточился на поддержании морального духа нации и устранении двусмысленности вокруг своих действий, используя для этого Twitter-аккаунт @IDFSpokesperson с такими твитами: «Видео: израильский пилот ждет, чтобы район покинули мирные жители, прежде чем нанести удар по цели youtube.com/watch?v=G6a112wRmBs ... #Gaza». Однако реальность информационных войн такова, что симпатии широкой аудитории, особенно плохо осведомленной ее части, привлекает та сторона, которой удается ярко освещать смерть и использовать это в пропагандистских целях. Тактика «Хамас» не нова, но растущая популярность таких платформ, как YouTube, Facebook и Twitter, позволяет организации охватить все более широкую западную аудиторию, которая каждым своим ретвитом, «лайком» и «плюс-один» повышает ее шансы в этой информационной войне.

Участники конфликта постараются парализовать виртуальные пропагандистские возможности противника в самом начале противостояния. Даже после его окончания не всегда понятно, где «черное», а где «белое», что уж говорить о начале! Вот почему равенство пропагандистских возможностей будет сильно влиять на отношение к конфликту мирного гражданского населения, руководителей стран, военных и СМИ. Более того, сама возможность *кому угодно* создать свою версию событий и поделиться ею с миром способна девальвировать любые утверждения, ведь такое количество противоречащих друг другу сообщений просто невозможно проверить. Во время войны следующим по важности и сложности фактором после доступа к технологиям становится управление данными (сбор, индексация, ранжирование и проверка информации, поступающей из зоны конфликта).

Современные коммуникационные технологии позволяют и жертвам, и агрессорам оспаривать слова оппонента более убедительно, чем когда-либо в истории средств массовой информации. В случае с властями страны от качества пропаганды может зависеть исход конфликта: от сохранения действующего режима до иностранного военного вмешательства. А мирным жителям города, окруженного правительственными войсками, удачное любительское видео с привязкой к спутниковой карте поможет опровергнуть утверждения властей и если уж не доказать их лживость, то хотя бы породить

сомнения в их правдивости. Хотя в ситуации, аналогичной вспышке насилия в Кот-д’Ивуар в 2011 году (в ходе спора о результатах выборов), когда обе стороны имеют примерно равные пропагандистские возможности, бывает очень трудно разобраться в том, что происходит на самом деле. А если ни один из противников не контролирует свою армию пропагандистов полностью (когда сочувствующие движению пользователи, независимо от его руководства, производят собственный контент), ситуация становится еще более запутанной.

В эпоху информационных войн непростые вопросы, которые задают себе все наблюдатели: с кем говорить для того, чтобы разобраться в конфликте, какую из сторон поддерживать и как это лучше делать, — становятся еще сложнее. (Особенно это касается случаев, когда не так много иностранцев владеют местным языком или отсутствуют действующие альянсы вроде НАТО или Сообщества развития юга Африки.) Важная информация, необходимая для принятия этих решений, оказывается погребенной под огромным объемом субъективных и противоречивых материалов, поступающих из зоны конфликта. Страны редко вводят войска, если нет полного понимания, что происходит, и даже в этом случае часто колеблются, опасаясь непредвиденных последствий в реальном мире и испытующего ока видеокамер круглосуточных новостных телеканалов[42].

Информационные войны вокруг иностранного конфликта могут влиять на внутреннюю политику и других государств. Предположим, что большинство американцев под впечатлением эмоциональных видеосюжетов одной из сторон конфликта считают, что военное вмешательство для его разрешения с моральной точки зрения оправдано; однако, судя по разведданным, имеющимся в распоряжении правительства США, эти кадры не отражают реального положения вещей. Как в такой ситуации следует поступать властям? Они не могут ни обнародовать секретные материалы, чтобы оправдать свою позицию, ни начать действовать в соответствии с мнением общества. Если обе стороны конфликта представляют одинаково убедительную информацию, наблюдателям остается только ждать. А

именно это и может быть нужно одному из участников противостояния.

В обществах, склонных к конфликтам на этнической или религиозной почве, информационные войны обычно начинаются задолго до появления искры, которая дает сигнал к открытой вооруженной борьбе. При этом мы знаем, что доступ к мобильной связи и интернету часто способен подлить масла в огонь, усилив как исторически существующее, так и искусственно подогреваемое недовольство, не снимая, а подчеркивая противоречия в подходах противников. После того как население получит доступ в анонимное виртуальное пространство, могут обостриться годами дремавшие религиозные разногласия. Мы уже были свидетелями того, как молниеносно вспыхивают религиозные страсти после появления в интернете противоречивых материалов. Достаточно вспомнить скандал по поводу карикатур на пророка Мухаммеда, опубликованных в Голландии в 2005 году, и сопровождавшиеся насилием демонстрации после появившегося в 2012 году фильма «Невинность мусульман». Понятно, что люди придумают еще очень много способов оскорбить друг друга в виртуальном пространстве. Но разжигающие ненависть материалы способны распространяться, словно вирус, и эта их особенность не позволит остаться незамеченным оскорблению, в какой бы части планеты оно ни было нанесено.

Конечно, материалы, предназначенные для использования в информационной войне, не то же самое, что данные разведки. Первые попытки участников конфликта развязать виртуальную информационную войну будут сведены к грубой пропаганде и дезинформации, передаваемой с помощью виртуальных платформ. Но со временем, когда такое поведение станет привычным и для людей, и для государств, эстетический разрыв между разведданными и материалами информационной войны начнет исчезать. Властям придется очень внимательно следить за тем, чтобы не принять одно за другое. Если сторона конфликта с умом подойдет к решению задачи, понимая, что именно нужно сделать для того, чтобы вызвать у аудитории нужное впечатление, она сможет соответствующим образом скорректировать идею и содержание своего сообщения.

Когда в распоряжении одного из участников противостояния имеются государственные ресурсы, он получает заметное преимущество в любой информационной войне. Однако даже если государство контролирует вышки сотовой связи, крупнейшие СМИ и интернет-провайдеров, абсолютной монополии на информацию добиться все равно невозможно. Когда все, что нужно пользователям для съемки, редактирования, загрузки в интернет и распространения контента, — это умещающийся на ладони телефон, никакой режим не может обеспечить своего полного доминирования в сети.

> Мощный толчок оппозиционному движению в Иране дал всего один видеоролик, снятый дрожащей в руках хозяина камерой мобильного телефона в ходе протестов, последовавших за выборами 2009 года, — знаменитое «видео Неды». Неда Ага-Солтан, молодая жительница Тегерана, была убита выстрелом в сердце солдатом-снайпером с крыши, едва выйдя из своей машины, чтобы немного передохнуть в тени здания. Поразительно, что этот случай был снят на чей-то мобильный телефон. Когда кто-то из прохожих пытался ей помочь, это тоже зафиксировали на видео. Эти ролики иранцы передавали друг другу в основном посредством пиринговой технологии через Bluetooth, поскольку к этому времени власти отключили сотовую связь, опасаясь протестов. Ролики все же попали в интернет и стали распространяться как вирус. Все видевшие их, в какой бы части мира ни находились, осуждали иранский режим, а в это время в Иране протестующие проводили марши с требованием справедливого суда над убийцей Неды. Этот шум привлек огромное внимание мировой общественности к протестному движению в Иране, и власти отчаянно пытались его заглушить.

Даже в странах с репрессивными режимами, где вовсю используется шпионское программное обеспечение, виртуальное преследование инакомыслящих и распространение телефонов с заранее установленными программами слежки, целеустремленные люди найдут способы передать свое сообщение за пределы страны. Это можно делать с помощью контрабандных SIM-карт, подпольных «ячеистых сетей» (то есть совокупности беспроводных устройств, где каждое действует как маршрутизатор, в результате чего возникает сеть передачи данных с множеством промежуточных узлов, а не с одним центральным хабом) или «невидимых» телефонов, конструкция которых не предполагает записи разговоров (скажем, в случае, когда все голосовые вызовы осуществляются по технологии VoIP) и позволяет пользоваться интернет-услугами анонимно. Государство не

может запретить распространение таких технологий — вопрос лишь в том, когда это произойдет. (Это касается даже преследуемых властями меньшинств, которых пытаются ограничить в использовании интернета.) Задолго до появления видео Неды в Иране попытались запретить использование спутниковых тарелок, но это привело лишь к *дальнейшему* распространению спутникового телевидения в стране. Сегодня иранский подпольный рынок спутникового оборудования — один из крупнейших в мире в расчете на душу населения, на нем зарабатывают даже некоторые члены правящего режима.

> Геноцид 1994 года в Руанде — крупномасштабный конфликт доцифровых времен, который унес, по некоторым оценкам, жизни 800 тысяч человек, наглядно показал, к чему может привести диспропорция информационных возможностей. В 1994 году радиоприемники были у всех народностей страны: хуту, тутси и тва, — но радиостанции контролировались хуту. Не имея возможности ответить, тутси оказались бессильными перед пропагандой и призывами к насилию, звучавшими в радиоэфире. Когда тутси пытались организовать собственное радиовещание, правительство, в котором доминировали хуту, направляло в офисы радиостанций полицию и бросало за решетку их персонал. Если бы у народности тутси в годы, предшествующие геноциду, были мощные мобильные устройства, аналогичные нынешним, возможно, в общественное мнение Руанды можно было внести ноту сомнения относительно правдивости правительственной пропаганды и кто-то из хуту мог бы посчитать ее недостаточно убедительной для того, чтобы поднять руку на своего соседа-тутси. Тутси могли бы транслировать свои материалы с мобильных устройств, не спрашивая разрешения у властей и не нуждаясь в посредниках для их создания и распространения. В ходе резни имена и адреса прятавшихся тутси передавали по радио, и остается только предполагать, как все сложилось бы, будь у жертв геноцида альтернативное каналы связи, например основанные на пиринговых сетях.

Последствия новых правил игры будут долгосрочными. Однако при всей потенциальной пользе этих правил никто не сможет предсказать, что именно мы утратим из-за устранения традиционных барьеров. Мы уже говорили о всплеске дезинформации, которая приведет к неверной интерпретации событий или неточному расчету ответных мер всеми действующими лицами конфликта. Вовсе не каждое жестокое преступление является актом геноцида, то есть систематического уничтожения представителей определенной этнической или религиозной группы. Дезинформация, даже распространяемая на

локальном уровне, способна создать серьезные проблемы: что будет делать местная власть с ворвавшейся в здание городского совета и требующей правосудия разъяренной толпой людей, посмотревших сфальсифицированный видеоролик? Представители властных структур будут постоянно сталкиваться с подобными вопросами, и им придется искать ответы, способные разрядить обстановку.

Лучшее и, возможно, единственно верное решение этих проблем — цифровая верификация контента. В конфликте, участники которого чрезвычайно активно ведут себя в виртуальном пространстве, внести какую-то ясность можно, только доказав, что фотография — это монтаж (проверив цифровой водяной знак), что видео было выборочно отредактировано (найдя владельца исходного ролика, из которого удалили отдельные фрагменты) или что якобы погибший человек на самом деле жив (проследив за его виртуальной личностью). В будущем свидетель нападения самозваной милиции в Южном Судане сможет к своим материалам добавлять цифровые водяные знаки, биометрические данные и спутниковые координаты, чтобы придать вес своим заявлениям, — это пригодится при общении с полицией или СМИ. Следующая очевидная стадия процесса — цифровая верификация. Сейчас журналисты и представители властей проводят перекрестную проверку полученной информации при помощи сведений из других источников. Когда большую часть работы возьмут на себя компьютеры, получить надежный результат будет еще легче.

В будущем могут быть созданы специальные группы международного мониторинга и проверки информации. Их станут направлять в зону конфликта, объективность освещения которого в сети вызывает сомнения. Как и Красный Крест, группы международного мониторинга и проверки информации могли бы считаться нейтральными агентами, только в их случае чрезвычайно хорошо оснащенными технически[43]. (Им не нужно постоянно находиться в зоне конфликта: иногда такую работу можно делать и через интернет. В тех же случаях, когда коммуникационная инфраструктура развита плохо или полностью контролируется одной из сторон противостояния, будет полезно оказаться в непосредственной близости от места событий, а также владеть языком

и знать культурные особенности их участников.) Сделанная такой группой отметка о достоверности материала была бы очень ценной и позволила бы средствам массовой информации и всем заинтересованным лицам и организациям относиться к нему всерьез. Конечно, государство или противоборствующие стороны могут отказаться от такой проверки, но это обесценит созданный ими контент и вызовет подозрения в его фальсификации.

Группы мониторинга и проверки информации будут изучать данные, а не дела, что придаст большой вес их выводам. Ознакомившись с ними, международное сообщество могло бы принимать решения о военном вмешательстве, отправке гуманитарной помощи или введении санкций. И, конечно же, такое доверие и ответственность означают неизбежные злоупотребления: группы мониторинга будут так же подвержены коррупции, как и другие международные организации. Правящие режимы постараются наладить с ними сотрудничество с помощью взяток или шантажа; кроме того, эксперты группы могут стать жертвой собственной предвзятости, которую обнаружат слишком поздно. Тем не менее в состав большинства групп международного мониторинга и проверки информации войдут достойные доверия технические специалисты и журналисты, и их присутствие в зоне конфликта повысит безопасность и обеспечит большую прозрачность действий всех его участников.

* * *

Помимо ведения маркетинговых войн, участники конфликта атакуют виртуальные активы, ценные, по их мнению, для противника. В качестве мишеней могут выступать сайты, онлайн-платформы и коммуникационная инфраструктура, имеющая стратегическое или символическое значение. Против этих объектов возможно использование распределенных атак типа «отказ в обслуживании» (DDoS), вирусов и другого кибероружия. Виртуальная борьба — от вялого противостояния до полномасштабных боевых действий — станет одной из составляющих тактики сторон конфликта. С помощью кибератак и разрушения коммуникаций противника можно не только помешать ему вести информационную войну, но и усложнить доступ к

ресурсам, информации и поддерживающей его аудитории. Успешный взлом компьютерной сети или базы данных позволит узнать о планах, распространять дезинформацию, действовать на опережение и даже следить за важными мишенями (например, получив мобильные номера лидеров противника и используя специальные приложения для определения местоположения абонентов).

Виртуальные атаки могут быть неспровоцированными или, скажем, продиктованными желанием мести. Сторона, проигравшая в ходе территориального конфликта, станет мстить противнику, выводя из строя ее пропагандистские сайты и лишив возможности громко заявлять о своей победе. Неэквивалентный обмен, но хоть что-то... Такой виртуальный аналог бомбардировки министерства связи и информации часто становится одной из первых целей в ходе реального конфликта. Репрессивные режимы смогут находить и выводить из строя финансовые порталы, используемые революционерами для получения денежных средств от представителей диаспоры. Хакеры, симпатизирующие какой-либо из сторон конфликта, будут пытаться взломать все, чем владеет ее противник: его каналы на YouTube, базы данных на его серверах. Когда НАТО начало военную операцию в Сербии в 1999 году, сочувствующие сербам хакеры атаковали сайты министерства обороны США и НАТО, причем небезуспешно. (Несколько дней практически «лежал» сайт службы по связям с общественностью НАТО, посвященный Косово; плохо работал почтовый сервер ведомства.)

В ближайшие десятилетия мир увидит появление первого в истории «умного» повстанческого движения. Конечно, для смены правительства по-прежнему необходимы оружие и люди, но теперь есть новые стратегии и современные технологии. Еще до объявления о начале кампании можно атаковать государственные линии связи, зная, что те представляют собой фактический (хотя и неофициальный) костяк оборонительной системы властей. Для этого повстанцам нужно получить от симпатизирующих им иностранных правительств все технические компоненты, необходимые для атаки: компьютерных червей, вирусы и биометрическую информацию, а затем вывести сети из строя — извне или изнутри. Виртуальный удар по инфраструктуре должен застать власти врасплох, а если атакующим удастся не

оставить следов, то еще и заставить ломать голову над тем, откуда пришла беда и кто за ней стоит. Желая еще больше запутать противника, повстанцы могут оставить ложный след, чтобы подозрения пали на кого-то еще. Пока правительство будет залечивать виртуальные раны, повстанцы нанесут новый удар, на этот раз методом «спуфинга» («обманывая» сетевое оборудование и выдавая себя за авторизованных пользователей), чтобы еще больше дезориентировать и нарушить сетевые процессы. (Если взломщикам удастся получить доступ к биометрической базе, это позволит похитить данные высших чиновников и от их имени делать в интернете какие-то заявления или совершать подозрительные покупки.) А затем повстанцы нацелятся на материальные активы, скажем, линии электропередач, и отключат их, чем вызовут волну недовольства населения, ошибочно направленного против правительства. Так «умное» повстанческое движение без единого выстрела, с помощью всего трех виртуальных ударов сможет мобилизовать массы на борьбу с правительством, даже не подозревавшим до этого момента о наличии внутреннего врага. После этого можно начинать военную операцию против властей, открыв второй фронт уже в реальном мире.

* * *

На будущие конфликты повлияют еще две четкие и в целом позитивные тенденции, ставшие следствием широкого доступа к мобильной связи и интернету. Во-первых, коллективная мудрость виртуального сообщества, во-вторых, невозможность полного удаления данных, которые могут использоваться в качестве доказательств (мы уже обсуждали это), ведь из-за этого тем, кто виновен в насильственных действиях, труднее отрицать свои преступления или преуменьшать их масштаб.

Коллективная мудрость виртуального сообщества — вещь неоднозначная. Многие наблюдатели осуждают некоторые крайности, присущие онлайн-среде, такие как агрессивная посредственность «стадного мышления» (консенсус, вырабатываемый группами пользователей) и характерная недоброжелательность посетителей

форумов, социальных сетей и других виртуальных площадок, подпитываемая анонимностью интернета. В свою очередь их оппоненты указывают на высокую степень точности и надежности основанных на краудсорсинге информационных платформ вроде Wikipedia. Каким бы ни было ваше мнение по этому поводу, ясно, что коллективная мудрость пользователей так или иначе скажется на будущих конфликтах.

Учитывая возросшую роль информации, к силовому противостоянию подключится большее количество людей, внося свой вклад в фиксацию происходящего. Благодаря распространению мобильных телефонов о происходящем будет знать больше жителей страны, чем в прежние времена, а с помощью интернета в конфликт окажется вовлеченным множество иностранных наблюдателей. В среднем на стороне добра людей всегда больше, чем на стороне агрессора. При наличии осведомленного о противостоянии населения есть потенциальная возможность мобилизации граждан против беззакония или пропаганды: если недовольных достаточно много, они найдут способ быть услышанными и начнут действовать, даже если поводом для их недовольства станет спор о приготовлении карри, как в Сингапуре.

Неуправляемость интернета может приводить к виртуальным самосудам, что иллюстрирует история с китайскими «поисковиками человеческой плоти» (*ренроу соусуо инцинь*).

> По сведениям Тома Доуни, которые он привел в своей нашумевшей статье, опубликованной в марте 2010 года в New York Times Magazine, несколько лет назад в виртуальном пространстве Китая возникла тревожная тенденция: пользователи интернета стали объединяться для травли лиц, вызвавших общественный гнев, выследив или вычислив их. (Это явление не ограничивается определенной онлайн-платформой или только китайским сегментом интернета, просто в этой стране оно особенно заметно благодаря нескольким громким случаям такого рода.) В 2006 году на китайских форумах появился страшный видеоролик о том, как женщина в туфлях на высоких каблуках насмерть затоптала котенка, и вся страна начала ее розыски. В результате скрупулезной детективной работы общими усилиями убийцу обнаружили в небольшом городке на северо-востоке Китая, и, когда ее имя, номер телефона и место работы стали известны общественности, ей пришлось спасаться бегством, как и тому, кто снимал этот видеоролик. Оказалось, что не только компьютеры могут отыскать

иголку в стоге сена: на то, чтобы найти эту женщину среди более миллиарда китайцев, понадобилось всего шесть дней.

Такое поведение толпы может привести к хаосу, но это не значит, что стоит отказаться от попыток обуздать его и направить в правильное русло. Предположим, что целью китайских пользователей была бы не травля убийцы котенка, а намерение отдать ее в руки правосудия. Если объединить усилия множества людей в ситуации внутреннего конфликта, когда государственные институты разрушены или потеряли доверие населения, это позволит получать более полную и точную информацию о происходящем, выслеживать находящихся в розыске преступников и заставлять их нести ответственность за содеянное.

Важность и полезность правосудия, основанного на краудсорсинге, блекнет в сравнении с еще одной приметой времени: невозможностью полного удаления данных. Очень важно как можно быстрее доводить информацию о совершаемой где-то жестокости до глобальной аудитории, а также хранить ее бесконечно долго и сделать доступной для всех, кто хочет на нее сослаться (для наказания виновных, отправления правосудия или для дальнейшего изучения). Возможно, власти и террористы обладают преимуществом благодаря автоматическому оружию, танкам и авиации, но им придется бороться с трудным противником — невозможностью уничтожить следы своих преступлений. Если правительство попытается блокировать связь, ему удастся сбить поток документальных материалов, уходящих за границу, но полностью остановить его не получится. Главное, что наличие этих свидетельств, пусть поначалу и вызывающих у кого-то сомнения, повлияет на пути развития конфликта, способы его разрешения и возможные последствия.

Преступника страшит наказание за содеянное или хотя бы его угроза, именно поэтому он стремится уничтожить следы. А в отсутствие неопровержимых улик противоположные версии событий могут запутать следствие и суд, причем это касается как граждан, так и государств.

В январе 2012 года Франция и Турция были втянуты в дипломатический конфликт после того, как французский сенат принял

закон (отмененный месяц спустя Конституционным советом страны), в соответствии с которым отказ признавать массовые убийства армян в Оттоманской империи в 1915 году геноцидом приравнивался к преступлению. Власти Турции, отрицавшие факт геноцида и утверждавшие, что было убито гораздо меньше 1,5 млн армян, назвали закон «расистским и дискриминационным» и заявили, что судить о тех убийствах должны историки. При наличии имеющихся у нас уже сегодня технологических устройств, онлайн-платформ и баз данных правительствам будет гораздо труднее оспаривать подобные факты, и не только потому, что оригинальные материалы будут храниться вечно, но и потому, что у всех желающих появится равный доступ к ним.

В будущем такие инструменты, как сверка биометрических данных, отслеживание SIM-карт и простые в использовании платформы для создания контента, обеспечат невиданный доселе уровень ответственности перед обществом. Свидетель преступления зафиксирует увиденное на своем телефоне и почти мгновенно идентифицирует преступника при помощи программного обеспечения распознавания лиц, не подвергаясь непосредственной опасности. После этого информация о преступлении или насилии со стороны полиции будет автоматически загружена в «облако» (что позволит сохранить данные в случае конфискации телефона свидетеля) и, возможно, направлена в международные контрольные или судебные органы. Рассмотрев представленные документы, международный суд начнет виртуальный процесс, за ходом которого смогут наблюдать жители страны, где живет обвиняемый. Возможно, главарей режима риск публичного позора и уголовного преследования и не испугает, но рядовые исполнители в следующий раз хорошо подумают, прежде чем применить насилие. Проверенные профессионалами свидетельства будут доступны на сайте Гаагского трибунала еще до начала судебного заседания, на котором свидетели смогут выступить заочно, не подвергаясь опасности.

Конечно, колеса судебной машины крутятся медленно, особенно в запутанном лабиринте международного права. И пусть система не сразу начнет реагировать на виртуальные свидетельства, механизм хранения проверенных данных создавать нужно уже сейчас — он сможет повысить эффективность правосудия. Помочь донести до

конечных пользователей информацию о наиболее опасных преступниках могло бы бесплатное приложение для смартфонов, созданное под эгидой Международного уголовного суда или иного авторитетного органа. Точно так же как китайский «поисковик человеческой плоти» позволяет точно вычислять местонахождение и контактные данные человека, можно было бы искать нарушителей закона, объявленных в розыск. (Не забывайте, что даже в самых отдаленных местах люди будут пользоваться мощными телефонами.) С помощью той же платформы сознательные пользователи всего мира могут собирать денежные средства для награды за поимку преступников, стимулируя быстрое их задержание. И тогда этих людей ждал бы не самосуд толпы, а суд и тюрьма.

Коллективная мощь населения виртуального мира явится серьезной сдерживающей силой для тех, кто проявляет жестокость по отношению к другим, замешан в коррупции и даже в преступлениях против человечности. Естественно, есть монстры, для которых не существует сдерживающих факторов, но для остальных потенциальные издержки антиобщественного поведения в цифровую эпоху вырастают очень заметно. Растет риск быть пойманным, а также вероятность того, что свидетельства о совершении преступления будут собраны и сохранены навечно, а свидетели используют все технические возможности, чтобы сообщить о случившемся максимально большему числу людей. Что касается потенциальных перебежчиков, то у них появится мощный стимул — возможность избежать обвинений в соучастии в задокументированных преступлениях. Будет разработана программа онлайн-защиты свидетелей, в рамках которой им будут предоставляться новые виртуальные личности (вроде тех, что продаются на черном рынке, — мы обсуждали это выше), чтобы мотивировать их на сотрудничество.

Сохраненные в цифровом виде свидетельства помогут вершить правосудие после окончания конфликта. Будущим комиссиям по установлению истины и примирению предстоит иметь дело с огромным количеством цифровых материалов, спутниковых изображений, любительских видео- и фотоматериалов, результатов вскрытия и свидетельских показаний. (Об этом речь впереди.) Страх наказания может оказаться сдерживающим фактором для

потенциальных агрессоров или по меньшей мере заставит их снизить уровень насилия.

Благодаря «облачному» хранению данных можно не только документировать насилие. Эта технология окажет людям, живущим в зоне конфликта, и другую очень важную услугу. В виртуальном пространстве информация и документы будут в большей сохранности, чем в реальном мире. Конечно, иногда вспышки насилия происходят неожиданно и застают людей врасплох. Но в ситуации с постепенной эскалацией конфликта можно предугадать, что придется бежать, и подготовиться к этому. Даже оказавшись за границей или в лагере беженцев, собственники смогут подтвердить права на свои дома, имущество и бизнес, поскольку будут располагать доказательствами, в том числе данными о границах участков, отмеченными при помощи Google Maps и GPS. Они сохранят копии свидетельств о собственности и иных документов в «облаке». Помочь в разрешении спора смогут цифровые платформы. Люди, оказавшиеся в зоне конфликта и вынужденные стать беженцами, смогут сделать фотографии всего своего имущества и воссоздать модель дома в виртуальном пространстве. А после возвращения точно сказать, что утрачено, и воспользоваться социальными сетями для поиска украденных вещей (после того как с помощью цифровой верификации подтвердят свое право на них).

Автоматическое оружие

Будущие участники конфликта, переходящего в стадию военных действий, столкнутся с тем, что поле битвы будет совершенно не похоже на то, что было в прошлом. Появление виртуального фронта не означает, что исчезает потребность в сложных видах вооружения и солдатах, действующих в реальном мире, и не умаляет роли человека. Если армия хочет вызывать симпатии своего населения, то ее командованию придется учитывать существование этих двух миров (и свою ответственность в обоих), иначе оно столкнется с тем, что, несмотря на новые технологии, которые превращают военнослужащих в совершенные машины убийства, общество относится к ним со все большей неприязнью.

Появление современного автоматического оружия благодаря достижениям в таких областях, как робототехника, искусственный интеллект и беспилотные летательные аппараты (БПЛА), представляет собой самый значительный сдвиг в технологии ведения войны с момента изобретения огнестрельного оружия. Или, как заметил военный историк Питер Сингер в своей прекрасной книге «Война с дистанционным управлением»[41], мы оказались в точке сингулярности (так в научном мире называют «состояние, в котором все меняется настолько радикально, что старые законы перестают действовать, поэтому мы не можем спрогнозировать происходящее там»). Как и в других случаях сдвига парадигмы в истории (микробная теория, изобретение книгопечатного пресса, теория относительности Эйнштейна), почти невозможно предсказать точно, как окончательный переход к полностью автоматическому оружию изменит ход человеческой истории. Все, что в наших силах, — это изучить имеющиеся сегодня подсказки, представить мышление людей на передовой и попытаться сделать какие-то выводы.

Идея интеграции информационных и военных технологий не нова: исследовательское подразделение Пентагона DARPA было создано еще в 1958 году в ответ на запуск первого в мире советского искусственного спутника Земли[45]. Настрой правительства США — ни в коем случае не дать застать себя врасплох еще раз — был столь решителен, что миссия DARPA определялась буквально так: «поддерживать технологическое превосходство вооруженных сил США и не допустить того, чтобы технологические новшества могли нанести ущерб национальной безопасности». После этого США стали мировым лидером в использовании передовых военных технологий, начиная от «умных» бомб и заканчивая беспилотными летательными аппаратами и роботами-саперами, предназначенными для обезвреживания взрывных устройств. Но Соединенные Штаты могут потерять свое преимущество. Поговорим об этом позже.

Легко понять, почему правительства и военные любят роботов и вообще автоматическое оружие: роботы не устают, не чувствуют страха, не испытывают эмоций, имеют сверхчеловеческие возможности и безукоризненно выполняют приказы. Как отмечает

Сингер, они уникально подходят для выполнения скучной, грязной и опасной работы. Тактические преимущества военных роботов ограничиваются лишь возможностями их производителей. Сегодняшние роботы не боятся пуль, имеют ультрасовременное вооружение, умеют распознавать и обезоруживать цели и несут на себе огромную нагрузку в суровых условиях жары, холода и отсутствия видимости. У военных роботов выносливость выше, а реакция быстрее, чем у любого солдата, и политики с гораздо большей готовностью пошлют в бой их, чем людей. Большинство из нас согласится с тем, что участие роботов в военных операциях на земле, на море или в воздухе в конечном счете приведет к меньшим человеческим жертвам как среди военных, так и среди мирного населения и меньшему материальному ущербу.

В ходе американских военных операций уже используется множество различных роботов. Больше десяти лет назад, в 2002 году, компания iRobot, которая изобрела робот-пылесос Roomba, представила робота-сапера PackBot — машину весом 21 килограмм, на гусеницах, как у танка, с видеокамерами и некоторой автономной функциональностью. Этого робота военные могли использовать для обнаружения мин, признаков химического или бактериологического заражения и самодельных взрывных устройств (СВУ), заложенных на обочинах дорог и в других местах[46]. Еще один производитель роботов, компания Foster-Miller, выпускает конкурента PackBot под названием TALON, а также первый вооруженный робот для использования в бою SWORDS, или «специальную боевую систему наблюдения и разведки». Еще существуют беспилотные летательные аппараты. Помимо широко известных БПЛА Predator в армии США используется как его уменьшенные (Raven, который запускается с рук и используется для воздушной разведки), так и более крупные версии (Reaper, который летает выше и быстрее, чем Predator, а также несет большую нагрузку). Из попавшего в редакцию журнала Wired и опубликованного в его блоге секретного документа Конгресса США следует, что в 2012 году на долю БПЛА приходился 31% всех военных самолетов (для сравнения: в 2005 году они составляли всего 5%).

Мы разговаривали со многими бывшими и действующими военнослужащими сил специального назначения, чтобы узнать их мнение о том, какое влияние окажет в следующие десятилетия на военные операции развитие роботостроения. По словам Гарри Уинго, сотрудника Google, в прошлом бойца отряда «морских котиков», компьютеры и «боты» полезно использовать для наблюдения, а боевые роботы хороши для того, чтобы занять опорную точку, преодолевая участок под огнем противника, или при зачистке здания. Он считает, что в следующем десятилетии на долю роботов будет приходиться больше операций с использованием огнестрельного оружия, «включая зачистку помещений, когда на прицеливание есть считаные доли секунды». Поначалу роботами будут управлять солдаты из укрытия, но в конце концов, уверен Уинго, «они смогут самостоятельно обнаруживать и уничтожать цель». В армии США вооруженные роботы SWORDS, способные в полуавтоматическом режиме распознавать противника и стрелять в него, применяются с 2007 года, хотя считается, что в реальном бою их пока не используют.

Но от солдат-людей в армии не откажутся, ведь полностью автоматизировать все их функции пока не удается. Ни один из существующих сегодня роботов не может действовать совершенно автономно, то есть обходиться без команд человека. Кроме того, в бою бывает необходимо оценивать ситуацию и принимать решение, опираясь на интуицию, чего роботы не смогут делать еще много лет (мы поговорим об этом позже). О том, какие технические устройства дополнят живых солдат и как будут выглядеть боевые подразделения, мы спросили бывшего бойца отряда «морских котиков», который, как выяснилось, принимал участие в операции по захвату убежища Усамы бен Ладена в мае 2011 года. Во-первых, он считает, что военнослужащих экипируют современными и безопасными планшетными компьютерами, которые позволяют получать информацию с камер БПЛА, загружать данные разведки и видеть передвижение других подразделений. У этих устройств будут уникальные, постоянно обновляющиеся карты, которые подробно описывают местность и содержат сведения об исторической значимости улиц и зданий, о владельцах домов, о передвижениях людей в помещениях, зафиксированных беспилотными разведчиками

при помощи инфракрасных лучей, чтобы солдаты лучше понимали, где находится их цель и чего нужно опасаться.

Во-вторых, изменятся обмундирование и снаряжение военнослужащих. Униформа будет производиться с применением тактильных технологий, что позволит получать сигналы в виде легкого сжатия или вибрации в определенном месте. (Предположим, сжатие левой икры может означать то, что подлетает вертолет.) Шлемы смогут обеспечивать лучший обзор. Встроенная в них система коммуникаций позволит командирам видеть то же, что и солдаты, и управлять их действиями с «заднего сиденья», то есть дистанционно, с базы. Система камуфляжа позволит менять цвет, текстуру, узор и даже запах униформы. А сама униформа станет «звучащей» и сможет маскировать передвижение солдата, например издавать какие-то природные звуки, скрывающие шум шагов. Использование легких и долговечных источников питания обеспечит надежность устройств: они не подведут в критический момент, не будут зависеть ни от перепадов температуры, ни от подзарядки. Кроме того, у солдат появится возможность уничтожить на расстоянии все свои технические устройства в случае их захвата врагом, чтобы не допустить утечки важной информации.

Конечно же, потребуется недоступный в гражданских технологиях высочайший уровень кибербезопасности, который позволит наладить мгновенную передачу данных и их надежную электронную защиту. Ведь если не обеспечить безопасность, никакие из перечисленных новшеств не будут стоить огромных затрат, необходимых на их разработку и внедрение.

К сожалению, создание новых видов оборудования станут тормозить подрядчики Пентагона. В США компании военно-промышленного комплекса уже работают над некоторыми из описанных инициатив. Под руководством DARPA ими созданы уже принятые на вооружение роботы. Однако по своей природе ВПК плохо приспособлен для инноваций. Часто из-за бюрократических процедур, свойственных подрядчикам и самому министерству обороны, глохнут даже инициативы DARPA, хотя финансируется агентство относительно щедро. Инновационный бум, характерный для американского сектора высоких технологий, отсекается от армии

нелогичной и устаревшей системой закупок, в результате чего страна упускает большие возможности. Без реформ, которые позволят военным агентствам и подрядчикам вести себя скорее как небольшие компании и стартапы (с их маневренностью и способностью принимать быстрые решения), неминуемое снижение военных расходов приведет не к эволюции, а скорее к укоренению существующей системы.

Военным хорошо знакома эта проблема. По словам Сингера, «как им вырваться из оков этой неработающей системы — стратегический вопрос для них». Крупные оборонные проекты застревают на стадии прототипа, на них не хватает времени и денег, в то время как коммерческие технологии и продукты придумывают, создают и выводят на рынок в рекордно короткие сроки. Работа над проектом объединенной тактической системы радиосвязи, которая должна была стать для армии новой сетью коммуникаций — аналогом интернета, началась еще в 1997 году; в сентябре 2012 года самостоятельный проект был закрыт, а функции заказчика подобных работ переданы структуре под названием «Объединенный тактический центр связи». К этому моменту затраты на него составили миллиарды долларов, тем не менее он до сих пор не готов к использованию в боевой обстановке. «Такого рода вещи недопустимы», — говорит Сингер.

Одним из выходов для военного ведомства и его подрядчиков могло бы стать использование коммерческих готовых продуктов, то есть покупка уже имеющихся на рынке технологий и устройств вместо разработки их «с нуля». Однако интеграция созданных внешними производителями продуктов — дело непростое, возможны длительные задержки хотя бы из-за необходимости выполнять специфические армейские требования (к надежности, удобству использования и безопасности). По словам Сингера, бюрократическая и неэффективная система подписания контрактов на закупки для нужд армии вынуждает находить поистине гениальные способы обойти препоны и получить результат. Иногда приходится покупать то, в чем возникает срочная нужда, за пределами стандартного процесса закупок, принятого в Пентагоне. Так, после начала эпидемии самодельных взрывных устройств в Ираке удалось быстро доставить на фронт защищенные от подрыва и атак из засад бронеавтомобили класса MRAP. Кроме того,

военнослужащие часто адаптируют для своих нужд и успешно используют коммерческие продукты.

Даже руководители военного ведомства признают преимущества, которые приносят эти изобретения. «В каком-то смысле армии помог спрос, сформированный на полях сражений в Ираке и Афганистане, — объясняет Сингер. — В Афганистане пилоты штурмовых вертолетов морской пехоты перед вылетом закрепляли iPad у себя на коленях и использовали его карты вместо встроенной системы навигации»[47]. И добавляет, что военных беспокоит возможный спад в применении инновационных обходных путей после того, как уменьшится прессинг военных действий. Остается только надеяться, что что-то изменится и инновации смогут пробиться через злосчастную систему военных закупок.

* * *

В прошлом благодаря технологическим прорывам Соединенные Штаты имели огромные стратегические преимущества. После создания первых ракет с лазерным наведением многие годы ни у одной из стран не было оружия, способного сравниться с ними по смертоносной силе и дальности действия. Однако со временем технологические преимущества в результате их копирования или утечки информации утрачиваются, сложные виды вооружения не являются исключением. Рынок беспилотных летательных аппаратов уже стал международным. Долгие годы лидировал Израиль сейчас активно продвигает и продает свои БПЛА Китай, а в 2010 году Иран раскрыл информацию о создании иранскими инженерами беспилотного бомбардировщика. Даже Венесуэла присоединилась к этому клубу, использовав свой военный альянс с Ираном для начала реализации программы по производству имеющих «исключительно оборонное назначение» беспилотных летательных аппаратов, которую возглавили иранские инженеры-ракетчики. Когда венесуэльского президента Уго Чавеса попросили подтвердить слухи об этой программе, он ответил: «Да, мы делаем это и имеем на это право. Мы свободная и независимая страна». Со временем беспилотные самолеты и вертолеты станут компактнее, дешевле и эффективнее. В

большинстве случаев, если только продукт оказывается на рынке (неважно, беспилотник это или компьютерная программа), ограничить его распространение не удается.

Мы спросили бывшего директора DARPA Регину Даган, как США относятся к высокой ответственности, которая связана с производством такого рода оружия: понятно, что просчитать все возможные последствия его создания не может никто. По ее словам, «людей всегда беспокоят побочные эффекты технологических новинок, особенно революционных. Действительно, можно привести примеры и позитивных, и негативных последствий их появления». Даган напомнила о том, какую озабоченность вызвали первые сенсационные сообщения о расшифровке генома человека: если у вас будет выявлена предрасположенность к синдрому Паркинсона, как изменится отношение к вам со стороны работодателя и страховой компании? «Но потом пришло понимание, что мы должны не стыдиться открытия, которое позволит выявлять генетическую предрасположенность к заболеванию, а создать систему правовой защищенности, которая гарантировала бы, что люди, у которых она выявлена, не будут лишены медицинской помощи», — объясняет она. Появление технологических новшеств и разработка защитных мер, которые могут потребоваться в связи с этим, должны происходить одновременно и сбалансированно.

Даган характеризует свою роль в агентстве так: «Вы не выполните свою миссию, нацеленную на достижение постоянного стратегического превосходства, если не готовы делать то, из-за чего люди могут почувствовать дискомфорт». Но в работе нужно активно использовать обратную связь: очень важно выслушивать предложения других людей и принимать от них помощь. «Агентство не может все сделать само. В обсуждении проектов должны участвовать другие заинтересованные структуры», — говорит она.

Приятно слышать, что в DARPA серьезно относятся к своей ответственности за развитие новых технологий. Однако далеко не все правительства разделяют этот разумный и осторожный подход. Широкое распространение беспилотных летательных аппаратов вызывает особую озабоченность: даже очень небольшим армиям они обеспечивают огромные преимущества. Не каждое правительство или

армия в мире владеет технической инфраструктурой и людскими ресурсами для того, чтобы иметь собственный флот беспилотников: приобрести их, открыто или тайно, могут лишь очень состоятельные покупатели. Но в конечном счете владение военными роботами, особенно БПЛА, станет стратегической прерогативой каждой страны: кто-то будет покупать их для того, чтобы получить преимущество, остальные — просто чтобы сохранить паритет.

Помимо соперничества на государственном уровне начнется борьба за обладание беспилотниками и роботами и использование их в своих интересах среди обычных людей и неправительственных структур. Сингер напоминает, что «и бизнес, скажем, медиагруппы или сельхозпроизводители, опыляющие посевы с воздуха, и правоохранительные органы, и даже преступники и террористы — все уже используют беспилотные летательные аппараты». В 2007 году довольно специфическая частная военная компания Blackwater, позже переименованная в Academi, LLC, вывела на рынок необычную услугу — аренду БПЛА для слежки и разведки. В 2009 году она подписала контракт с ЦРУ об оснащении бомбами принадлежащих управлению беспилотников.

Известно много случаев, когда частные компании по собственной инициативе создавали и использовали беспилотные летательные аппараты. Компании, обладающие недвижимостью, применяют беспилотники для аэрофотосъемки своих владений. Некоторые университеты приобрели их в исследовательских целях (так, в Университете Канзаса можно получить диплом в области беспилотной авиации). А в 2012 году нам попалась информация об услуге «Такокоптер» (если вы нестерпимо захотели пирожок тако[48], можете выбрать его с помощью смартфона, указать свои координаты и ждать беспилотника с заказом). Правда, потом оказалось, что это мистификация — но вполне реализуемая с технической точки зрения — и, вероятно, скоро это будет сделано.

Мы уже говорили о том, что легкие и недорогие «повседневные» БПЛА, разработанные для военных целей, станут особенно популярным товаром на международном рынке вооружений и на подпольных рынках оружия. Дистанционно управляемые самолеты,

автомобили и катера, способные вести наблюдение, перехватывать цели противника и нести и приводить в действие бомбы, добавят новый класс задач армии в зонах боевых действий. И если «гражданские» версии вооруженных беспилотников станут достаточно совершенными, мы вполне можем оказаться свидетелями их воздушного боя. Возможно, впервые это случится в Мексике, где у наркокартелей есть и желание, и ресурсы для приобретения такого оружия.

Правительства постараются ограничить доступ к ключевым технологиям, облегчающим производство беспилотников для широкой потребительской аудитории, но регулировать их распространение будет очень сложно. Прямой запрет нереален, и даже скромные попытки контролировать гражданское их использование во вполне мирных странах не увенчаются успехом. Если правительство США потребует от населения регистрировать свои беспилотные летательные аппараты и запретит их полеты в определенных местах (скажем, вблизи аэропортов и государственных объектов) и пересечение ими границ штатов, совсем нетрудно представить упрямцев, которые сумеют найти способ обойти запреты, внося изменения в конструкцию своих беспилотников, делая их анонимными или снабжая их каким-то подобием технологии «стелс». И все же могут быть подписаны международные договоры о запрещении экспорта крупных БПЛА в обход государственных каналов. Страны, имеющие самые большие возможности для поставок БПЛА, могут прийти к заключению некоего аналога Договора об ограничении стратегических вооружений (ОСВ), целью которого было сократить количество единиц ядерного оружия у США и СССР во времена холодной войны.

Государствам придется много работать над задачей защиты своих морских и сухопутных границ от растущей угрозы со стороны вражеских беспилотных летательных аппаратов, поскольку их трудно обнаружить. Так как автономные системы навигации становятся все доступнее, беспилотники превращаются в миниатюрные крылатые ракеты, которые невозможно перехватить после запуска. Разведывательные беспилотники не так страшны, как ракетоносные, но будут расцениваться как угроза, поскольку обнаружить их нелегко. Возможно, самым эффективным способом уничтожить вражеский

БПЛА окажется электронный — взлом его киберзащиты, а не применение грубой силы. После этого начнется, по словам Сингера, «битва за контроль» — борьба за то, чтобы заставить машину сотрудничать и «убедить» ее сделать не то, что предполагает ее миссия.

> В конце 2011 года власти Ирана с гордостью продемонстрировали совершенно неповрежденный американский беспилотник RQ-170 Sentinel. Как утверждалось, его обнаружили в иранском воздушном пространстве и посадили на землю благодаря тому, что удалось взломать его систему защиты (представители США, в свою очередь, сообщили лишь о том, что БПЛА был «потерян»). Неназванный иранский инженер рассказал газете The Christian Science Monitor, что они с коллегами заставили беспилотник «приземлиться там, где захотели, не взламывая сигнал системы дистанционного управления и каналы связи» с командным центром американцев, поскольку знали об уязвимости в системе GPS-навигации самолета. Версия с передачей ложных координат (эта техника известна как «спуфинг») возможна, но маловероятна, поскольку эта задача невероятно трудна в реализации (чтобы добраться до GPS, иранцам нужно было преодолеть армейское шифрование, заглушив сигналы связи и подменив их своими).

Вполне возможно, что государства придут к подписанию международных договоров с обязательством не посылать беспилотные летательные аппараты в воздушное пространство друг друга или достижению договоренности считать разведывательные беспилотники допустимым нарушением. Или появятся международные требования о том, чтобы разведывательные БПЛА легко отличались от тех, которые несут вооружение. Трудно сказать определенно. Некоторые страны создадут объединенный «щит от беспилотников», напоминающий ядерные альянсы времен холодной войны, и мы увидим первые в мире зоны с запретом полетов беспилотных летательных аппаратов. Если небольшие и не очень богатые страны не смогут позволить себе создание или покупку собственных беспилотных бомбардировщиков, но опасаются нападения с воздуха своего агрессивного соседа, они будут вступать в альянсы с одной из сверхдержав, чтобы гарантировать себе некоторую защиту. Но маловероятно, чтобы страны, не имеющие беспилотников, не попытались изменить

ситуацию: захваченный иранцами БПЛА-шпион Sentinel стоил всего $6 млн.

Распространение роботов и беспилотных летательных аппаратов увеличит количество конфликтов в мире — получив в свое распоряжение такие инструменты, государства будут стремиться их испытать, — но снизит вероятность полномасштабной войны. На то есть несколько причин. Одна из них заключается в том, что это достаточно новое явление: все международные соглашения, касающиеся различных видов вооружения (Договор о нераспространении ядерного оружия, Договор по ПРО, Конвенция о запрещении химического оружия и так далее), были подписаны задолго до появления БПЛА. Необходимо обозначить границы, установить правовые нормы, а политики должны научиться использовать эти инструменты ответственно и с учетом общей стратегии. Существуют и этические аспекты, которые следует обсудить публично (сейчас такая дискуссия идет в США). Все эти соображения заставят власти разных стран проявлять осторожность в период активного распространения беспилотников.

Мы должны не забывать и о такой проблеме, как возможность потери контроля над беспилотными летательными аппаратами, как это было с ядерным оружием. Существуют обоснованные опасения, способны ли такие страны, как Пакистан (по некоторым оценкам, он владеет примерно сотней ядерных зарядов), обеспечивать безопасность своего ядерного арсенала и не допустить их кражи. По мере появления больших флотилий БПЛА повышается риск того, что какой-то из них попадет «не в те руки» и будет использован против иностранного посольства, военной базы или культурного центра. Представьте себе следующий теракт, сравнимый по масштабам с 11 сентября 2001 года, но проведенный не путем угона коммерческих авиалайнеров, а с помощью беспилотников, похищенных у государства. Такая опасность подтолкнет к заключению договоров, в которых будут выработаны требования по должной охране БПЛА.

Государствам придется совместно или по отдельности выработать правила использования БПЛА и решить, попадут ли они под те же нормы регулирования суверенности воздушного пространства, что и обычные самолеты. Взаимные опасения будут удерживать власти от

эскалации конфликта с участием беспилотников. Даже когда выяснилось, что американский БПЛА Sentinel нарушил воздушное пространство Ирана, реакция Тегерана свелась к хвастовству и демонстрации захваченного трофея,
а не к мести.

Снижение смертности среди военнослужащих благодаря использованию беспилотных летательных аппаратов будет благосклонно воспринято обществом и снизит вероятность полномасштабного военного конфликта. У нас уже есть статистика, которую можно изучать: новости о беспилотниках в США появляются на протяжении нескольких лет. За несколько месяцев до президентских выборов 2012 года в результате утечек информации из правительства появились подробные статьи о секретных операциях с использованием БПЛА, санкционированных Бараком Обамой. Судя по реакции американцев на удары беспилотных бомбардировщиков как в «официальных» зонах боевых действий, так и в «неофициальных» — в Сомали, Йемене и Пакистане, — операции по ликвидации террористов с участием беспилотников кажутся обществу гораздо более приемлемыми, чем использование солдат. Такие акции вызывают меньше вопросов и протестов. Некоторые сторонники сокращения присутствия США в мире даже поддерживают расширение программы применения БПЛА в качестве законного способа выполнения этой задачи.

Мы лишь недавно научились воевать так, чтобы не соприкасаться с противником физически и эмоционально, до определенной степени лишив войну личностной составляющей, и пока не знаем всех политических, культурных и психологических последствий этого. Сейчас «дистанционные» военные действия ведутся чаще, чем когда бы то ни было, а в будущих конфликтах их роль станет еще более заметной. Исторически к ним относилось использование ракет, но в будущем станет возможным еще более значительное дистанцирование действующих лиц от поля битвы. В конце концов, жертвы *другой* стороны редко становятся важным фактором международной политики и объектом общественного внимания: если американские войска не подвергаются опасности, интерес публики тут же резко падает. Это, в свою очередь, означает меньшую озабоченность населения вопросами

национальной безопасности: когда на горизонте не предвидится опасности для наших солдат, тише голоса и «ястребов», и «голубей». Чем больше у властей вариантов действий, не привлекающих общественного внимания, тем больше задач по обеспечению безопасности они могут выполнить без объявления войны или отправки войск, что снижает вероятность возникновения крупномасштабного вооруженного конфликта.

* * *

Можно только приветствовать прогнозируемое снижение жертв среди мирного населения и материального ущерба, а также риска ранений и гибели военнослужащих, однако переход к полностью автоматизированному ведению боевых действий принесет новые проблемы. Главная из них — обеспечение кибербезопасности оборудования и информационных систем. Обмен данными между всеми устройствами, наземными роботами, беспилотными летательными аппаратами и их командным пунктом управления, где находятся люди, должен быть быстрым и безопасным. Необходимо обеспечить качественную инфраструктуру или хорошую связь между боевыми частями и их базами. Вот почему армия обычно создает собственные коммуникационные сети, а не полагается на имеющиеся. Пока роботы, действующие на поле боя, не обзаведутся автономным искусственным интеллектом, помехи или разрыв связи могут превратить эти машины в бесполезную груду железа, к тому же еще и опасную, ведь захват вражеского робота поможет получить доступ к секретной технологии. И не только к технологии: это позволит изучить его программное обеспечение, использованные инженерные решения, а также секретные данные вроде координат расположения вражеских боевых частей. (Трудно представить себе, что государства откажутся от соблазна провести кампанию дезинформации и сознательно посадить на чужой территории — или позволить противнику захватить — беспилотник-приманку с записанной в нем ложной информацией и собранный с использованием вводящих в заблуждение компонентов.) В войнах с участием роботов обе противоборствующие стороны для пресечения вражеской активности будут использовать кибератаки,

применяя или спуфинг (то есть выдавая себя за авторизованного участника сети), или ложные цели, чтобы запутать датчики и ослабить боевые порядки противника. Конечно, производители попытаются встроить в свои устройства отказоустойчивые механизмы для снижения вреда от таких атак, но сделать роботов «пуленепробиваемыми» для любых технологических хитростей будет очень трудно.

Военнослужащие и создатели роботов столкнутся с ошибками, допущенными при разработке. Уязвимости и ошибки встречаются в любой сети, и часто единственный способ их исправить — это дождаться, когда о них узнают хакеры или независимые специалисты по компьютерной безопасности. Разобраться в программах, которые необходимы для работы столь сложных устройств, крайне нелегко: там миллионы и миллионы строк кода, и вероятность ошибок очень высока. Даже когда разработчики знают об уязвимых местах, их не так просто устранить. Считается, что о бреши в защите системы GPS, которой воспользовались иранцы, напав на американский беспилотник и посадив его, Пентагону было известно с боснийской кампании 1990-х годов. В 2008 году в распоряжении спецслужб США впервые оказался изъятый у шиитских повстанцев в Ираке ноутбук с записями видеокадров, снятых американскими беспилотными летательными аппаратами, которые иракцам удалось перехватить, просто направив на него спутниковую тарелку и использовав дешевую программу SkyGrabber, которую можно купить в сети за $26. Предназначается она для пиратского скачивания фильмов и музыки. Линии обмена данными между беспилотником и его пунктом управления тогда не шифровались.

В ближайшем будущем управлять этими устройствами будут люди и ошибок избежать не удастся. Если человек с его хрупкой психикой оказывается в условиях боевых действий, в ситуации непредсказуемости, это может привести к посттравматическому стрессу, тяжелым эмоциональным расстройствам и психическим срывам. Пока люди будут участвовать в войнах, будут и ошибки.

Устройства, способные воевать без участия человека, не смогут заменить людей ни непосредственно в бою, ни в центре принятия решений до тех пор, пока искусственный интеллект не заменит

человеческий мозг полностью. Ошибки совершают даже самые умные машины. Как отмечает Питер Сингер, когда во время Первой мировой войны на полях сражений появился танк, он казался непобедимым, пока кто-то не придумал противотанковый ров. Бывший министр обороны Афганистана Абдул Рахим Вардак, с которым мы познакомились в Кабуле незадолго до его отставки, с улыбкой рассказывал нам, как в 1980-е годы он вместе с другими моджахедами боролся с советскими танками, замазывая грязью их смотровые щели и сооружая покрытые ветками и листвой ямы-ловушки вроде тех, которые за десять лет до этого вьетконговцы использовали против американских солдат. Сингер проводит более современные параллели: «Наземные роботы, которых наши солдаты используют в Ираке и Афганистане, поразительно высокотехнологичны, однако повстанцы поняли, что они могут бороться с ними с помощью простых ловушек, всего лишь выкапывая глубокие ямы, в которые те падают. Они даже подобрали определенный угол наклона стен, чтобы роботы не выбирались обратно». Интеллект этих роботов ограничен, и, пока они проходят полевые испытания, их операторы и разработчики будут постоянно сталкиваться с вражескими контрмерами, которые *не смогли* предугадать. Им придется постоянно совершенствовать свои продукты. Подобные асимметричные ответы противника окажутся непреодолимой трудностью даже для самых совершенных технологий.

Однако человеку мало одних лишь навыков решения задач. Есть уникальные человеческие черты, важные в военных условиях, которые даже определить трудно, не то что наделить ими роботов: это свое мнение, эмпатия и доверие. Что-то наверняка будет утрачено, если роботы возьмут на себя функции солдат. В ходе наших бесед с военнослужащими сил специального назначения все они, ссылаясь на свой боевой опыт, подчеркивали чрезвычайную важность доверия к однополчанам и чувства братства. Некоторые из них учились вместе и многие годы воевали бок о бок, изучив привычки и почти без слов понимая действия и ход мыслей друг друга. По их словам, они могут общаться при помощи взгляда. Смогут ли роботы когда-нибудь перенять человеческие способности считывать невербальные подсказки?

Способен ли робот на смелый поступок? Может ли пожертвовать собой? Может ли робот, обученный обнаруживать и уничтожать цель, иметь какие-то понятия об этике или сдержанности? Сможет ли он когда-нибудь отличать ребенка от невысокого взрослого? Если робот застрелит мирного жителя, кого в этом винить? Представьте, что лицом к лицу столкнулись вооруженный наземный робот и шестилетний мальчик с аэрозольным баллончиком краски, которого послали повстанцы. Как бы ни действовал робот, автономно или под управлением человека, у него есть две возможности: выстрелить в невооруженного ребенка или оказаться выведенным из строя, поскольку мальчишка просто ослепит его, распылив краску на высокотехнологичные камеры и датчики. Как бы поступили вы, управляя роботом, задает вопрос Сингер. Мы не можем отдавать роботов под трибунал или как-то еще наказывать их. Еще многие годы доминирующую роль в военных операциях будут играть люди, несмотря на то что роботы становятся все более разумными и все лучше интегрируются в «человеческие» боевые подразделения.

Новые способы вмешательства

Переход конфликтов на новую стадию, для которой характерно применение виртуального и автоматического оружия, означает, что в будущем в распоряжении государств-агрессоров окажется более широкий диапазон средств ведения войн. Расширятся возможности для вмешательства в конфликт со стороны граждан, бизнес-сообщества и иностранных государств.

На международном уровне единственным органом, который, с одной стороны, представляет все страны мира, а с другой — способен придать легитимность иностранному военному вмешательству, является Совет безопасности ООН. Маловероятно, что страны мира в достаточной мере серьезно пересмотрят полномочия, которыми была наделена организация при ее создании в 1945 году, несмотря на призывы к действию и все возрастающее давление на власть со стороны гражданского общества. Почти невозможно будет получать новые мандаты и право на интервенцию, учитывая то, что для изменения Устава ООН требуются голоса 194 стран-участниц.

В некоторых областях международных отношений появятся и окажутся жизнеспособными новые формы иностранного вмешательства, организованного в рамках альянсов с ограниченным числом участников. Вполне возможно, что в какой-то чрезвычайной ситуации несколько стран решат совместными усилиями вывести из строя военных роботов «заблудшего» государства. Можно также представить себе, что в рамках НАТО кто-то из его стран-участниц добьется введения нового типа мандатов на вмешательство в конфликт, которые будут давать право на ввод войск с целью установления буферных зон безопасности с независимыми и защищенными сетями связи. Это могло бы стать популярным методом: фактически речь идет о естественном расширении доктрины «Обязанность защищать», которая легла в основу принятого в 2011 году решения Совета безопасности ООН о разрешении военной интервенции в Ливию (включая авиаудары по стране), начатой впоследствии НАТО. Вполне возможно, что мы станем свидетелями того, как члены НАТО мобилизуют беспилотники для организации над районом, контролируемым повстанцами, — первой в истории зоны, свободной от полетов, которая функционирует без участия человека и поэтому не предполагает риска для жизней солдат.

Желание действовать заставит находить и другие выходы, не ограничивающиеся формальными институтами вроде НАТО, например в виде разовых коалиций между населением и компаниями. Ни те ни другие не могут сформировать армию для военной интервенции, но зато способны внести свой вклад в организацию жизненно необходимых сетей связи в зоне конфликта. И тогда вмешательство в этот конфликт будет заключаться в захвате контроля над интернетом или в помощи повстанцам, создающим собственную независимую и безопасную сеть. Если же правящий режим начнет манипуляции со связью, то страны — участники международной коалиции, не дожидаясь одобрения ООН, восстановят нормальный доступ населения к сети.

Но важен не доступ к мобильной связи и интернету как таковой (у населения, оказавшегося в зоне конфликта, он, вероятнее всего, есть), а то, что людям позволяет делать безопасная и быстрая сеть. Врачи во временных госпиталях смогут координировать распределение

лекарств, организовывать их доставку на местном и международном уровне и документировать увиденное. Повстанцы получат надежную систему коммуникаций, не зависящую от контролируемой правительством инфраструктуры и более удобную, чем обычная радиосвязь. А мирные жители смогут общаться со своими родственниками за границей, используя платформы, которые иначе были бы им недоступны из-за блокировки властями, получать от них деньги и передавать им информацию посредством безопасных каналов, прокси-серверов и специальных инструментов для обхода механизмов защиты.

Заинтересованные государства могли бы направить в неспокойную страну что-то вроде коалиционных сил специального назначения, чтобы помочь повстанцам обрести независимость от контролируемого властями интернета и создать собственную телекоммуникационную сеть. Сегодня это уже делается, но без поддержки какого-либо правительства, силами добровольцев. Ливийские министры рассказали нам о храбром американце по имени Фред, который приплыл в Бенгази — оплот оппозиции — на деревянной лодке, вооруженный лишь коммуникационным оборудованием и желанием обеспечить оппозиционеров независимой системой доступа в интернет. Первым делом он уничтожил «жучки» времен Каддафи. В будущем же такие операции станут уделом военных, особенно в местах, недоступных с моря.

Изменится и состав коалиции, организующей интервенцию. Новыми заметными игроками станут страны с небольшим населением, но мощным технологическим сектором. Сегодня одним из самых активных участников международных миротворческих миссий является Бангладеш. В будущем важную роль в «цифровых» миссиях станут играть такие технологически развитые государства, как Эстония, Швеция, Финляндия, Норвегия и Чили. «Интернет-коалиция» окажет повстанцам не только политическую поддержку, но и обеспечит их цифровым оружием в виде широкополосного доступа в интернет, временной независимой сети сотовой связи и средств кибербезопасности. Эти страны смогут внести свой вклад и в военную часть миссии, направив в зону конфликта своих наземных роботов и беспилотные летательные аппараты. Некоторые государства, особенно

небольшие, будут исходить из того, что легче, дешевле и политически целесообразнее создавать арсенал автоматических «солдат» для использования его в международных акциях, чем поддерживать и направлять в зону боевых действий обычные войска.

В этих коалициях примут участие технологические компании, неправительственные организации и частные лица, причем все они внесут по-своему ценный вклад в общее дело. Компании будут разрабатывать бесплатные программы, отвечающие нуждам населения страны, где происходит конфликт, или предложат ее жителям бесплатные обновления своих продуктов. Неправительственные организации в сотрудничестве с операторами связи и интернет-провайдерами будут создавать базы данных с информацией о жителях и их потребностях, особенно отмечая тех, кто проживает в нестабильных или изолированных районах страны. А частные лица, записавшись добровольцами, станут тестировать эти новые сети и продукты, помогая находить ошибки и уязвимые места и обеспечивая разработчиков критически важной обратной связью.

* * *

Вне зависимости от уровня развития технологий конфликты и войны в реальном мире будут существовать всегда, и решение о применении в них машин и кибероружия представляется нам очень гуманным. Технический прогресс уравнивает возможности всех пользователей, в том числе и участников конфликта, позволяя им достичь большего, то есть донести свою точку зрения до более широкой аудитории, увеличить объем контента, активнее использовать роботов и прочие виды кибероружия, поражать большее количество стратегических целей. Хорошо, что у людей повышается ответственность за свои действия, ведь полностью удалить цифровые свидетельства преступления теперь невозможно. Однако развитие технологий делает конфликт более сложным явлением, хотя и снижает связанный с ним риск.

Будущие участники конфликтов — страны, повстанцы, армия — поймут, что в случае виртуального противостояния следует проводить такой же всесторонний этический, тактический и стратегический

анализ, как и в случае реального конфликта, и это будет оказывать влияние на принимаемые ими решения. С одной стороны, агрессоры станут активнее действовать на менее рискованном виртуальном фронте: заниматься онлайн-дискриминацией и наносить упреждающие кибердудары по врагу. С другой стороны, наличие этого виртуального фронта свяжет им руки, заставляя их сдерживаться на фронте реальном. И, как мы увидим далее, сама возможность открыть виртуальный фронт создает предпосылки для вмешательства, вполне действенного и при этом сводящего к минимуму потребность рисковать войсками или вовсе отменяющего потребность в них. В случае иностранного военного вмешательства в ход конфликта можно использовать патрулирование свободной от полетов зоны с помощью беспилотных летательных аппаратов или применять роботов-миротворцев, но все же набор таких мер довольно ограничен. Зато после окончания конфликта и начала восстановления страны открываются бесконечные возможности для использования высоких технологий.

Примечания к главе 6

ГЛАВА 7

Будущее возрождения страны

Очевидно, что технологии помогают наэлектризовать общество и даже расколоть его, но могут ли они вновь объединить его? Возрождение нормальной жизни после конфликта или стихийного бедствия — процесс долгий и трудный. Здесь не помогут флешмоб или вирусный ролик. Но если коммуникационные технологии сами по себе и не восстановят разрушенную страну, они могут оказать большую помощь в улучшении политической, экономической и социальной ситуации. Те инструменты, которые мы сегодня используем исключительно для развлечения, в посткризисных обществах будут применяться по-новому, а люди получат доступ к информации и другим ресурсам.

Высокие технологии не способны предотвратить стихийное бедствие и остановить гражданскую войну, но могут сделать менее болезненным процесс соединения осколков общества. Со временем прежние модели и методы восстановления страны видоизменятся или отомрут. В будущем усилия по возрождению страны, как и предшествующий им конфликт, получат виртуальную составляющую. Ремонтировать дороги, восстанавливать мосты, возводить дома будут все так же с помощью строительной техники, но параллельно с этим станут восстанавливать связь — то, что раньше казалось второстепенным делом. Восстановленная система коммуникаций поможет отстраивать физическую инфраструктуру страны, реконструировать ее экономику и государственное управление. Поэтому поговорим о возможных в будущем подходах к планированию развития посткризисного общества, о новых участниках этого процесса, появившихся благодаря интернету, а также об инновационной политике.

Вначале — коммуникации

Восстановление разрушенной в результате рукотворного или природного катаклизма страны — задача пугающе трудная. Все ее составляющие — от строительства дорог и зданий до обеспечения населения необходимыми товарами и услугами — требуют огромных ресурсов, многостороннего опыта и, конечно же, терпения. Правильное применение современных технологий может значительно облегчить этот процесс, и мы убеждены, что в грядущем успешное возрождение страны будет в значительной степени зависеть от коммуникационных технологий и быстрых каналов связи.

Появится новый прототип реконструкции: гибкий модульный набор адаптируемых средств и моделей, который можно подстроить под нужды каждого конкретного посткризисного общества. Лежащая в основе этого прототипа философия предполагает наличие обратной связи даже на самом начальном этапе работы, когда продукт еще несовершенен, — это дает наилучший результат. Именно так, методом проб и ошибок, действуют технологические компании. (Вот откуда возник любимый афоризм предпринимателей из отрасли высоких технологий: «если провал, то быстрый».) Для формирования этого нового подхода к реконструкции страны потребуется время, но в конечном счете он окажется гораздо эффективнее прежнего.

Основной компонент прототипа реконструкции (и это отличает его от традиционного подхода) — принцип «сначала коммуникации», или «сначала мобильные». Восстановление и совершенствование связи уже сейчас цементирует процессы возрождения разрушенных обществ. А в будущем современная и быстрая коммуникационная инфраструктура станет высшим приоритетом всех участников реконструкции, и не в последнюю очередь потому, что от нее будет зависеть успех всей их работы. Сдвиг в этом направлении мы наблюдаем последние десять лет.

Еще совсем недавно, в начале 2000-х годов, при возрождении страны после окончания внутреннего конфликта речь шла не столько о восстановлении коммуникаций, сколько об их создании. До смены режима ни в Афганистане, ни в Ираке не было ничего похожего на сотовую связь. Правительство талибов жестко пресекало любые попытки внедрить потребительские технологии (хотя небольшая GSM-сеть для чиновников в стране все же имелась); Саддам Хусейн

полностью запретил мобильные телефоны в своем тоталитарном государстве. Когда эти режимы пали, страна осталась практически без инфраструктуры, а население — без современных технических устройств. Стороны противостояния пользовались самыми простыми средствами связи (обычно радиостанциями).

> Когда в Ирак в 2003 году прибыли американские команды восстановления страны, то попали в «телекоммуникационную пустыню». Проблему представляло даже использование спутниковой связи, ведь телефоны работали, только если оба собеседника находились вне зданий. Нет нужды говорить, что это не очень удобно в зоне боевых действий[49]. Чтобы быстро поправить положение, Агентство по снабжению сил коалиции (CPA) заключило с региональным оператором MTC-Vodafone контракт на установку вышек и оказание услуг сотовой связи на юге страны, а другой оператор, MCI, получил одобрение на работу в Багдаде. По словам одного из бывших служащих CPA, с которым мы говорили, вышки появились по всей стране буквально за день, а сотрудники администрации и миссии ООН получили тысячи мобильных телефонов, которые нужно было распространить среди значимых местных политических игроков. (Не правда ли, странно, что все номера начинались с «917»? То есть у них был такой же региональный код, как у пяти районов Нью-Йорка.) Эти меры позволили создать необходимую инфраструктуру и вдохнули жизнь в умиравшую отрасль связи Ирака. С тех пор уже несколько лет она находится на подъеме.

В Афганистане, где ООН организовала сеть сотовой связи сразу после падения режима талибов (для населения услуги были бесплатными, чтобы стимулировать спрос), за последнее десятилетие мобильный рынок значительно вырос. Во многом это произошло благодаря решению властей выдавать лицензии частным игрокам. К 2011 году в Афганистане было четыре крупных оператора с общей абонентской базой около 15 млн человек. Команды по восстановлению страны, прибывшие в Ирак и Афганистан, начинали с чистого листа: отсутствие инфраструктуры, абонентов и неясные коммерческие перспективы. Учитывая скорость распространения сотовой связи в мире, маловероятно, что кто-то еще когда-либо столкнется с такой уникальной ситуацией.

В Гаити после землетрясения 2010 года основной задачей в области коммуникаций было не создание, а масштабное восстановление поврежденной инфраструктуры. Несмотря на разрушения, которые коснулись всей страны, связь заработала довольно быстро. В

результате мощного землетрясения и серии последовавших за ним более слабых подземных толчков мобильная инфраструктура пострадала значительно, но благодаря быстрой реакции и сотрудничеству местных телекоммуникационных компаний и армии США ее удалось восстановить уже через несколько дней. По сообщениям двух крупнейших сотовых операторов страны, Digicel и Voila, через десять дней после удара стихии они вышли на 70–80% своей прежней нагрузки.

Джаред в то время работал в Государственном департаменте. Он вспоминает, как вскоре после гаитянского землетрясения связался с послом США в Индонезии, чтобы поговорить об уроках, которые следовало извлечь. Цунами унесло 230 тысяч жизней в 14 странах Юго-Восточной Азии. Основная мысль была понятна: восстановите вышки сотовой связи, включите связь и не слушайте тех, кто считает, будто связью нужно заниматься после спасения людей. Не после, а одновременно с этим.

На Гаити и до землетрясения подавляющее большинство вышек работали от генераторов электроэнергии. Поэтому, для того чтобы обеспечить покрытие, нужно было скорее решить вопрос поставок топлива, чем ремонта инфраструктуры. А еще организовать охрану вышек, потому что находившиеся в отчаянном положении люди пытались красть горючее. В результате связь, работавшая несмотря на повсеместные разрушения и хаос, оказалась жизненно важным инструментом координации действий спасателей и отправки помощи в те районы, жители которых в ней особенно остро нуждались. Кроме того, необходимо было дать людям возможность связываться с родственниками и друзьями, живущими как в стране, так и за рубежом. Первые фотографии, которые мир увидел после стихийного бедствия, были сделаны и отправлены гаитянцами с помощью мобильных телефонов. Все, кто участвовал в ликвидации последствий катастрофы, признают ключевую роль, которую сыграла работающая связь в условиях масштабных разрушений и огромных человеческих потерь.

Восстания в арабском мире, начавшиеся в 2010 году, — еще один пример преимуществ, которые обеспечивает подход «сначала коммуникации». Оперативное восстановление связи компанией

Vodafone в Египте незадолго до отставки Хосни Мубарака стало предвестником появления более гибкого и сильного сектора телекоммуникаций. По словам CEO Vodafone Витторио Колао, «наши люди ночевали в технических центрах: мы хотели первыми восстановить оказание услуг после снятия запрета на работу. Мы подвозили туда продукты и воду, сняли номера в соседних отелях и усилили охрану, чтобы никто не смог прорваться к нам и отключить сеть». В результате этих усилий компания Vodafon действительно стала первым оператором сотовой связи, заработавшим после отключения. А слово «первый» очень важно для тех, кто стремится захватить крупный египетский рынок, где у абонентов внезапно появилось множество тем для разговоров. Колао рассказал о дальновидной стратегии, которую они использовали, чтобы вызвать симпатии египтян: «Мы позволяли абонентам звонить в кредит». А еще в Vodafon сняли ограничения на трафик для абонентов из Египта, «чтобы, когда сеть заработала, каждый мог позвонить в пределах лимита в 20 евро и сообщить родственникам, что все в порядке».

Зависимость от телекоммуникаций отражает сегодня степень их важности даже для самых бедных стран. Однако, говоря о восстановлении сети, мы пока имеем в виду лишь голосовую связь и текстовые сообщения, а не интернет. В ближайшие 10 лет ситуация изменится, поскольку во всем мире люди все больше полагаются на передачу данных. И после кризиса требования восстановить соединение с интернетом многократно перекроют нынешние призывы наладить голосовую связь и передачу SMS. Это будет соответствовать интересам и населения, и спасателей, и тех, кто занимается возрождением страны, ведь быстрый интернет позволяет решать задачи с большим успехом. Если понадобится, благотворительные организации смогут развернуть сеть мобильных вышек 4G-связи и организовать на их основе доступ в сеть, пусть и медленный. С мобильного телефона данные будут передаваться на ближайшую вышку, затем на следующую, и так до тех пор, пока, наконец, не попадут в оптоволоконный канал, соединенный с быстрым интернетом. Скорость работы в сети будет низкой, но все же достаточной для того, чтобы такие мобильные решения помогли в восстановлении страны.

* * *

Отличительной чертой прототипа реконструкции станет то, что лидерами этого процесса будут телекоммуникационные компании, независимо от того, государственные они или частные. Сегодня правительственные контракты на восстановление инженерной инфраструктуры часто заключаются с такими крупными подрядчиками, как Bechtel, и другими инжиниринговыми корпорациями. Когда в мире осознают обоснованность подхода «сначала коммуникации», первыми в страну начнут приходить операторы. В посткризисных обществах наладить надежную связь нужно как можно быстрее, ведь она позволяет координировать работу по спасению людей и восстановлению разрушенного; выстраивать диалог с населением; поддерживать власть закона; организовывать распределение помощи; искать пропавших людей; помогать беженцам осваиваться в новых условиях. У сотовых операторов появится четкая коммерческая мотивация инвестировать ресурсы в создание современной сети связи и ее обслуживание. Если регулирование сектора телекоммуникаций будет правильно выстроено с самого начала, выиграют все: компании будут зарабатывать, участники процесса восстановления страны получат в свое распоряжение более оперативные и качественные инструменты, а население в целом — доступ к надежной, быстрой и дешевой связи (особенно при наличии на рынке конкурентов в виде иностранных компаний).

Долгосрочная выгода от наличия здорового сектора телекоммуникаций заключается в том, что он способствует росту экономики, даже если на достижение стабильности уходит много времени. В целом прямые инвестиции в создание инфраструктуры, рабочих мест и системы услуг влияют на экономику более благотворно, чем краткосрочные программы помощи, а операторы связи относятся к самым прибыльным и устойчивым представителям делового мира. Так, афганская компания Roshan — не только крупнейший мобильный оператор в стране, но и лидер по объему инвестиций и уплаченных налогов. Она дает работу тысячам афганцев и обеспечивает 5% доходов бюджета. И все это несмотря на неразвитую инфраструктуру, бедное население и десять лет войны! В

будущем наиболее разумные участники программы восстановления страны — правительства, транснациональные корпорации и благотворительные организации — признают важнейшую роль компаний сектора телекоммуникаций и не станут относиться к ним как к конкурентам, считая создание сетей связи первоочередной задачей, решение которой нельзя откладывать.

Поскольку телекоммуникации — бизнес прибыльный (особенно после кризиса, когда уровень активности абонентов необычно высок), местные и международные игроки стремятся воспользоваться благоприятной возможностью принять в нем участие. Талантливые местные программисты с помощью программных средств с открытым кодом начнут строить собственные платформы и приложения, помогая поднимать экономику страны, или сотрудничать с иностранными компаниями и организациями, повышая свою квалификацию. Большая часть инвестиций в отрасли связи будет направлена на улучшение качества полезных для населения услуг, однако есть некоторый риск, что появляющаяся бизнес-элита превратится в новую «цифровую олигархию». Это могут быть местные предприниматели с хорошими связями, решившие воспользоваться ситуацией и захватить контроль над ключевой отраслью, или руководители международных компаний, стремящиеся расширить свои империи. Здесь основная ответственность ляжет на тех, кто управляет процессом восстановления: учитывая его хаотичность и динамизм, нужно очень осторожно подходить к выбору решений и эффективно использовать свои полномочия.

Помимо предпринимателей и «цифровых олигархов» есть еще одна группа инвесторов. Это представители национальной диаспоры, стремящиеся участвовать в восстановлении страны. Их интерес не столько финансовый, сколько личный. В будущем инвесторы, которые собираются выйти на новые рынки, поймут, что благодаря глобальному распространению интернета связь с интересующими их странами может быть гораздо более тесной и многообразной. Такие инструменты, как Google Alerts, социальные сети и мгновенный перевод с иностранного языка, позволяют инвесторам чувствовать себя намного ближе к жизни стран, в которых они работают, а также лучше представлять ситуацию в диаспоре. В результате вложения будут более

успешными, а отношения между инвесторами и обществом — более плодотворными.

Мало кто понимает это так же хорошо, как Карлос Слим Хелу — мексиканский телекоммуникационный магнат и богатейший человек в мире. Слим принадлежит к 15-миллионной ливанской диаспоре: его отец эмигрировал в Мексику в 1902 году, спасаясь от призыва в армию Оттоманской империи. Сегодня Слим владеет множеством компаний и ведет бизнес во всем мире (в том числе контролирует 8% акций газеты New York Times). Он рассказывал нам о том, как эмигрантское детство повлияло на его взгляды: «Думаю, что тогда я был не столько ливанцем, сколько гражданином мира. А сегодня ощущаю себя одновременно выходцем из Ливана, которому близки его проблемы, бизнесменом из Латинской Америки и человеком, несущим ответственность перед странами, в которых веду свой бизнес».

Он говорит о том, что его опыт не уникален, и предсказывает, что в будущем люди станут «более глобальными *и* более локальными» одновременно, сочетая в себе тягу к стране, в которой родились, деловые интересы и чистое любопытство. Он считает себя представителем «бизнес-диаспоры», члены которой — транснациональные предприниматели — «вовсе не смотрят на страну лишь как на источник быстрой наживы. Мы приходим надолго, занимаемся бизнесом и участвуем в ее развитии». Это может показаться слишком «романтичным», но на самом деле это трезвый расчет: «Развивая рынок, создавая спрос, воспитывая потребителей, вы расширяете свои возможности и укрепляете бизнес».

Мир становится все более взаимосвязанным. Входные барьеры для тех, кто хочет открыть свое дело, снижаются, и членство в «бизнес-диаспоре» вовсе не является привилегией тех, кто способен инвестировать значительные средства. Представьте себе студента из Индианы, с факультета вычислительной техники, написавшего игру для ведущей социальной сети, которая внезапно стала популярной среди шри-ланкийских пользователей. У студента и начинающего предпринимателя может не быть заграничного паспорта (и тем более каких-то знаний о Шри-Ланке), но игра вдруг начинает приносить ему хороший доход, неважно почему. Его любопытство растет, он добавляет в Facebook и Google друзей из Шри-Ланки, следит за

местными новостями в Twitter, узнает все больше и больше и, наконец, отправляется туда. То есть за очень короткое время ему удастся «сродниться» со страной, а ведь раньше на это могли уйти годы. В будущем с чем-то подобным столкнутся миллионы предпринимателей и разработчиков программного обеспечения, ведь онлайн-рынки окажутся больше и разнообразнее, чем можно представить.

В контексте восстановления страны такой прогноз, конечно же, обнадеживает, но даже крупнейшие телекоммуникационные компании, действующие из самых лучших побуждений, не могут полностью заменить государственные институты. Существует набор базовых товаров и услуг, обеспечить которыми свое население может только правительство: это безопасность, здравоохранение, снабжение чистой водой, транспортная инфраструктура и среднее образование. Развитие информационных технологий и доступ в сеть повысят эффективность выполнения этих функций, но лишь в сочетании с усилиями государственных органов.

В результате своего первого коллапса, случившегося в 1991 году, Сомали стало самым ярким примером несостоятельного государства. Одно переходное правительство сменялось другим, будучи не в состоянии справиться с голодом, межклановыми войнами, внешней агрессией, террористическими группировками и региональной раздробленностью страны. Возросшая популярность мобильных телефонов в последние несколько лет стала одной из немногих историй успеха на фоне этой анархии. Несмотря на неспокойную обстановку и отсутствие нормально функционирующего правительства, отрасль телекоммуникаций сыграла важнейшую роль во многих аспектах жизни общества, обеспечивая сомалийцев работой и информацией, делая более безопасной их жизнь и давая возможность связываться с миром. Вообще-то операторы сотовой связи — это единственные организованные структуры в Сомали, которые не зависят от отношений между кланами и племенами и функционируют во всех трех регионах страны: на юге и в центре Сомали (Могадишо), в Пунтленде на северо-востоке и Сомалиленде на северо-западе. В Сомали всего один коммерческий банк (созданный в мае 2012 года), и до появления мобильных телефонов для перевода денежных средств жителям страны приходилось полагаться на неформальную сеть

«хавала», операции в которой никак не регистрировались. Сегодня благодаря услуге мобильного перевода сотни тысяч сомалийцев могут пересылать деньги друг другу и получать денежную помощь из-за рубежа. А с помощью специальных платформ на базе SMS-рассылки они пользуются электронной почтой, получают котировки акций и информацию о погоде.

Чтобы хоть немного улучшить положение населения Сомали, иностранные неправительственные организации и частные компании регулярно запускают пилотные проекты на базе мобильных технологий. (Помимо прочего, мы наблюдали попытки построить платформу для поиска работы с помощью SMS и создать мобильную медицинскую систему с использованием дистанционной диагностики пациентов.) Впрочем, большая их часть заканчивается неудачей, что неудивительно, если учесть чрезвычайно враждебную для бизнеса среду и отсутствие безопасности. Вот почему большинство инноваций в Сомали происходят на местном уровне. Здесь, как и во всех развивающихся странах, наиболее креативные решения создаются силами самих сомалийцев, и как нигде они вызваны острой необходимостью.

Отсутствие центрального правительства в Сомали означает, что сектор телекоммуникаций никто не регулирует, что толкает тарифы вниз, поскольку при благоприятной возможности (и достаточно сильной тяге к риску) предприниматели могут просто взять и построить сеть. В ситуации, когда перестает работать государственный аппарат, это обычное дело. В первые недели после падения режима Саддама Хусейна сотовый оператор из Бахрейна попытался расширить свою зону охвата на юг Ирака, стремясь получить новых абонентов благодаря религиозной близости (население этого региона, как и в самом Бахрейне, преимущественно мусульмане-шииты). Но из-за страха перед разжиганием религиозной розни проект был свернут по решению командования оккупационных войск.

Благодаря абсолютно свободной от регулирования деловой среде в Сомали действуют рекордно низкие для Африки тарифы на местную и международную связь, а также на интернет, что делает использование мобильных устройств и интернета вполне доступным для населения страны, живущего в глубокой нищете. Часто бывает так, что

представитель сомалийской диаспоры в США звонит родственникам на родину, а они вешают трубку и *перезванивают* ему. Телекоммуникационные компании могут сохранять издержки на очень низком уровне и наращивать абонентскую базу, не теряя при этом прибыльности: нет ни налогов, ни платы за лицензию, ни иных обязательных сборов. Проникновение мобильной связи в Сомали гораздо выше, чем можно предполагать: около 20–25%. Четыре крупных оператора предлагают услуги голосовой связи и передачи данных не только во всей стране, но и на сопредельной территории Кении.

Несмотря на эти успехи в телекоммуникациях, Сомали остается исключительно опасной страной, а повстанцы по-прежнему используют доступ к мобильной связи и интернету для совершения насилия. Члены исламистской группировки «Аль-Шабааб» с помощью звонков и SMS угрожают миротворцам Африканского союза. Исламистские радикалы вводят запреты на применение мобильных банковских платформ и разрушают телекоммуникационную инфраструктуру. При этом пираты на сомалийском побережье пользуются местной сотовой связью, опасаясь, что их спутниковые телефоны можно отследить с кораблей международных сил. В докладе Совета безопасности ООН, опубликованном в 2012 году, глава крупнейшего сомалийского сотового оператора Hormuud был включен в список лиц, которым запрещено перемещение по миру, после того как выяснилось, что он является одним из главных спонсоров «Аль-Шабааб». (В докладе также говорится, что Али Ахмед Нур Джимал запустил в Hormuud мобильную систему денежных переводов как раз для того, чтобы организовать анонимное финансирование этой террористической организации.)

Конечно, ситуация в Сомали непростая. Но рано или поздно страна вырвется из кокона нестабильности, и тогда правительство наверняка найдет в национальных телекоммуникационных компаниях партнеров, готовых к сотрудничеству.

* * *

В идеале усилия по возрождению страны должны включать в себя не только воссоздание разрушенного и улучшение существующих методов и институтов, но и создание новых, с тем чтобы снизить риск повторения катастрофы в будущем. У большинства посткризисных обществ, при всем их различии в деталях, есть общие базовые потребности, которым приблизительно соответствуют основные компоненты государственного строительства. К ним относятся административный контроль над территорией, монополия на насилие, уверенное управление финансами государства, инвестиции в человеческий капитал, создание необходимой инфраструктуры и соблюдение гражданских прав и обязанностей[50]. И хотя в удовлетворении этих базовых потребностей посткризисное правительство может полагаться на иностранную помощь (финансовую, техническую и дипломатическую), основную работу ему придется сделать самостоятельно. А если реконструкция кажется чем-то чужеродным или не соответствующим политическим и экономическим целям общества, вероятность неудачи значительно возрастает.

Информационные технологии помогут защитить частную собственность, ведь сведения о недвижимости, хранящиеся в виртуальном пространстве, находятся в безопасности и позволяют законному собственнику предъявить на нее свои права с наступлением мира. А инвесторы вряд ли станут вкладывать деньги в рынки стран, если не уверены в безопасности. В Ираке после вторжения войск коалиции были созданы три комиссии для обработки заявлений местных жителей и беженцев о возврате изъятой режимом Саддама Хусейна недвижимости или выплате компенсаций за нее. Параллельно появился специальный орган по решению имущественных споров. Все эти важные шаги в деле восстановления Ирака сократили количество попыток насильственного возврата собственности в условиях послевоенной нестабильности. Однако, несмотря на благие намерения (к 2011 году было получено свыше 160 тысяч заявлений), работе комиссий мешали некоторые бюрократические ограничения, в результате которых многие требования привели к сложным судебным разбирательствам. В будущем страны усвоят иракский урок: многих

проблем в случае конфликта можно избежать благодаря более прозрачной и надежной системе защиты прав собственности. Если правительство введет в эксплуатацию онлайновую кадастровую систему (где будут храниться сведения о стоимости и границах земельных участков) с картографическим приложением, населению будет доступна информация обо всех частных и государственных землях, и даже мелкие споры (скажем, межевые) можно будет разрешать, направляя заявления официально назначенному онлайн-арбитру.

В будущем люди станут создавать не только резервные копии своих данных, но и «бэкап» правительства. В постепенно возникающем прототипе реконструкции параллельно с реальными институтами будут существовать виртуальные, одновременно выполняя роль их резервной копии — на всякий случай. И вместо здания для физического хранения документов и выполнения государственных функций министерству будет достаточно иметь «облачное» хранилище информации и онлайн-платформу. Если город разрушит цунами, все министерства продолжат свою работу в виртуальном пространстве, пока их деятельность не будет восстановлена в полном объеме.

Благодаря виртуальным институтам новое или пережившее кризис правительство сможет более-менее эффективно оказывать услуги обществу, а также участвовать в процессе реконструкции страны. Конечно, виртуальные общественные институты не заменят реальные, но окажут им огромную поддержку. Министерство социальной помощи, отвечающее за организацию крова над головой, по-прежнему будет нуждаться в физическом контакте с населением, но при наличии информации сможет, скажем, более эффективно распределять жилье. Виртуальное министерство обороны или министерство внутренних дел не обеспечат соблюдение законов, но проконтролируют своевременную выплату зарплаты военным и полицейским, что снимет напряжение. И хотя правительствам непривычно доверять свои данные компаниям — владельцам «облачных» хранилищ, наличие резервных копий обеспечивает спокойствие и вполне оправдывает такое решение.

Население, в свою очередь, получает своего рода страховку, которая гарантирует сохранность информации, выплату зарплат и безопасность

баз данных со сведениями о населении страны и членах диаспоры. Оно охотнее подключится к процессу реконструкции, а бремя нецелевых расходов и коррупции, этих вечных спутников природных катаклизмов и вооруженных конфликтов, значительно снизится. Может пасть правительство, может разрушиться физическая инфраструктура, но виртуальные институты выживут.

Правительства, вынужденные работать в изгнании, будут делать это на совсем ином уровне, нежели правительства Польши, Бельгии и Франции, которые бежали в Лондон во время Второй мировой войны. При условии надежного функционирования виртуальных институтов эффективность и возможности удаленной работы по управлению страной станут беспрецедентными. Конечно, это вынужденный шаг, вызванный природным катаклизмом или затянувшимися гражданскими войнами. Представьте себе, что правительство Сомали не может больше работать в Могадишо (там слишком обострилась ситуация из-за того, что город захватили боевики «Аль-Шабааб», или из-за полного разрушения инфраструктуры в результате межклanового противостояния). При наличии виртуальных институтов чиновники на время переехали бы в другое место, даже за границу, и при этом оставили за собой некое подобие контроля над ситуацией в стране. Выплата зарплат, координация деятельности благотворительных организаций и иностранных доноров, открытое общение с населением позволит сохранить определенный кредит доверия общества. Конечно, виртуальное дистанционное управление всегда остается крайней мерой (ясно, что увеличение дистанции не может не сказаться на отношении людей к власти). Кроме того, успешность удаленной работы зависит от определенных условий. В частности, это быстрые, надежные и безопасные сети; технически совершенные платформы; 100-процентный доступ населения в интернет. Сегодня ни одна страна не готова к этому — и меньше всех Сомали, но, если начать выстраивать эти системы уже сейчас, в нужный момент ими можно будет воспользоваться.

Потенциальная возможность действовать удаленно может повлиять и на политических эмигрантов. Если публичным фигурам, живущим за пределами своих стран, понадобится канал связи с родиной (хорошо известно, как аятолла Хомейни записал в Париже аудиокассеты со

своим обращением и они были тайно доставлены в Иран и распространены там), то сегодня есть множество быстрых, безопасных и эффективных способов. В будущем политики в изгнании смогут сформировать мощные и компетентные виртуальные институты и, как следствие, теневое правительство, которое будет взаимодействовать с населением страны и стараться отвечать его нуждам.

Это не такая большая натяжка, как может показаться. Благодаря интернету политики, которые живут за рубежом, будут гораздо меньше оторваны от своих соотечественников, чем прежде. Хорошо представляя тенденции и настроения в обществе, они смогут расширить свое влияние с помощью сообщений, рассчитанных на владельцев простых устройств и пользователей популярных платформ. Лидерам оппозиции не обязательно жить в одном городе, чтобы создать партию или движение: преодолеть придется только различия в идеологии, а не расстояния. А когда эти политики сформируют мощную базу поддержки и видение будущего своей страны, то смогут связываться со сторонниками на родине и передавать им все необходимые материалы, причем делать это не пересекая ее границ, быстро, безопасно и так широко, что никакое правительство не сможет остановить этот информационный поток.

В борьбе за умы и сердца аудитории оппозиционные политики в изгнании будут использовать подконтрольные им виртуальные институты.

> Представьте себе теневое правительство, которое из-за рубежа финансирует силы безопасности, состоящие из иностранных граждан и защищающие оплот оппозиции на родине. При этом его министерство здравоохранения находится в Париже (откуда управляет системой независимых госпиталей, координирует бесплатные кампании вакцинации, предлагает виртуальные медицинские программы, организует работу врачей, способных ставить диагнозы удаленно), а онлайн-школы и университеты размещены в Лондоне. Такое правительство в изгнании может организовать выборы в парламент, проведя в интернете и предвыборную кампанию, и голосование, причем парламентарии будут жить в разных странах, а видеотрансляцию заседаний в режиме реального времени смогут посмотреть миллионы пользователей по всему миру. Даже такого виртуального, но при этом реально функционирующего теневого кабинета может быть достаточно, чтобы население страны перестало поддерживать официальное правительство и перешло на сторону созданного и управляемого политиками, находящимися в изгнании.

Последняя отличительная черта прототипа реконструкции — весомый вклад интеллектуалов из диаспоры. Это характерная черта правительств в изгнании, однако теперь сфера деятельности соотечественников, живущих за рубежом, не будет ограничиваться лишь политикой или финансами. При наличии доступа в интернет будут сотрудничать, выполняя широкий круг задач, активисты по обе стороны границы. Члены диаспоры владеют бесценными знаниями и навыками, необходимыми для восстановления страны. Доступность коммуникационных технологий даст посткризисному обществу возможность воспользоваться этим богатым источником человеческого капитала. Признаки такого подхода уже проявляются. Представители сомалийской диаспоры активно использовали такие инструменты, как Google Map Maker, чтобы отмечать районы Африканского Рога, затронутые засухой 2011 года, и при этом составляли очень точные карты, что невозможно без знания обстановки и связей в местных сообществах.

В будущем мы станем свидетелями формирования своего рода корпуса резервистов из представителей диаспоры, организованного по профессиональному признаку: врачи, полицейские, строители, учителя и так далее. Власти страны будут стремиться получить информацию о сообществах соотечественников, живущих за рубежом (при условии, что они не враждебны существующему режиму), чтобы знать, какими навыками обладают его члены, и воспользоваться ими в трудные для родины времена.

Некоторые диаспоры сегодня гораздо более успешны, чем население их страны (это касается иранской, кубинской и ливанской диаспор, а также небольших групп вроде монов и сомалийцев). Но связи со своим отечеством поддерживает лишь часть сообществ. Остальные, осознанно или нет, сделали выбор в пользу новой родины — из-за больших возможностей, безопасности и качества жизни. Однако по мере распространения мобильной связи и интернета разрыв между диаспорой и населением страны ее происхождения будет сокращаться, поскольку коммуникации и социальные сети укрепляют культурные, языковые и политические связи между этими группами. А те, чей отъезд попадает под определение «утечка мозгов», будут

покидать страну пусть и бедную, с авторитарным режимом и отсутствием возможностей для самореализации, но с гораздо более развитыми коммуникациями, чем сегодня. Это значит, что на новом месте они смогут принести пользу и своей исторической родине, создав для нее виртуальную «экономику знаний», опираясь на образовательную систему, человеческий капитал и ресурсы развитых стран.

Предприимчивость и эксплуатация

В стране, пережившей крупный вооруженный конфликт или природный катаклизм, появляются новые игроки: сотрудники благотворительных организаций, журналисты, сотрудники ООН, консультанты, бизнесмены, спекулянты и туристы. Одни приезжают, чтобы помочь, другие — в надежде использовать кризисную обстановку для получения политических или экономических выгод. Многие совмещают то и другое, причем довольно эффективно[51].

Но даже те участники, для которых финансовый интерес не главное, не руководствуются исключительно альтруистическими мотивами участия в реконструкции. Посткризисная страна очень заманчива для некоммерческих организаций: это одновременно отличная лакмусовая бумажка для новичков и возможность показать свою ценность донорам для уже состоявшихся структур. Этот наплыв новых игроков — и альтруистов, и авантюристов — может принести и огромную пользу, и страшный вред. Перед теми, кто планирует восстановление страны, будет стоять непростая задача: сбалансировать интересы и действия всех этих людей и организаций, чтобы процесс шел наиболее продуктивно.

Наличие доступа к сети поощряет и облегчает альтруистические порывы. Становятся заметнее и понятнее страдания других людей, появляется больше возможностей что-то для них сделать. Кто-то может смеяться над активизацией «сетевого активизма», когда участие в общественной деятельности не требует практически никаких усилий, но это наше будущее, и составить о нем представление можно на примере таких дальновидных международных организаций, как Kiva, Kickstarter и Samasource. Все три действуют на базе простых онлайн-

платформ, причем первые две занимаются краудфандингом (Kiva фокусируется на микрофинансировании, а Kickstarter — на творческих задачах), а Samasource организует аутсорсинг «микропроектов» корпораций, помогая найти исполнителей в развивающемся мире. Внести свой вклад в восстановление далекой страны можно не таким прямолинейным способом, как пожертвование денежных средств, а, скажем, создавая обучающие или информационные материалы — и то и другое очень важно для процесса возрождения.

В результате того, что все больше людей в мире получают доступ к сети, будет расти количество потенциальных доноров и волонтеров, готовых помочь в случае крупномасштабного кризиса. Поскольку информация о конфликтах и стихийных бедствиях распространяется по различным платформам на всех языках в режиме реального времени, о кризисе в любой стране становится известно практически мгновенно. И пусть не все, кто узнал эту новость, немедленно бросятся на помощь, таких людей будет достаточно для того, чтобы масштаб участия добровольцев в спасательных операциях резко вырос.

> Хорошим примером того, что ожидает нас в будущем, может стать ликвидация последствий землетрясения в Гаити. Масштаб разрушений в окрестностях столицы этой густонаселенной и чрезвычайно бедной страны просто поражает: с лица земли были стерты дома, больницы и государственные учреждения; транспортная система и линии связи оказались парализованными; погибли сотни тысяч человек, свыше 1,5 млн остались без крыши над головой[52]. После катастрофы прошли считаные часы, когда правительства соседних стран направили в Гаити спасательные команды, а в следующие несколько дней помощь пообещали или даже выделили многие государства мира.
>
> Общественность отреагировала с еще большим энтузиазмом. В ходе инновационной кампании «SMS-помощи» за несколько дней Красный Крест собрал более $5 млн: абоненты мобильных сетей могли отправить SMS со словом «Гаити» на специальный короткий номер (90999) и пожертвовать $10, которые автоматически списывались с их счета. В целом по данным Фонда мобильных пожертвований, создавшего техническую инфраструктуру, которой пользуются многие НКО, посредством мобильных платформ было собрано свыше $43 млн. Специалисты гуманитарной организации «Телеком без границ», специализирующейся на организации связи в чрезвычайных ситуациях, высадились в Гаити уже на следующий день после землетрясения и занялись организацией колл-центров, с помощью которых гаитянцы могли бы связаться с близкими людьми. А спустя пять дней после катастрофы портал гуманитарных

новостей AlertNet, проект фонда Thompson Reuters Foundation, запустил первую в своем роде услугу Emergency Information Service, что позволило жителям Гаити получать информационные SMS.

Спасательные работы постепенно сменились долгосрочными проектами по восстановлению страны, и через несколько месяцев в Гаити работали уже десятки тысяч сотрудников некоммерческих организаций. Трудно представить себе, что столько организаций смогут эффективно заниматься одним делом, с четкими целями и не мешая друг другу, в одном месте, особенно в такой небольшой, густонаселенной и опустошенной стихией стране, как Гаити. И действительно, через некоторое время начали появляться тревожные сообщения о неэффективном распределении помощи. Из-за плохого управления склады были заполнены неиспользованными и просроченными медикаментами. В переполненных лагерях вспыхнула холера, которая угрожала тем, кто выжил после землетрясения. Финансовая помощь от институциональных доноров, в основном иностранных правительств, приходила с задержками и с трудом поддавалась учету, а из того, что было направлено, до самих гаитянцев доходили какие-то крохи, остальное оседало в карманах распределяющих организаций. Прошел год после катаклизма, а сотни тысяч жителей Гаити по-прежнему жили в палатках в антисанитарных условиях, поскольку правительство и его партнеры из числа НКО так и не нашли возможность обеспечить их жильем. Несмотря на внимание СМИ, активный сбор финансовых пожертвований, планы по координации усилий и добрые намерения, после того разрушительного землетрясения гаитянцы не получили должной помощи.

Отрицательный опыт Гаити был внимательно изучен специалистами, которые извлекли из него важные уроки. Пол Фармер в книге «Гаити после землетрясения»[53] привел общую точку зрения: всему виной — неблагоприятное стечение обстоятельств, вызванное обширными разрушениями, наложенными на бюрократическую неэффективность и серьезные застарелые проблемы гаитянского общества. Не стоит думать, что коммуникационные технологии могли бы исправить все беды Гаити, но при правильном и активном применении онлайн-платформ процесс координации усилий всех участников прошел бы более гладко. В будущем в каких-то похожих ситуациях можно было бы достичь больших результатов с меньшими потерями и за более короткое время. Далее мы изложим свое мнение, хотя отлично понимаем, что крупные НКО и иностранные правительства, которые обычно помогают восстанавливать страну, могут их отвергнуть из страха потерпеть неудачу или лишиться своего влияния.

* * *

Во время следующей волны природных катаклизмов и конфликтов, которые придутся на цифровую эпоху, модель работы международных благотворительных организаций, вероятно, изменится. Вследствие появления большего количества потенциальных доноров и более активного проведения информационных кампаний в каждом посткризисном обществе сначала будет возникать, а затем лопаться «пузырь НКО», что приведет к децентрализации оказания помощи и множеству экспериментов в этой области.

Исторически благотворительные организации со стажем отличаются друг от друга не столько методами, сколько брендом. Внимание публики гораздо легче привлечь броским логотипом, пронзительной рекламой и настойчивыми призывами внести пожертвование, чем подробными отчетами о логистике поставок, закупке противомоскитных сеток и постепенном улучшении ситуации в пострадавшем регионе. Возможно, лучший пример такого подхода — известный видеоролик «Кони-2012», созданный неправительственной организацией Invisible Children для привлечения внимания к войне, которая уже несколько десятков лет идет на севере Уганды. Хотя миссия НКО вполне благородна — прекратить зверства, чинимые угандийской военизированной группировкой «Господня армия сопротивления», — наблюдатели, хорошо знакомые с историей конфликта, включая многих угандийцев, считают, что ролик вводит зрителей в заблуждение, упрощает проблему и в конечном счете служит определенным целям организации. Тем не менее меньше чем за неделю ролик собрал больше 100 млн просмотров (став первым в истории вирусным видеороликом, которому это удалось), в основном благодаря известным личностям с миллионами читателей в Twitter. Первая волна критики этой НКО и ее деятельности, основанная на обвинениях в том, что 70% собранных пожертвований были направлены на «производственные нужды» (в основном зарплаты), не смогла затормозить рост организации. Потом произошел странный случай, привлекший всеобщее внимание: один из основателей вдруг обнажился в общественном месте, после чего был арестован, и история этой НКО закончилась.

Как мы уже говорили, в цифровую эру маркетинг будет играть особенно заметную роль. Любой, кто зарегистрировал НКО или благотворительную организацию (или решил обойтись без регистрации), может создать яркую онлайн-платформу с высококачественным контентом и классным мобильным приложением. Для индивидуумов и организаций это самый быстрый и простой способ «отметиться». Их истинная сущность: насколько они устойчивы и компетентны, как управляют своими финансами, хороши ли их программы — мало что значит. Используя в своих интересах слабое знание донорами реалий жизни в далекой стране, новые игроки найдут способ эксплуатировать это (совсем как некоторые радикальные создатели стартапов, уверенные, что стиль важнее сути). А когда случится стихийное бедствие и на сцену выйдут НКО, окажется, что на ней соседствуют как организации со стажем, так и стартапы, то есть группы, активно ведущие себя в сети и собравшие некоторый начальный капитал, но не проверенные в деле. Такие стартапы будут более целеустремленно выполнять свою миссию, чем традиционные благотворительные организации, и казаться столь же, если не более, компетентными. Они привлекут к себе внимание, но не смогут в полной мере помочь нуждающимся. Некоторые окажутся вполне состоятельными, но большинство не справятся с задачей из-за отсутствия наработанных связей и технических навыков профессиональных организацией со стажем, а также плохого знания проблемы.

Несоответствие между маркетинговой активностью и результатами деятельности благотворительных стартапов будет раздражать традиционные НКО. Ведь и те и другие конкурируют за одни и те же ресурсы, а стартапы оттягивают их, пользуясь лишь виртуальной харизмой и знанием различных интернет-аудиторий. Они будут выставлять крупных институциональных игроков неуклюжими, неэффективными, оторванными от жизни, лишенными индивидуальности монстрами, упрекать их высокими накладными расходами и раздутым штатом и обещать вместо этого обеспечить донорам близость к получателям помощи за счет устранения ненужных посредников. Для доноров-новичков, стремящихся внести свой вклад в восстановление страны, это обещание прямого контакта

окажется крайне привлекательным маркетинговым ходом, ведь благодаря доступу в интернет многие из них уже чувствуют свою личную вовлеченность в кризис.

Представьте себе недавнего выпускника университета из Сиэтла, неравнодушного к происходящему в мире альтруиста, готового пожертвовать несколько долларов на доброе дело. Скоро он не только сможет быть «свидетелем» каждого крупного несчастья — его засыплют призывами помочь нуждающимся. Ими будут забиты его папка «Входящие», лента Twitter, профиль в Facebook и поисковые выдачи. Несмотря на обилие предложений, он все же попытается разобраться в них и быстро принять решение, основываясь на внешних факторах: у какой группы лучше сайт, активнее поведение в социальных сетях, известнее сторонники. Если он не эксперт, то как ему решить, какая из организаций достойна пожертвования? Ему придется полагаться на доверие, а в этом смысле преимущество у тех, кто способен лучше организовать продвижение и донести свое предложение.

Существует вполне реальный риск, что такие стартапы вытеснят традиционные НКО. Некоторые из них будут по-настоящему полезными, но далеко не все окажутся настоящими. Новыми возможностями прямого маркетинга и низкими барьерами для входа воспользуются авантюристы. Когда, наконец, их призовут к ответу, доверие доноров будет потеряно (или возникнет инерция, или появятся другие мошенники). Кроме того, мы столкнемся с переизбытком имиджевых проектов известных звезд шоу-бизнеса и представителей деловой элиты, чьи энергичные кампании еще сильнее отвлекут внимание от реальной, практической работы. В конечном счете превращение «добрых дел» в соревнование маркетинговых бюджетов приведет к увеличению количества игроков, но уменьшению объема помощи, поскольку старожилы будут оттерты новичками.

Как мы говорили, чтобы помогать, нужно обладать опытом. Но когда игроков слишком много, становится труднее координировать оказание помощи, устанавливать реалистичные цели и контролировать их достижение. И здесь пригодятся высокие технологии. Власти страны могут создать централизованную базу данных всех НКО, фиксируя их достижения, вести мониторинг результатов и присваивать

им рейтинг, в том числе на основе отзывов населения. Системы мониторинга и оценки, которые помогают повысить ответственность и выявить недостатки благотворительных организаций, уже появились. Это Charity Navigator — база данных организаций гражданского общества One World Trust и NGO Ratings, но они сами являются НКО и поэтому не имеют каких-либо возможностей активно влиять на работу других организаций. Представьте себе создание системы расчета рейтинга, которая помогает донорам определить направление их финансирования, где используются данные о деятельности, финансовом положении и качестве управления организацией, а также отзывы представителей местных сообществ и получателей помощи. Такой инструмент мог бы иметь вполне практическое значение: скажем, те, чей рейтинг падает ниже определенного значения, теряют право на получение финансирования от правительства или попадают под контроль и проверку регулирующих органов. В отсутствие интегрированной, прозрачной системы ранжирования и мониторинга благотворительных организаций правительства и частные доноры будут погребены под потоком призывов сделать пожертвование, не имея возможности выделить наиболее компетентных и законопослушных игроков.

А потом этот пузырь лопнет, как и все остальные. Процесс оказания помощи замрет, а институциональные доноры потеряют доверие к проектам восстановления других стран. Когда же осядет пыль, выживут только те организации, у которых есть четкая стратегия, лояльные доноры и большой опыт эффективных и прозрачных операций. Одни из них будут опытными экспертами по оказанию помощи, другие — новичками, но и те и другие должны суметь приспособиться к специфике проектов по реконструкции, характерных для цифровой эпохи. Нужно не только реализовывать крупные программы с измеримыми результатами, но и обладать отличными навыками виртуального маркетинга, уметь представлять свою деятельность в выгодном свете и обеспечивать как доноров, так и получателей помощи механизмом обратной связи. Умение продемонстрировать ответственность и стремление к прозрачности значат многое.

Сохранится стремление к непосредственному взаимодействию между донорами и получателями помощи. Уже сегодня складывается долгосрочный тренд — децентрализация распределения помощи, и некоммерческие организации берут на вооружение новые методы. Система, в которой действовали несколько ключевых игроков (крупных институциональных НКО), превращается в широкую сеть из более мелких участников. Если прежде пожертвования вносились через центральное отделение Красного Креста или международной организации по защите прав детей Save the Children, то сегодня хорошо информированные доноры все чаще выбирают конкретные и наиболее близкие им программы или направляют взносы в небольшие НКО-стартапы. Самые дальновидные из традиционных НКО перестроят свою деятельность, перестанут просто распределять средства сверху вниз и будут выступать скорее в роли агрегаторов, помогая преодолеть разрыв между донорами и получателями помощи, передавая им опыт по-настоящему личного общения. Можно связывать врачей из развитых стран с пострадавшими из регионов, затронутых землетрясением, сохраняя при этом полный контроль над программой. (Понятно, что такой тесный контакт интересен не всем донорам. Для них будет предусмотрена возможность отказаться от этой функции.)

Нельзя не учитывать роли, которую в условиях новой цифровой экосистемы распределения помощи станут играть жители пострадавших от природного катаклизма или внутреннего конфликта стран. В частности, наличие доступа в сеть повлияет на то, как будет решаться проблема вынужденных переселенцев — одна из крупнейших и наиболее частых проблем, с которыми сталкиваются посткризисные общества. Из-за границы почти невозможно повлиять на факторы, которые вызывают появление вынужденных переселенцев, — войну, голод, стихийные бедствия. Но их жертвам способны помочь мобильные телефоны. У большинства переселенцев они будут, а среди тех, у кого телефонов не окажется, благотворительные организации их распределят. Лагеря беженцев оборудуют точками доступа в интернет на базе технологии 4G, и это позволит людям связываться друг с другом легко и почти бесплатно, а при наличии мобильных телефонов задача регистрации упростится донельзя.

Большинство вынужденных переселенцев и беженцев среди главных своих проблем называют отсутствие информации. Обычно они не знают, как долго пробудут в этом месте, когда им доставят еду, а если не доставят, то где найти ее самостоятельно, где взять дрова и воду, как обстоят дела с лечением, что им может угрожать. При наличии регистрации и доступа к специализированным платформам, созданным специально для ответов на такие вопросы, беженцы станут получать оповещения, сориентируются в обстановке и узнают о том, где и когда распределяют продукты и вещи международные благотворительные организации. Для поиска пропавших людей будут активно использоваться программы распознавания лиц. С помощью системы голосового ввода неграмотные пользователи смогут ввести в поисковый запрос имена потерянных родственников и узнать, есть ли информация о них в базе данных вынужденных переселенцев и беженцев. При наличии онлайн-платформ и мобильных телефонов у администрации лагерей появится возможность классифицировать и организовать его жителей в соответствии с их навыками, опытом и интересами. Как правило, в лагерях беженцев много людей востребованных профессий (врачи, учителя, футбольные тренеры), но, пока они участвуют в жизни сообщества не в полную силу, люди передают информацию о них из уст в уста. У жителей таких лагерей должен быть доступ к специальному приложению, в котором можно будет указать свою профессию или найти человека с нужными навыками, и тогда удастся привлечь к общественно полезной деятельности всех, кто хочет и может работать.

Широкое распространение мобильных телефонов создает новые возможности для тех, кто хочет изменить существующую модель распределения помощи. Несколько предприимчивых пользователей с начальными навыками создания приложений могут построить открытую платформу, с помощью которой такие же, как они, нуждающиеся в поддержке будут формировать список потребностей и свои контактные данные, направлять их в «облако» и ждать, когда появятся индивидуальные доноры, выберут их и передадут им свои пожертвования напрямую. Это несколько похоже на ту модель, которая используется в Kiva для организации сделок микрофинансирования, с той лишь разницей, что здесь шире спектр возможностей,

индивидуальнее подход и пожертвования вместо займов. (Естественно, прежде чем такие платформы заработают, их создателям придется разрешить множество технических и юридических проблем.)

А теперь представьте себе, что эта платформа выстроила партнерские отношения с крупной благотворительной организацией, которая донесет информацию до более широкой международной аудитории, одновременно проверив ее, насколько возможно, чтобы успокоить скептиков. И тогда какая-нибудь жительница западной страны, оторвавшись от просмотра на своем iPad ролика с записью футбольного матча, в котором участвовал ее сын, сможет изучить карту мира (интерактивную и постоянно обновляемую), на которой будет видно, кто, где и в чем нуждается. А выслушав историю, рассказанную человеком, самостоятельно решить, кому стоит помочь, и перечислить пожертвование или микроссуду непосредственно их получателю через систему мобильных денежных переводов, так же быстро и просто, словно отправить SMS.

Проблема подобных платформ заключается в том, что бремя продвижения заявки ложится непосредственно на того, кто нуждается в помощи. В лагерях беженцев жизнь достаточно трудна и без того, чтобы заботиться о том, как произвести впечатление человека нуждающегося; кроме того, жесткая конкуренция за ресурсы, к которой подталкивают получателей помощи такие платформы, сомнительна с точки зрения этики. Возможен риск, что доноры, которые плохо разбираются в ситуации или не знают истинного положения вещей, будут непропорционально щедро поддерживать тех, кто лучше продвигает свою историю (или просто обманывает систему), а не тех, кому действительно нужна помощь. Следствием исключения из процесса опытных НКО станет то, что такие доноры не смогут правильно определять потребности в помощи и, соответственно, справедливо распределять ее. В отсутствие механизмов контроля общедоступная система прямых пожертвований почти наверняка приведет к *менее* равномерному распределению ресурсов. Исследователи из Сингапура проанализировали динамику займов, выданных посредством сайта Kiva, и показали, что кредиторы склонны к дискриминации заемщиков, отдавая предпочтение внешне привлекательным, светлокожим и менее тучным людям.

Кроме того, появление подобных платформ говорит о том, что встречное желание иметь более прямую связь с донорами есть и у получателей помощи. Они *хотят*, чтобы отношения строились именно так, а это бьет по тем организациям, которые уже давно не новички в деле восстановления пострадавших регионов. Конечно же, многие жители посткризисных стран (впрочем, как и развивающихся) будут рады возможности напрямую продвигать себя в качестве заемщика, если это обеспечит их более надежным источником средств. Но таких меньшинство. В отличие от сервиса Kiva, где выдают микроссуды, здесь речь идет о просьбе пожертвований, причем публичной. Гордость — универсальное человеческое качество, и часто чем меньшим имуществом человек обладает, тем выше ценит свою гордость. Трудно представить себе, что в поисках финансирования вынужденные переселенцы, беженцы и прочие нуждающиеся готовы будут «рекламировать» свою нужду международной аудитории. Традиционные благотворительные организации выполняют одну важную функцию — создают дистанцию между получателями помощи и теми, кто ее оказывает. Так что, несмотря на все описанные перемены: НКО-стартапы, микропрограммы финансирования, децентрализованное распределение помощи, — не стоит забывать о том, как возникли те или иные аспекты благотворительности и почему некоторые из них работают хорошо.

Пространство для инноваций

Если в разрушении общественных институтов и систем и есть что-то позитивное, то это возможности для реализации новых идей. Пространство для инноваций существует повсюду, даже в трудоемком и непростом деле восстановления страны, а наличие быстрых каналов связи, сильных руководителей и разнообразных технических устройств — смартфонов и планшетов — позволяет эти инновации ускорить.

Мы уже видели, как можно использовать возможности интернета в посткризисной ситуации.

Ярким примером является работа проекта Ushahidi (в переводе с суахили — «свидетельство очевидца»), картографической платформы с открытым кодом, которая позволяет агрегировать данные пользователей и строить информационную карту. После гаитянского землетрясения в 2010 году всего лишь через час после удара стихии волонтеры Ushahidi из США на базе простой картографической программы построили обновляющуюся в режиме реального времени карту. При этом был выделен специальный короткий номер (4636), чтобы жители пострадавших районов могли посылать на него текстовые сообщения, а сводную информацию затем передавали национальные и местные радиостанции Гаити. Все данные о разрушениях, потребностях в спасательной технике и оборудовании, оказавшихся в ловушке людях, случаях насилия и преступлений сразу же попадали на интерактивную онлайн-карту. Многие текстовые сообщения были на креольском, и сотрудники Ushahidi сформировали сеть из тысяч американцев гаитянского происхождения, так что время на перевод сократилось до десяти минут. В течение нескольких недель на карту были нанесены данные из 2500 сообщений. По словам Кэрол Уотерс, директора по коммуникациям и партнерским программам Ushahidi, многие из них были очень простыми: «Крыша обрушилась, но я еще жив». Благодаря быстрой реакции и навыкам программирования команды проекта Ushahidi были спасены многие жизни.

В будущем подобные кризисные карты станут нормой; возможно, их создание инициирует правительство. При централизации информации в рамках официального и доверенного источника удастся избежать ряда проблем, с которыми столкнулся Ushahidi (некоторые НКО не знали о существовании этой платформы). Конечно, существует опасность, что государственные проекты станут жертвой бюрократии или юридических ограничений и не будут столь эффективными, как частные проекты вроде Ushahidi. Но если карта, созданная под эгидой правительства, все же позволит немедленно реагировать на события, ее потенциал окажется неизмеримо выше, ведь она сможет агрегировать гораздо больше данных. Такую карту можно использовать и в процессе восстановления пострадавших районов: с ее помощью власти будут делиться информацией о проектах реконструкции и получать обратную связь.

С помощью этих карт жители пострадавших районов могли бы узнавать о границах небезопасных зон (где заложены мины или действуют вооруженные группировки), о качестве покрытия сотовой связи, о распределении инвестиций и ходе восстановления нормальной жизни. А благодаря сообщениям людей правительство будет знать о

совершенных преступлениях, случаях насилия и коррупции. Интегрированная система информирования на случай кризиса не только сделает жизнь людей безопаснее, но также снизит потери, уровень коррупции и дублирования, свойственные любым проектам реконструкции. Конечно, не всегда власти ставших жертвой кризиса стран заинтересованы в такой прозрачности, но если о существовании этой модели будет известно, то население и международное сообщество окажут давление на правительство, достаточное для ее реализации. Это может стать условием предоставления иностранной помощи. И, естественно, в развертывании такой системы с готовностью поучаствует множество негосударственных партнеров и волонтеров.

Главным приоритетом властей в любой посткризисной ситуации остается обеспечение безопасности. И в этом тоже помогут интерактивные карты, однако их будет недостаточно. Первое время после окончания конфликта — наиболее сложное, потому что переходное правительство должно доказать людям, что оно контролирует положение и слышит их, или же оно рискует быть сметенным тем же народом, который его выбрал. Налаживая повседневную жизнь, люди должны чувствовать, что можно без страха открывать свое дело, восстанавливать дома и возделывать посевы, а значит, власти, которые стремятся завоевать доверие населения и возродить страну, должны снизить уровень неопределенности в обществе. Грамотное использование современных технологий поможет правительству восстановить власть закона.

Благодаря своей функциональности мобильные телефоны станут ключевым каналом передачи информации и чрезвычайно ценным фактором повышения безопасности. В странах с боеспособной армией ответ на вопрос, будут военные гарантировать соблюдение законов или сами нарушать их (совершая преступления или захватывая власть), зависит не столько от мотивации людей в форме, сколько от их веры в компетентность правительства. Проще говоря, большинству из них важно знать, получат ли они денежное довольствие вовремя и в полном объеме и кто за это отвечает.

Технологические платформы помогут поддерживать законность и в этом случае. Каждый полицейский и военнослужащий будет иметь

специальный мобильный телефон с несколькими хорошо защищенными приложениями, одно из которых должно отвечать за выплату зарплат и служить интерфейсом между владельцем телефона и соответствующим министерством. В Афганистане телекоммуникационная компания Roshan запустила пилотную программу электронных выплат служащим национальной полиции Афганистана посредством мобильной банковской платформы — огромный шаг в сторону обуздания чудовищной коррупции, которая душит финансовую систему страны. С помощью другого приложения офицер сможет докладывать о своих действиях в течение дня, как если бы делал записи в специальном журнале, причем данные будут сохраняться в «облаке», чтобы командиры впоследствии могли измерить эффективность и результативность его работы. Еще одно приложение явится инструментом обучения или виртуальным наставником для сотрудников-новичков (как в Ливии, где многие бойцы народной милиции интегрировались во вновь созданную армию) и одновременно средством безопасного и анонимного информирования командиров о случаях коррупции или иных незаконных действиях их коллег.

Позиции государства в деле поддержания безопасности укрепятся, если население будет сообщать о нарушениях закона с помощью мобильных платформ. Каждый владелец мобильного телефона в любой момент сможет зафиксировать нарушения, выступая одновременно и потенциальным свидетелем, и следователем, причем число таких людей намного превышает количество сотрудников правоохранительных органов. При благоприятном развитии событий люди будут проявлять бдительность, активно пользоваться этой мобильной системой и формировать вместе с властями более безопасное и честное общество, руководствуясь патриотическими соображениями или собственными интересами. А при неблагоприятном — когда значительная часть населения не доверяет правительству или перешла на сторону его оппонентов (как те, кто боролся с Каддафи) — такие каналы обратной связи можно использовать для дезинформации и пустой траты времени полиции.

Важно не только решить базовые проблемы безопасности, но и привлечь население к процессу восстановления страны. При наличии

качественных мобильных платформ и желания правительства обеспечить прозрачность рядовые граждане смогут отслеживать достигнутые успехи, сообщать о коррупции, вносить свои предложения и включиться в диалог между правительством, НКО, другими международными организациями — и все это при помощи мобильного телефона. Мы разговаривали с президентом Руанды Полем Кагаме, одним из самых технически грамотных руководителей в Африке, и спросили его, как мобильные технологии меняют отношение людей к местным проблемам. По его словам, «когда людям что-то понадобится — в социальном, экономическом плане или в плане безопасности, — они обратятся к своим телефонам, потому что телефоны будут их единственным способом самозащиты. Если кому-то нужна срочная помощь, он ее получит». Кагаме считает, что мобильная связь полностью изменила правила игры для населения развивающихся стран, особенно в тех случаях, когда страна пытается оправиться от недавнего конфликта или кризиса. Доверие к правительству жизненно важно, а благодаря использованию открытых платформ оно возникает быстрее: «Мы в Руанде запустили программу общественного контроля и реагируем на информацию, которой с нами делятся члены местных сообществ». Эффективность этой программы повышается за счет применения современных технологий, подчеркивает Кагаме.

Поскольку участие общественности становится неотъемлемой чертой установления власти закона (по крайней мере если стране приходится бороться с последствиями конфликта или стихийного бедствия), постепенно в обществе повысится и ответственность за свои действия. Страх перед грабителями или мародерами останется, но в будущем люди станут хранить документы, подтверждающие владение личными вещами и семейными реликвиями, в виртуальном пространстве, так что после восстановления порядка будет несложно доказать, что именно было утрачено. Можно стимулировать отправку на определенный адрес фотографий грабителей с добычей (даже если это полицейские), назначив за это, например, вознаграждение. Конечно, остается риск мести со стороны преступников, однако большинство людей преодолевают его и согласны рисковать. А чем больше свидетелей готовы сообщить о преступлении, тем сильнее

снижается риск для каждого. Представьте, что ограбление знаменитого Багдадского музея 2003 года произошло на 20 лет позже: как долго воры могли бы прятать украденные сокровища (не говоря уже о том, чтобы попытаться продать их), если бы об этом случае мгновенно узнала вся страна и люди были мотивированы на то, чтобы сообщить о местонахождении преступников?

Кража исторических ценностей задевает гордость нации и наносит урон ее культуре, но кража оружия представляет собой большую опасность для стабильности страны. Тяжелое вооружение и стрелковое оружие обычно «исчезает» после завершения конфликтов и оказывается на черном рынке (его размер оценивается в $1 млрд в год), а затем попадает в руки членов неформальной милиции, гангстеров и военных других стран. Эту проблему поможет решить радиочастотная идентификация (RFID) с использованием радиометок. Радиометки содержат цифровую информацию и могут иметь размер с рисовое зернышко. Сегодня их можно встретить на чем угодно — от телефонов и паспортов до продуктов, которые мы покупаем. (Их используют даже владельцы домашних животных: вживление радиометки под кожу или закрепление на ухе помогает отыскать потерявшихся любимцев.) Если бы крупные страны — производители оружия договорились устанавливать неизвлекаемые радиометки на все свои продукты, это упростило бы поиск тайников с оружием и помогло пресекать незаконные поставки вооружения. Учитывая, что сегодняшние радиометки можно легко уничтожить, «поджарив» их в микроволновке, следующее поколение должно быть лучше защищено от уничтожения и подделки. (Думается, что начнется очередная технологическая игра в «кошки-мышки» между правительствами, которые хотят отслеживать поставки оружия с помощью радиометок, и подпольными торговцами оружием, которые не склонны афишировать свои сделки.) Если обнаружено вооружение с радиометками, то можно узнать источник его происхождения при условии, что конструкция чипов позволяет хранить такие данные. Скорее всего, это не остановит нелегальные поставки оружия, но окажет давление на крупнейших игроков рынка.

Страны, которые спонсируют повстанческие движения и снабжают их оружием, хотят контролировать его использование. При наличии

радиометок провести расследование довольно легко. Точное количество ливийских революционеров не было известно практически никому, и, учитывая невозможность проконтролировать распределяемое среди них оружие, властям стран, которые этим занимались, приходилось взвешивать выгоды от проведения успешной революции и возможные последствия того, что это оружие окажется на черном рынке. (В начале 2012 года часть оружия, которым пользовалось ливийское ополчение, оказалось в Мали, в руках воинственных туарегов. После возвращения в страну состоящих из туарегов подразделений бывшей армии Каддафи это создало условия для вооруженного мятежа.)

При создании системы электронного контроля за поставками вооружений придется преодолеть множество трудностей: разработка оружия с радиометкой потребует крупных затрат; производители часть прибыли получают за счет черного рынка их продуктов; и властям, и торговцам оружием выгодна анонимность существующей системы дистрибуции. Трудно представить, что какая-то из сверхдержав ради долгосрочного блага добровольно пожертвует возможностью создавать тайные склады оружия или продавать его через посредников. Более того, они могут заявить, что есть опасность возникновения *нового* конфликта, если кто-то подбросит в зону противостояния оружие из непричастной к нему страны. Впрочем, многое зависит от мнения международной общественности.

К счастью, существует множество других путей использования технологии RFID в процессе восстановления страны. С помощью радиометок можно отслеживать поставки гуманитарной помощи и других жизненно важных товаров, проверять подлинность лекарств и иных продуктов, тем самым снижая коррупцию и «откаты» при реализации крупных контрактов. Всемирная продовольственная программа проводила эксперимент: отслеживание поставок продовольствия в Сомали с помощью штрихкодов и радиометок, чтобы определить, какие поставщики ведут себя честно и действительно доставляют продукты в нуждающиеся в них регионы. Благодаря такой системе контроля — недорогой, универсальной и надежной — можно заметно оздоровить ситуацию с распределением гуманитарной помощи, повысив ответственность и собирая

информацию, которой можно воспользоваться для измерения успешности и эффективности этой работы даже в регионах с низким проникновением интернета.

* * *

В посткризисный период для решения проблем бывших участников боевых действий власти могут воспользоваться таким инструментом, как мобильные устройства. Обмен оружия на мобильные телефоны способен стать ключевым элементом любой программы разоружения, демобилизации и реабилитации. При всей неоднозначности правительства Поля Кагаме с точки зрения соблюдения прав человека и государственного управления оно провело успешную демилитаризацию десятков тысяч бывших солдат в рамках Руандийского проекта демобилизации и реабилитации. «Мы считаем, что те, кто воевал, смогут изменить свою жизнь, только если мы дадим им инструменты», — объясняет Кагаме. В пакет предложений участникам боевых действий входила «некоторая сумма денег, а еще мобильные телефоны, чтобы они могли увидеть открывающиеся перед ними перспективы». Большинство участников этой продолжающейся программы также проходят обучение, которое готовит их к интеграции в общество. Важным компонентом является психологическая подготовка. Мы видели реализацию программы в действии: больше всего это напоминает летний лагерь с учебными классами, общежитием и спортивными играми, что понятно, ведь многие участники боевых действий в Руанде еще практически дети. Главное здесь — собрать их вместе с сотнями таких же, имеющих похожий опыт, и развить в них уверенность в том, что жизнь продолжается и после окончания войны.

Слова Кагаме свидетельствуют о том, что не за горами те времена, когда так же будут поступать и другие страны. По окончании любого конфликта высшим приоритетом является разоружение его участников. (Цель разоружения, которое иногда также называют «демилитаризацией», или «сдачей оружия», состоит в том, чтобы лишить участников конфликта, будь то повстанцы, народное ополчение или армейские подразделения, оставшиеся от прежнего

режима, возможности вести боевые действия.) В соответствии с типичной программой разоружения, демобилизации и реабилитации участники конфликта в течение определенного времени сдают оружие миротворцам, часто получая за это определенную компенсацию. Чем дольше длился конфликт, тем больше времени нужно на разоружение.

> Для создания государства Южный Судан (нам представилась возможность посетить его в январе 2013 года) потребовались годы борьбы между армиями севера и юга Судана, и новое южносуданское правительство сразу признало необходимость провести полномасштабную программу разоружения. На эту программу правительствами Китая, Японии, Норвегии и США, а также ООН было выделено больше $380 млн, а власти по обе стороны границы договорились до 2017 года разоружить около 200 тысяч человек. Два соседних государства, Уганда и Кения, обеспокоенные возможностью превращения бывших бойцов в наемников и нелегального перетекания оружия через их границы, также пообещали поддержку в усилении системы национальной безопасности обеих стран, что представляет собой критически важный элемент плана. Однако в районе Великих Африканских озер продолжают сохраняться очаги конфликтов, ситуация там непредсказуемая, так что к этим заверениям стоит относиться с определенной долей скепсиса.

В большинстве случаев после окончания вооруженного конфликта приходится иметь дело с участвовавшими в нем вооруженными, а теперь не имеющими работы, цели в жизни, социального статуса и места в обществе людьми. Если эти проблемы не решать, бывшие солдаты могут вернуться к насилию, особенно если у них есть оружие. И может так оказаться, что для властей страны, стремящихся мотивировать участников конфликта сдать свои АК-47С, хорошим выходом будет обменивать их на смартфоны. Бывшие солдаты нуждаются в компенсации, статусе и возможности сделать следующий шаг. Если им объяснить, что смартфон — это не просто устройство для связи, но и инструмент для получения льгот и платежей, он превращается в инвестицию, на которую имеет смысл обменять оружие.

В рамках такой инициативы каждое общество в зависимости от своих культурных особенностей и уровня технических знаний предложит свой, несколько отличающийся от остальных компенсационный пакет. В его основе будет лежать универсальный

набор: бесплатный смартфон из премиального сегмента, дешевые тарифные планы на звонки и передачу SMS, кредит на приобретение мобильных приложений и субсидирование передачи данных, чтобы можно было недорого пользоваться интернетом и электронной почтой. Эти смартфоны должны быть более качественными, чем те телефоны, что в среднем использует население, и дешевле в применении. В них могут быть заранее загружены привлекательные для бывших солдат приложения, которые ускорят их развитие, например уроки английского или базовый курс обучения грамоте. И тогда подросток из лагеря беженцев в Южном Судане, еще в детстве разлученный с родителями и взявший в руки оружие, получил бы устройство, которое позволит ему связываться не только с родственниками, но и с потенциальными кураторами из суданской диаспоры, возможно, с ровесниками, нашедшими прибежище в США, и начать новую жизнь.

На начальной стадии подобные программы могли бы оплачивать государства-доноры, впоследствии перекладывая бремя расходов и контроль за их реализацией на сами пострадавшие от конфликта страны. Тогда власти получат возможность присматривать за бывшими участниками вооруженного конфликта и их интеграцией в общество с помощью программного обеспечения, заранее загруженного в телефон и позволяющего в течение некоторого времени следить за передвижениями его владельца или анализировать посещенные им сайты. Если выяснится, что бывший солдат нарушает определенные правила, он потерял бы право пользоваться выгодным тарифным планом или даже самим телефоном. Государство могло бы применять политику трех предупреждений: после первого раза, когда участник программы пропустил виртуальный аналог встречи с сотрудником службы пробации[54] в заранее оговоренное время, он получает короткое видеопредупреждение; второе нарушение — и на некоторый период приостанавливается тарифный план; третье — и право пользования тарифным планом прекращается, а телефон изымается.

Конечно, добиваться выполнения этих правил нелегко, но в таком случае у правительства есть хоть какой-то рычаг воздействия в отличие от схемы с разовой выплатой компенсации. Впрочем, помимо использования полезных приложений и статусных телефонов

существуют другие способы сделать эту программу привлекательной. Бывшие солдаты, скорее всего, будут рассчитывать на материальные льготы или пенсии, чтобы обеспечивать свои семьи, поэтому увязать такие платежи с мобильным телефоном — разумный способ удержать их на правильном пути.

Однако для того чтобы проект «оружие в обмен на телефоны» заработал, он должен стать частью масштабной программы, поскольку одной раздачи телефонов недостаточно для интеграции в мирную жизнь тысяч бывших солдат. Следует предусмотреть возможность выплачивать ее участникам дополнительную денежную компенсацию или выдавать какие-то аксессуары к их телефонам в обмен на фотографии тайников с оружием или мест массового захоронения. Чтобы отказаться и от оружия, и от ощущения силы, которое оно дает, бывшие солдаты должны почувствовать уважительное отношение к себе и получить справедливую, по их мнению, компенсацию. Вернуться к мирной жизни таким людям помогут занятия по развитию определенных профессиональных навыков.

> В Колумбии очень успешно реализуется программа разоружения, демобилизации и реабилитации бывших партизан, в рамках которой создана большая сеть центров поддержки, предлагающих им образовательные, юридические и медицинские услуги. В отличие от многих аналогичных программ, правительство Колумбии сознательно размещает центры реабилитации в наиболее важных районах. Оно стремится вызвать максимальное доверие со стороны как участников боевых действий, так и общества. Такие центры устроены по принципу домов для сбежавших из дома подростков и в конечном счете становятся частью местного сообщества, поскольку к их работе постепенно подключаются жители района. Власти используют бывших партизан в качестве проводников идеи, что насилие не может помочь в решении проблем страны. Участники программы, выходцы из Революционных вооруженных сил Колумбии — террористической организации, созданной сорок восемь лет назад, — часто выступают в университетах и проводят круглые столы.

Однако пока неясно, ускорят коммуникационные технологии процесс примирения в обществе или замедлят его. С одной стороны, широкое распространение мобильных устройств поможет гражданам в ходе конфликта собрать доказательства нарушений, чтобы после его окончания могло восторжествовать правосудие. С другой — если будет

обнародовано огромное количество документов, зафиксировавших случаи насилия и страдания (к тому же способных храниться вечно и активно распространяться по сети), социальная или этническая группа, ставшая жертвой конфликта, может ожесточиться еще больше. Излечение общества, разорванного на части вооруженным конфликтом, — процесс достаточно болезненный, требующий в каком-то смысле коллективной «потери памяти». Чем больше свидетельств, тем больше придется прощать.

В будущем окажется возможным с помощью высоких технологий документально фиксировать и сохранять ход различных юридических процедур, в том числе репараций, люстраций (как в случае запрета занимать государственные посты членам иракской партии «Баас»), заседаний комиссий по установлению истины и примирению и даже судебных процессов. Это повысит прозрачность таких процедур и информированность общества в целом. В этом есть и плюсы, и минусы. Для многих иракцев телетрансляция суда над Саддамом Хусейном стала своего рода катарсисом, но при этом превратила скамью подсудимых в сцену, с которой диктатор и его сторонники могли обратиться к своей аудитории. Как говорит Найджел Сноад, бывший руководитель миссий ООН, ныне работающий в Google, «группам борцов за права человека и торжество правосудия стоит разработать информационную систему для фиксации своих воспоминаний и рассказов об убитых и пропавших без вести в ходе конфликта». И если затем свести воедино эти свидетельства и воспоминания «с обеих сторон, то, несмотря на противоречивые версии событий и эпизодические перепалки на форумах и в комментариях, возникнет пространство, где можно будет попросить прощения, рассказать правду и постепенно примириться с прошлым».

Медленный и болезненный процесс примирения с появлением интернета не изменится. Общество, выздоравливающее после конфликта, станет свидетелем публичного признания вины, приговоров, наказания и великодушных жестов прощения, и это станет сильнейшим психологическим потрясением. Привычные модели уголовного преследования на международном уровне за преступления против человечности работают слишком медленно, бюрократизированы и поощряют коррупцию. Десятки преступников

месяцами находятся в Международном уголовном суде (неофициально его называют «трибунал в Гааге»), прежде чем начнется рассмотрение их дела. В настоящее время после завершения конфликта предпочтительнее использовать местную судебную систему, чем неповоротливые международные институты.

Распространение технологий эту тенденцию, скорее всего, усилит. Благодаря огромному объему цифровых свидетельств преступлений и насильственных действий крепнут ожидания, что правосудие рано или поздно восторжествует, а черепашья скорость реакции таких международных органов, как Международный уголовный суд, не позволяет надеяться на их быструю адаптацию к происходящим изменениям. Трибунал в Гааге вряд ли когда-либо примет в качестве доказательств вины неверифицированные видеоролики, снятые мобильным телефоном (хотя такие организации, как Witness, и пытаются этого добиться). А вот местные суды, действующие более гибко и в условиях меньших ограничений, могут оказаться открытыми к последним достижениям технологии цифровых водяных знаков, которые позволяют провести успешную аутентификацию оригинальных материалов. И люди будут все больше отдавать предпочтение этим судебным органам.

Местный характер правосудия означает, что лицо, принимающее решение, будь то формальный судья, вождь племени или неформальный лидер общины, должен очень глубоко разбираться в ситуации и жить жизнью своего сообщества: чувствовать происходящие в нем процессы, знать главных героев и злодеев, понимать все то, в чем с таким трудом пытается разобраться далекий международный суд. Столкнувшись с цифровыми свидетельствами, такой человек не будет нуждаться в их верификации, поскольку и люди, и места, на них изображенные, ему хорошо знакомы. После завершения кризиса люди, как правило, очень хотят как можно быстрее воздать преступникам по заслугам. Неизвестно, будут ли местные суды справедливее международных, но что они будут действовать быстрее — это совершенно точно.

Эта тенденция проявится в будущих комиссиях по установлению истины и примирению — временных юридических структурах, возникших после завершения крупного конфликта.

После геноцида в Руанде новые власти страны отвергли использованную в ЮАР модель установления истины и примирения, заявив, что примирение возможно только после того, как будут наказаны виновные. Но у формальной судебной системы на осуждение предполагаемых организаторов геноцида ушло слишком много времени: более 100 тысяч жителей Руанды провели в заключении несколько лет, ожидая своей очереди предстать перед судом. Поэтому была создана новая система местных судов, основанная на традиционном способе разрешения конфликтов на уровне общины, который называется «гакака». В «гакакских» трибуналах обвиняемых судило местное сообщество, назначавшее им смягченное наказание в случае, если они признавали свою вину, откровенно рассказывали о случившемся или идентифицировали останки своих жертв. Несмотря на то что в основе «гакака» лежит «народное правосудие», это довольно сложная система многоступенчатого принятия решений. Первая ступень — так называемый «уровень первичной ячейки»: обвиняемый предстает перед трибуналом из представителей общины, где было совершено преступление. Этот трибунал определяет степень серьезности преступления и решает, где следует судить обвиняемого: в суде общины, района или провинции, — причем во всех трех случаях возможна апелляция. Система пока далека от совершенства. Ей присущи все традиционные культурные предрассудки, в том числе исключение женщин из числа судей и более мягкие наказания за преступления, совершенные против женщин. Но в остальном правосудие вершится быстро, и сообщество, как правило, удовлетворено его результатом. Поэтому правительствам других стран мира, столкнувшимся со схожими проблемами в посткризисной ситуации, стоит присмотреться к этой модели и адаптировать ее, учитывая, насколько успешно она решает задачу примирения.

Независимо от того, решат ли люди передать свои цифровые свидетельства в трибунал в Гааге или в местный суд, у них, конечно же, будет больше возможностей участвовать в переходном процессе, целью которого является отправление правосудия и примирение общества. Они смогут мгновенно загружать документы, фотографии и иные материалы, имеющие отношение к участникам конфликта или к бывшему репрессивному режиму, в международный «облачный» банк данных, информация в котором структурирована и распределена в соответствии с различными делами. Позднее эти свидетельства могут использовать судьи, журналисты и другие заинтересованные лица. Возможность сохранять воспоминания участников событий и помещать отзывы о них позволит людям выразить свою обиду организованно (например, используя алгоритмы агрегирования наиболее содержательных комментариев) и поддержит их уверенность

в том, что по окончании конфликта ничто не будет утрачено. Пользователи интернета смогут следить за ходом суда над наиболее крупными фигурами бывшего режима на экране своего мобильного телефона в режиме реального времени, в какой бы стране мира он ни проходил, и иметь под рукой всю информацию о любой стадии судебного процесса. Сохранение документальных свидетельств (как физических, так и виртуальных) о преступлениях павшего режима служит не только целям правосудия: если будут обнародованы все грязные секреты прежнего правительства, никогда больше власть не решится на подобные шаги. Политических экспертов часто беспокоит опасность скатывания государства назад, к авторитарному режиму, после завершения конфликта, и они внимательно следят за признаками такого поворота; предотвратить это поможет полное раскрытие информации о преступлениях прежнего режима: как именно преследовали диссидентов, как шпионили за населением в интернете, как выводили деньги из страны.

* * *

Из всех рассмотренных нами тем будущее возрождения страны, вероятно, внушает наибольший оптимизм. Мало что может сравниться по разрушительности с вооруженным конфликтом или стихийным бедствием, или и тем и другим одновременно, но мы видим четкую тенденцию: восстановление после кризиса происходит все быстрее и со все более удовлетворительными результатами. В отличие от других аспектов геополитики мир действительно учится на каждом примере восстановления, разбираясь, что работает, что нет, а что может быть улучшено. Разумное применение коммуникационных технологий и повсеместный доступ в сеть ускорят восстановление после кризиса, помогут информировать людей, дадут им больше полномочий и помогут сделать общество лучше, сильнее и жизнеспособнее. И все, что для этого нужно, — немного творчества, хорошие каналы связи и воля к инновациям.

Примечания к главе 7

Заключение

Охватывая взглядом все возможности и вызовы будущего, мы видим дивный новый мир, самый динамичный и волнующий период в истории человечества. За короткие сроки произойдет столько изменений, сколько не знало ни одно поколение людей. Их масштаб пока даже трудно оценить, отчасти благодаря устройствам, которые мы держим в руках.

В своей знаменитой книге «Эпоха одушевленных машин: когда интеллект компьютеров превзойдет человеческий», вышедшей в 1999 году, футурист Рэй Курцвейл[55] сформулировал новый «закон ускорения отдачи». Он пишет: «Технология — это продолжение эволюции другими средствами, следовательно, это эволюционный процесс». Для эволюции характерен экспоненциальный темп роста, при этом отдача вложений постоянно ускоряется. То же самое происходит и с компьютерными вычислениями, которые представляют собой основу любой известной нам сегодня технологии. Даже при наличии неизбежных ограничений закон Мура обещает нам всего через несколько лет бесконечно маленькие процессоры. Каждые два дня появляется столько цифрового контента, сколько было создано за весь период с момента возникновения цивилизации до 2003 года, а это около пяти эксабайтов[56] информации. При этом доступ в интернет пока имеют лишь два миллиарда человек из семи. Когда технологии распространятся по всей планете, сколько новых идей родится, сколько новых точек зрения будет озвучено, сколько новых творений создано и насколько быстрее мы сможем почувствовать их влияние на нас? Появление в виртуальном пространстве новых людей — благо и для них, и для нас. Коллективная выгода от обмена человеческим знанием и творческой энергией растет также экспоненциально.

Информационные технологии будут столь же повсеместны, как электричество. Они станут настолько обыденными, настолько проникнут в жизнь, что нашим детям будет трудно понять, как мы могли жить без них раньше. Поскольку благодаря интернету доступ в

мир технологий открывается миллиардам людей, любую проблему придется рассматривать и с учетом ее технологического аспекта, который придется учитывать правительствам, компаниям и обычным людям.

В долгосрочной перспективе любые попытки сдержать скорость распространения интернета или урезать его использование потерпят неудачу: информация, как вода, всегда найдет выход. Приспособиться к этим переменам и воспользоваться их следствиями постараются все: государства и их граждане, коммерческие и некоммерческие структуры, консультанты, террористы, инженеры, политики, хакеры. Но никто не сможет их контролировать.

Мы убеждены, что, получив доступ в сеть, выиграет большинство жителей нашей планеты: повысится эффективность, откроются новые возможности, вырастет качество жизни. Однако, хотя выгоды от наличия интернета получат практически все, опыт пользователей будет различным. Сложится своего рода сетевая кастовая система, и многое будет зависеть от того, какое место человек в ней занимает. На самом верху пирамиды крошечная группа пользователей сможет отгородиться от части негативных сторон технологической революции за счет высокого уровня доходов, уникальных возможностей доступа или географического положения. Средний класс станет двигателем перемен, ведь именно к нему относятся изобретатели, активные члены диаспор и владельцы малого и среднего бизнеса. Это те два миллиарда, у которых уже есть доступ в сеть.

Самые большие изменения затронут жизнь оставшихся пяти миллиардов человек (они вскоре тоже станут членами «сетевого клуба»). С одной стороны, они получат наибольшую выгоду от доступа к сети, с другой — столкнутся с самыми серьезными вызовами цифровой эпохи. Именно эти люди будут совершать революции и испытывать на прочность полицейские государства, но они же окажутся под колпаком своих правительств, на них будет обращена виртуальная ненависть экстремистских группировок, их будут дезориентировать в ходе информационных войн. Многие проблемы их мира сохранятся и после глобального распространения технологий.

* * *

Итак, что же мы знаем о нашем будущем мире?

Во-первых, понятно, что технологии как таковые не панацея от всех болезней современного общества, хотя их разумное использование может изменить мир к лучшему. Компьютеры и люди станут делить между собой все больше обязанностей в зависимости от того, у кого какие задачи получается лучше решать. Человеческий интеллект будет использоваться для выработки суждений, принятия интуитивных решений, анализа нюансов и уникального межличностного общения. Компьютерная мощь пригодится для хранения гигантских объемов информации, бесконечно быстрых вычислений и действий, недоступных нам в силу ограничений человеческой биологии. Компьютеры помогут нам анализировать огромные массивы данных, находить корреляцию и строить прогнозы, помогающие выследить террористов, но задача их задержания и наказания будет по-прежнему решаться людьми. Использование роботов благодаря их быстрой реакции позволит сохранять человеческие жизни непосредственно в бою, но для определения конкретных условий их применения и выработки плана их действий понадобится суждение человека.

Во-вторых, виртуальное пространство не изменит и не улучшит существующий мировой порядок. Скорее, приведет к усложнению практически всех его аспектов. Граждане и государства будут предпочитать тот мир, который, как им кажется, они больше контролируют: первые — виртуальный, вторые — реальный. Это противостояние просуществует столько же, сколько и сам интернет. Чтобы начать революцию, может оказаться достаточно горстки храбрецов, действующих в виртуальном пространстве. Однако жесткими мерами власти вполне способны подавить выступления на улицах. Сплотившись, меньшинство объявит об образовании виртуального государства, но, если что-то пойдет не так, как задумывалось, бунтари проиграют и в виртуальном, и в реальном мире.

В-третьих, государствам придется проводить по две внешние и две внутренние политики, по одной на каждый из миров, иногда противоречивые. Положим, какая-то страна организует кибератаку

против недруга, пойти войной на которого и мечтать не могла бы. Или давать возможность диссидентам выпустить пар в интернете и прочесывать городские улицы в поисках оппозиционеров, жестоко подавляя любые акции протеста. Или участвовать в виртуальных интервенциях, даже не собираясь отправлять людей (или роботов) в реальный бой.

И, наконец, благодаря распространению интернета и мобильных телефонов люди получат небывалую власть. Но за это придется платить, рискуя в первую очередь сохранением тайны частной жизни и ослаблением безопасности. Новые технологии дают возможность собирать и хранить много персональных сведений: о вашем прошлом, настоящем и будущем местонахождении, о просмотренной вами информации — и хранить так долго, как нужно для корректной работы программ. Такая информация никогда не была доступна прежде, и всегда существует опасность, что ее используют против вас. Все это будет регулироваться национальными законодательствами, но подходы к регулированию могут очень сильно отличаться, причем не только между демократическими или авторитарными странами, но и в рамках схожих политических систем. Вероятность утечки информации возрастает, и, несмотря на наличие механизмов защиты, хранить ее в тайне с течением времени станет все сложнее из-за человеческих ошибок и преступных действий. Ответственность за безопасность данных лежит на компаниях, организующих их хранение, и в этом смысле ничего не изменится. Однако пользователи также не должны беспечно относиться к защите своих персональных данных.

Чтобы не лишиться тайны частной жизни, нам нужно бороться, особенно в моменты национального кризиса, ведь после каждого страшного теракта «ястребы» настаивают на том, чтобы власти получали право на доступ ко все новой частной — или уже не частной — информации. В такой ситуации правительствам придется решать, где проходит черта, которую нельзя переступать. Функция распознавания лиц сделает жизнь безопаснее, позволит подтверждать личность гражданина в любой ситуации, от переписи до выборов, и ловить преступников. Но в то же время даст властям возможность усилить контроль над населением.

А что можно сказать о сохранении секретов, ведь это одинаково важно и для граждан, и для общественных институтов? Новые возможности для шифрования информации и распространения ее среди других людей вызовут и неожиданные проблемы. Скоро любая группа единомышленников — от преступников до диссидентов — сможет взять какие-то секретные материалы (возможно, программный код или конфиденциальные документы), зашифровать их, а затем разделить ключ от шифра на несколько фрагментов и раздать их всем членам группы. После этого они договорятся об условиях публикации этих материалов, то есть о том, в какой ситуации все должны соединить свои фрагменты и сделать материалы достоянием гласности. Такой ход может использоваться для давления или шантажа. И если в руки какой-то террористической группировки, например «Аль-Каиды», попадут некие секретные материалы (скажем, имена и адреса агентов ЦРУ, работающих под прикрытием), она может распространить их в зашифрованном виде среди своих членов, выдать им фрагменты ключа и пригрозить США обнародовать информацию в случае нападения на нее.

* * *

Мы хотим сказать, что в будущем нам придется иметь дело с историей уже двух цивилизаций: материальной, которая развивается тысячи лет, и виртуальной, только-только формирующейся. Они будут более-менее мирно сосуществовать, отчасти компенсируя недостатки друг друга. Виртуальный мир позволит активным гражданам избегать репрессий государства, объединяться и заниматься протестной деятельностью; остальные смогут просто бродить по сети, обучаться и развлекаться. В реальном мире будут устанавливаться правила и приниматься законы, призванные обуздать анархию мира виртуального и защитить людей от хакеров-террористов, дезинформации и спекулирования на их юношеских проступках. Вечное хранение виртуальных данных не позволит преступникам уничтожить улики против себя и отрицать вину, так что ответственность людей за свое поведение в реальном мире вырастет до небывалых высот.

Произойдет взаимовлияние виртуальной и материальной цивилизации, а баланс между ними определит, каким станет наш мир. С нашей точки зрения, этот мир, при всем его несовершенстве, окажется справедливее, прозрачнее и интереснее, чем можно себе представить. Как при заключении любого социального контракта, пользователи добровольно пожертвуют некоторыми вещами, которые ценят в реальном мире: приватностью, безопасностью, сохранностью персональных данных, — ради преимуществ, которые они получают, имея доступ в мир виртуальный. И наоборот, почувствовав вдруг, что кто-то посягает на эти преимущества, они примут все меры для того, чтобы призвать виновных к ответственности и изменить материальный мир.

Однако у нас есть повод для оптимизма. И это не перспективы, которые открывает обладание фантастическими устройствами и использование голографических проекций. Развитие технологий и доступ в интернет помогают бороться со злоупотреблениями, страданием и насилием. Когда готовность рисковать поддержана возможностями, человек может все. Лучшее, что все мы способны сделать для повышения качества жизни на планете, — это обеспечить людям доступ в сеть и предоставить им возможности технологий. Обеспечьте им доступ, и все остальное они сделают сами. Они уже знают, что им нужно и что они собираются строить, и найдут способ сделать это даже с помощью минимальных средств. Всем, кто стремится к экономическому процветанию, соблюдению прав человека, социальной справедливости, новым знаниям или самопознанию, стоит подумать над тем, как с помощью интернета не только достичь поставленных целей, но и продвинуться гораздо дальше. Мы не можем уничтожить неравенство и ненависть, однако, давая людям технологии, мы в состоянии изменить баланс сил в их пользу в надежде, что люди найдут им применение. Будет нелегко, но оно того стоит.

Примечания к заключению

Благодарности

Эта книга стала результатом почти трехлетнего сотрудничества, но ее появление было бы невозможно без щедрой помощи наших близких, друзей и коллег.

В первую очередь мы многим обязаны Софи Шмидт, которая в течение десяти месяцев была нашим «внутренним» редактором, критиком и соавтором. Одаренность, стратегическое мышление и аналитические способности Софи помогли воплотить наши идеи в жизнь. Софи, с ее глубоким пониманием и мира политики, и мира технологий, оказалась уникальным человеком, сумевшим увязать, с одной стороны, технические и геополитические темы, с другой — исторический анализ и футуристические описания и при этом сохранить требуемую научную строгость текста. А еще Софи сопровождала нас в поездках по многочисленным горячим точкам мира, о которых мы писали.

Мы хотим сказать большое спасибо Совету по международным отношениям, откуда летом 2000 года нам поступило первое предложение написать совместную статью в Foreign Affairs. Та статья навела нас на размышления, которые способствовали появлению этой книги. Отдельное спасибо
Ричарду Хаасу и другим руководителям Совета.

Мы благодарны нашему другу Скотту Малькомсону, который оказался незаменимым партнером и советчиком на ранних стадиях подготовки рукописи. Еще до того как мы пригласили Скотта поучаствовать в работе над этим проектом, мы восхищались его работой в качестве журналиста, эксперта по внешней политике и писателя. Благодаря его обширным познаниям, опыту анализа международной политической системы и пониманию разрушительных сторон технического прогресса он стал идеальным
редактором первых вариантов рукописи. Но больше всего благодарны за то, что за это время мы смогли подружиться с таким чудесным и ярким человеком.

Отдельное спасибо первым читателям рукописи Роберту Зоеллику, Анне-Мари Слаутер, Мичико Какутани, Алеку Россу и Иэну Бреммеру. Все они, несмотря на занятость, смогли выделить время для содержательного отзыва и профессиональной оценки.

Мы бы не написали эту книгу без помощи наших коллег-исследователей. Благодарим Кэйт Кронтирис: она помогла убедиться, что в основе наших смелых заявлений лежат надежные количественные данные. Хотим сказать спасибо Эндрю Лиму, проводившему исследования, которые оказались полезными для каждой главы. Мы поражены его способностью глубоко проанализировать тему практически за день. Большое спасибо Талии Бити, которая присоединилась к нам на завершающем этапе и очень помогла нам.

Мы хотим поблагодарить всех тех, с кем провели оказавшиеся бесценными личные беседы, особенно бывшего госсекретаря Генри Киссинджера, президента Руанды Поля Кагаме, премьер-министра Малайзии Мохда Наджиба Абдул Разака, бывшего президента Мексики Фелипе Кальдерона, саудовского принца аль-Валида бин Талала, командующего сухопутными войсками Пакистана Ашфака Парвеза Кайани, основателя WikiLeaks Джулиана Ассанжа, мексиканского бизнесмена Карлоса Слима Хелу, премьер-министра Туниса Хамади Джебали, бывшего руководителя DARPA, а ныне сотрудницу Google Регину Даган, старшего вице-президента Android Энди Рубина, главного аналитика Microsoft Крейга Манди, CEO Vodafone Витторио Колао, старшего партнера аналитической компании Brookings Питера Сингера, бывшего главу «Моссад» Меира Дагана, CEO отелей Taj Пракаша Шуклу и бывшего министра экономики Мексики Бруно Феррари.

На разных этапах работы над книгой нам давали ценные советы коллеги, друзья и родственники. Хотелось бы поблагодарить Пита Блаустейна, экономиста, восходящую звезду, чьи замечания оказались очень полезными; Джеффри Маклина за его бесценный стратегический анализ будущего войн и конфликтов; Тревора Томпсона, который помог нам представить будущие поля сражений, и Николаса Бергрюена — он одним из первых мотивировал нас написать эту книгу, а также читал первые ее версии.

Knopf — удивительное издательство, и оно заслужило свою репутацию. Его руководитель Сонни Мета подбадривал нас, побуждал ставить амбициозные задачи и написать книгу, которую читатели будут ждать с большим нетерпением. Знаменитый Джонатан Сигал вполне заслуживает свою репутацию, его креативность и прозорливость помогли сделать нашу рукопись значительно лучше. Спасибо Полу Богаардсу, Марии Мэсси и Эрину Хартману, вы настоящие профессионалы!

Наш агент Мел Паркер помог найти издателя, который разделял наши взгляды. Хотелось бы также поблагодарить многих сотрудников Google, которые делились с нами своими мыслями на разных стадиях работы над книгой. Постоянным источником вдохновения для нас были сооснователи Google Ларри Пейдж (также CEO компании) и Сергей Брин. Уточнить некоторые прогнозы помог менеджер по продуктам в Google Ideas и мечтатель Джастин Косслин. Лукас Диксон, партнер Google Ideas и блестящий инженер, вместе с нами проработал технические аспекты книги. Нам очень помогли беседы со многими действующими и бывшими членами команды Google: Си-Джей Адамсом, Ларри Элдером, Никеш Арора, Джейн Баек, Бренданом Баллоу, Энди Берндтом, Эриком Брюером, Шоной Браун, Скоттом Карпентером, Кристин Чен, Ди-Джеем Коллинзом, Ясмин Долатабади, Марком Элленбогеном, Эриком Гроссом, Джилл Хазелбакер, Шейн Хантли, Минни Ингерсол, Эми Ламберт, Энн Лавин, Эрезом Левином, Дамианом Менчером, Мисти Мускатель, Дэвидом Прессото, Скоттом Рубином, Найджелом Сноадом, Альфредом Спектором, Мэттью Степка, Астро Теллером, Сабастьяном Труном, Лоррейн Туохилл, Рэйчел Уэтстоун, Майком Виячеком, Сюзан Войкики и Эмили Вуд.

Очень многие в Google помогали нам с организацией поездок, необходимых для того, чтобы появилась эта книга: Дженифер Бартс, Кимберли Бердсэл, Гэвин Бишоп, Кимберли Купер, Даниэла Крокко, Доминик Каннингэм, Дэниел «Мистер Ди» Феер, Энн Хайят, Дэн Кейсерлинг, Марти Лев, Пэм Шор, Мануэл Темез и Брайан Томпсон.

Выражаем признательность за их идеи всем нашим друзьям и коллегам: Эллиоту Абрамсу, Рузанне Башир, Майклу Блумбергу, Ричарду Брэнсону, Крису Бросу, Джордану Брауну, Джеймсу Брайеру,

Майку Кляйну, Стиву Коллу, Питеру Диамандису, Ларри Даймонду, Джеку Дорси, Мохамеду Эль-Эриану, Джеймсу Фэллоусу, Саммер Феликс, Ричарду Фонтейну, Дову Фоксу, Тому Фрестону, Малкольму Гладуэллу, Джеймсу Глассману, Джеку Голдсмиту, Дэвиду Гордону, Шине Грейтенс, Крейгу Хэткофу, Майклу Хэйдену, Крису Хьюзу, Уолтеру Исааксону, Дину Камену, Дэвиду Кеннеди, Эрику Керру, Парагу Кханна, Джозефу Концелману, Стивену Краснеру, Рэю Курцвейлу, Эрику Ландеру, Джейсону Либману, Клаудии Мендоза, Евгению Морозову, Дамбисе Мойо, Элону Маску, Меган О’Салливан, Фарах Пандит, Барри Павелу, Стивену Пинкеру, Джо Полишу, Алексу Поллену, Джейсону Раковски, Лайсе Рэндалл, Кондолизе Райс, Джейн Розенталь, Ноуриель Рубини, Кори Шейк, Вэнсу Серчуку, Майклу Спенсу, Стивену Стедману, Дэну Твинингу, Декеру Уокеру, Мэтью Вакcману, Тиму Ву, Джиллиан Йорк, Хуану Зарате, Джонатану Зиттрейну и Этану Цукерману.

Мы хотели бы также поблагодарить парней из Peak Performance, особенно Джо Дудейла и Хосе и Эмили Гомесов, за то, что помогали нам сохранить форму на последних этапах работы над книгой.

А теперь — о самых близких.

От Джареда: особая благодарность Ребекке Коэн, которая, пока мы писали, превратилась из подруги в жену. Она была нашим интеллектуальным партнером и одним из наиболее ценных советчиков. Благодаря ее опыту и юридическим знаниям мы разобрались во множестве провокационных вопросов, которые в конечном счете стали важнейшими темами нескольких глав. Благодарю за родственную поддержку Ди и Дональда Коэнов, Эмили и Джеффа Нестлеров, Аннет и Пола Шапиро, Одри Беа и Аарона и Рэйчел Зубаты. Отдельно выражаю признательность моему дяде Алану Миркину, ветерану издательского дела, на чей совет всегда можно положиться.

От Эрика: бесконечная благодарность Венди Шмидт, которая привнесла человечность и смысл в жизнь сухого технического руководителя. Она способна удивительно органично соединить мир человека и мир технологий.

—Э. Ш., Д. К.,
январь 2013 г.

Об авторах

Эрик Шмидт — председатель совета директоров компании Google, в которую пришел в 2001 году. С 2001 по 2011 год был CEO Google и координировал техническую и бизнес-стратегию компании вместе с ее основателями Сергеем Брином и Ларри Пейджем. До этого работал председателем совета директоров и CEO Novell, а также техническим директором Sun Microsystems, Inc., аналитиком в Xerox Palo Alto Research Center (PARC), Bell Laboratories и Zilog. Член президентского совета по науке и технике, член научно-технического совета при премьер-министре Великобритании и пожизненный член Совета по международным отношениям. С 2006 года состоит в Национальной инженерной академии, с 2007 года — в Американской академии искусства и наук, возглавляет совет директоров фонда New America, а с 2008 года является попечителем Института перспективных исследований в Принстоне, штат Нью-Джерси.

Джаред Коэн — основатель и директор научного центра Google Ideas; стипендиат Родса Оксфордского университета; автор книг «Дети джихада» (Children of Jihad), «Сто дней тишины» (One Hundred Days of Silence) и статей в Foreign Affairs, Police Review, SAIS Review, Hoover Digest, The Washington Post и The International Herald Tribune. В 2006–2010 гг. был членом Комитета политического планирования госсекретаря США и ведущим советником Кондолизы Райс и Хиллари Клинтон, сейчас является членом Совета по международным отношениям, а также Консультативного совета при директоре Национального центра по борьбе с терроризмом.

Примечания

Введение

Интернет относится к тем изобретениям…
Несколько измененная цитата из выступления Эрика Шмидта на конференции JavaOne в Сан-Франциско в апреле 1997 г. В оригинале звучала так: «Интернет — это первая вещь, которую человечество создало, но до конца не успело понять; это крупнейший анархический эксперимент в истории». Мы изменили фразу в соответствии с нашим мнением, что это не первое, но одно из немногих таких изобретений наряду с ядерным оружием, паровым двигателем и электричеством.

впервые любой из нас…
К технологическим революциям относится появление книгопечатного пресса, телеграфа, радио, телевидения и факсимильного аппарата; но всем им был нужен посредник.

350 миллионов…
См. данные для 2000 г. в Estimated Internet Users (World) and Percentage Growth, ITU World Telecommunication Indicators (2001), referred to by Claudia Sarrocco and Dr. Tim Kelly, Improving IP Connectivity in the Least Developed Countries, International Telecommunication Union (ITU), Strategy and Policy Unit, 9, ссылка по состоянию на 23 октября 2012 г. http://www.itu.int/osg/spu/ni/ipdc/study/Improving%20IP%20Connectivity%20in%20the%20Least%20Developed%20Countries1.pdf.

превысив два миллиарда…
См. данные для 2010 г. в Global Numbers of Individuals Using the Internet, Total and Per 100 Inhabitants, 2001–2011, International Telecommunication Union (ITU), ICT Data and Statistics (IDS), ссылка по состоянию на 8 октября 2012 г. http://www.itu.int/ITU-D/ict/statistics/.

с 750 миллионов до более чем пяти миллиардов…

См. итоги для 2000 и 2010 гг. в Mobile-Cellular Telephone Subscriptions, International Telecommunication Union (ITU), ICT Data and Statistics (IDS), ссылка по состоянию на 8 октября 2012 г. http://www.itu.int/ITU-D/ict/statistics/.

большинство из восьми миллиардов землян…
См. итог для населения обоих полов в World Midyear Population by Age and Sex for 2025, U.S. Census Bureau, International Data Base, ссылка по состоянию на 8 октября 2012 г. http://www.census.gov/population/international/data/idb/worldpop.php.

многим традиционным институтам…
Мы уже некоторое время обсуждали эту концепцию, но к такому пониманию пришли только после разговора с нашим другом Алеком Россом. Он заслуживает славы ее соавтора. См. Alec Ross. How Connective Tech Boosts Political Change // CNN, 20 июня 2012 г., http://www.cnn.com/2012/06/20/opinion/opinion-alec-ross-tech-politics/index.html.

запрещал использование мобильных телефонов…
Better than Freedom? Why Iraqis Cherish Their Mobile Phones // Economist, 12 ноября 2009 г., http://www.economist.com/node/14870118.

с перебоями в снабжении продуктами, водой и электричеством…
Iraq: Key Facts and Figures // BBC, 7 сентября 2010 г., http://www.bbc.co.uk/news/world-middle-east-11095920.

мусор не убирался годами…
Zaineb Naji and Dawood Salman. Baghdad’s Trash Piles Up // Environmental News Service, 6 июля 2010 г., http://www.ens-newswire.com/ens/jul2010/2010-07-06-01.html.

Назад к тексту

Глава 1. Наше будущее «я»

пять с лишним миллиардов человек…
The World in 2011: ICT Facts and Figures // International Telecommunication Union (ITU), ссылка по состоянию на 10 октября 2012 г., http://www.itu.int/ITUD/ict/facts/2011/material/ICTFactsFigures2011.pdf.
Из этого источника следует, что в 2011 г. доступ к интернету имели 35% жителей Земли. Мы учли прогнозные темпы роста населения планеты и оценили количество человек, которые присоединятся к виртуальному миру, в 5 миллиардов.

как сегодня влияет на жизнь…
Придумала пример с рыбачками Ребекка Коэн, мы только местом действия определили Конго.

В Африке уже 650 млн абонентов сотовой связи…
Africa's Mobile Phone Industry 'Booming' // BBC, 9 ноября 2011 г., http://www.bbc.co.uk/news/world-africa-15659983.

в Азии — около 3 млрд…
См. количество абонентов сотовой связи в Азии и Тихоокеанском регионе в 2011 г. в Key ICT Indicators for the ITU/BDT Regions (Totals and Penetration Rates) // International Telecommunication Union (ITU), ICT Data and Statistics (IDS), версия от 16 ноября 2011 г., http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html.

Большинство этих людей пользуются лишь базовыми функциями телефонов…
Там же. Сравните количество абонентов сотовой связи с количеством пользователей мобильного широкополосного доступа для 2011 г.

продолжительность жизни не превышает 60, а в некоторых местах — и 50 лет…

Country Comparison: Life Expectancy at Birth // CIA, World Fact Book, ссылка по состоянию на 11 октября 2012 г., https://www.cia.gov/library/publications/the-world-factbook/rankorder/2102rank.html#top.

Это касается даже…
Один из авторов провел лето 2001 г. в этой далекой деревне, где не было электричества, проточной воды, мобильных и обычных телефонов. Вернувшись туда осенью 2010 г., он заметил красивые вышитые бисером чехлы, в которых женщины масаи хранили свои мобильные телефоны.

обширной китайской «шанжай»…
Nicholas Schmidle. Inside the KnockoffTennis-Shoe Factory // New York Times Magazine, Global edition, 19 августа 2010 г., http://www.nytimes.com/2010/08/22/magazine/22fake-t.html?pagewanted=all.

принтеры способны фактически «распечатывать» физические объекты…
The Printed World: Three-Dimensional Printing from Digital Designs Will Transform Manufacturing and Allow More People to Start Making Things // Economist, 10 февраля 2011 г., http://www.economist.com/node/8114221.

копии мотоциклов в натуральную величину…
Patrick Collinson. Hi-Tech Shares Take US for a Walk on the High Side // Guardian (Manchester), 16 марта 2012 г., http://www.guardian.co.uk/money/2012/mar/16/hi-tech-shares-us.

«общительных роботов», способных распознавать человеческие жесты…
Sarah Constantin. Gesture Notes to Pages 18–26 265 Recognition, Mind-Reading Machines, and Social Robotics // H+ Magazine, 8 февраля 2011 г., http://hplusmagazine.com/2011/02/08/gesture-recognition-mind-reading-machines-and-social-robotics/.

В 2012 году японская команда исследователей одной из лабораторий роботостроения…
Helen Thomson. Robot Avatar Body Controlled by Thought Alone // New Scientist, июль 2012 г., 19–20.

Двадцатичетырехлетний кениец Энтони Мутуа…
Shoe Technology to Charge Cell Phones // Daily Nation, May 2012, http://www.nation.co.ke/News/Shoe+technology+to+charge+cell+phones++/-/1056/1401998/-/view/printVersion/-/sur34lz/-/index.html.

поместил чип в подошву своего ботинка…
Там же.

Чип, изобретенный Мутуа, вот-вот начнут производить серийно…
Там же.

Khan Academy…
В качестве раскрытия информации: Эрик Шмидт входит в совет директоров Khan Academy.

заменив лекции видеороликами…
Clive Thompson. How Khan Academy Is Changing the Rules of Education // Wired Magazine, August 2011, размещено в интернете 15 июля 2011 г., http://www.wired.com/magazine/2011/07/ff_khan/.

В 2012 году этот подход протестировал в Эфиопии Массачусетский технологический институт…
Nicholas Negroponte. EmTech Preview: Another Way to Think About Learning // Technology Review, 13 сентября 2012 г., http://www.technologyreview.com/view/429206/emtech-preview-another-way-to-think-about/.

раздавали планшеты с загруженным в них контентом…
David Talbot. Given Tablets but No Teachers, Ethiopian Children Teach Themselves // Technology Review, 29 октября 2012

г., http://www.technologyreview.com/news/506466/given-tablets-but-no-teachers-ethiopian-children-teach-themselves/.

уровень грамотности один из самых низких в мире…
Field Listing: Literacy // CIA, World Fact Book, ссылка по состоянию на 11 октября 2012 г., https://www.cia.gov/library/publications/the-world-factbook/fields/2103.html#af.

в 2012 году в штате Невада стали выдавать лицензии на беспилотные автомобили…
Chris Gaylord. Ready for a Self-Driving Car? Check Your Driveway // Christian Science Monitor, 25 июня 2012 г., http://www.csmonitor.com/Innovation/Tech/2012/0625/Ready-for-a-self-driving-car-Check-your-driveway.

законность их использования была подтверждена в Калифорнии…
James Temple. California Affirms Legality of Driverless Cars // The Tech Chronicles (blog), San Francisco Chronicle, 25 сентября 2012 г., http://blog.sfgate.com/techchron/2012/09/25/california-legalizes-driverless-cars/; Флорида приняла аналогичный закон, см. Joann Muller. With Driverless Cars, Once Again It Is California Leading the Way // Forbes, 26 сентября 2012 г., http://www.forbes.com/sites/joannmuller/2012/09/26/with-driverless-cars-once-again-it-is-california-leading-the-way/.

в 2012 году Управление по контролю за продуктами и лекарствами США одобрило первую электронную таблетку…
Erin Kim. ‘Digital Pill’ with Chip Inside Gets FDA Green Light // CNN Money, 3 августа 2012 г., http://money.cnn.com/2012/08/03/technology/startups/ingestible-sensor-proteus/index.htm; Peter Murray. No More Skipping Your Medicine — FDA Approves First Digital Pill // Forbes, 9 августа 2012 г., http://www.forbes.com/sites/singularity/2012/08/09/no-more-skipping-your-medicine-fda-approves-first-digital-pill/.

содержит микроскопический датчик размером один квадратный миллиметр…
Там же.

активизации электрической цепи желудочным соком…
Daniel Cressey. Say Hello to Intelligent Pills: Digital System Tracks Patients from the Inside Out // Nature, 17 января 2012 г., http://www.nature.com/news/say-hello-to-intelligent-pills-1.9823; Randi Martin, 266, примечания к с. 26–30 FDA Approves ‘Intelligent’ Pill That Reports Back to Doctors // WTOP, 2 августа 2012 г., http://www.wtop.com/267/2974694/FDA-approves-intelligent-pill-that-reports-back-to-doctors.

приемник может собирать информацию…
Cressey. Say Hello to Intelligent Pills // Nature, 17 января 2012 г. и Martin. FDA Approves ‘Intelligent’ Pill // WTOP, 2 августа 2012 г.

следить за тем, что человек ест…
Randi Martin. FDA Approves ‘Intelligent’ Pill That Reports Back to Doctors // WTOP, 2 августа 2012 г.

Специалисты по тканям смогут выращивать новые органы…
Henry Fountain. One Day, Growing Spare Parts Inside the Body // New York Times, 17 сентября 2012 г., http://www.nytimes.com/2012/09/18/health/research/using-the-body-to-incubate-replacement-organs.html?pagewanted=all; Henry Fountain. A First: Organs Tailor-Made with Body’s Own Cells // New York Times, 15 сентября 2012 г., http://www.nytimes.com/2012/09/16/health/research/scientists-make-progress-in-tailor-made-organs.html?pagewanted=all; Henry Fountain. Synthetic Windpipe Is Used to Replace Cancerous One // New York Times, 12 января 2012 г., http://www.nytimes.com/2012/01/13/health/research/surgeons-transplant-synthetic-trachea-in-baltimore-man.html.

врачи смогут узнать о пациенте…

Gina Kolata. Infant DNA Tests Speed Diagnosis of Rare Diseases // New York Times, 3 октября 2012 г., http://www.nytimes.com/2012/10/04/health/new-test-of-babies-dna-speeds-diagnosis.html?_r=1; Gina Kolata. Genome Detectives Solve a Hospital's Deadly Outbreak // New York Times, 22 августа 2012 г., http://www.nytimes.com/2012/08/23/health/genome-detectives-solve-mystery-of-hospitals-k-pneumoniae-outbreak.html; Gina Kolata. A New Treatment's Tantalizing Promise Brings Heartbreaking Ups and Downs // New York Times, 8 июля 2012 г., http://www.nytimes.com/2012/07/09/health/new-frontiers-of-cancer-treatment-bring-breathtaking-swings.html.

благодаря успехам фармакогенетики…
One Size Does Not Fit All: The Promise of Pharmacogenomics // National Center for Biotechnology Information, Science Primer, версия от 31 марта 2004 г., http://www.ncbi.nlm.nih.gov/About/primer/pharm.html.

революция «мобильного здоровья»…
mHealth in the Developing World // m+Health, ссылка по состоянию на 23 октября 2012 г., http://mplushealth.com/en/SiteRoot/MHme/Overview/mHealth-in-the-Developing-World/.

Сегодня с помощью мобильных телефонов…
Lakshminarayanan Subramanian et al.. SmartTrack // CATER (Cost-effective Appropriate Technologies for Emerging Region), New York University, ссылка по состоянию на 11 октября 2012 г., http://cater.cs.nyu.edu/smarttrack#ref3.

вроде рентгеновских, но с меньшим уровнем радиации…
Kevin Spak. Coming Soon: X-Ray Phones // Newser, 20 апреля 2012 г., http://www.newser.com/story/144464/coming-soon-x-ray-phones.html.

собака не может съесть «облачное» хранилище файлов…
Похожую идею выразил нью-йоркский художник Том Чини в 2012 г. На одном из его рисунков школьник оправдывается перед

учительницей: «Мою домашнюю работу съело облако». См. Cartoons from the Issue // New Yorker, 8 октября 2012 г., http://www.newyorker.com/humor/issuecartoons/2012/10/08/cartoons_20121001#slide=5.

Назад к тексту

Глава 2. Будущее личности, государства и персональных данных

у людей может усилиться психологическая склонность искать подтверждение своей позиции…
Эли Парисер в своей книге «Пузырь фильтрации: что от вас скрывает интернет» (The Filter Bubble: What the Internet Is Hiding from You. New York: Penguin Press, 2011) называет это «пузырем фильтрации».

недавнее исследование ученых из Университета штата Огайо…
R. Kelly Garrett and Paul Resnick. Resisting Political Fragmentation on the Internet // Daedalus 140, no. 4 (осень 2011 г.): 108–120, doi:10.1162/DAED_a_00118.

популярные в определенных этнических группах имена…
Steven D. Levitt and Stephen J. Dubner, Freakonomics: A Rogue Economist Explores the Hidden Side of Everything (New York: William Morrow, 2005). Это исследование показывает, что имена не являются причиной успеха или неудач детей, но все же представляют собой некоторые факторы (в частности, социально-экономические), способные влиять на шансы ребенка. См. Steven D. Levitt and Stephen J. Dubner. A Roshanda by Any Other Name // Slate, 11 апреля 2005 г., http://www.slate.com/articles/business/the_dismal_science/2005/04/a_roshanda_by_any_other_name.single.html.

несколько банкиров с Уолл-стрит привлекали…
Nick Bilton. Erasing the Digital Past // New York Times, 1 апреля 2011 г., http://www.nytimes.com/2011/04/03/fashion/03reputation.html?pagewanted=all.

Ассанж поделился с нами двумя своими главными соображениями…
Джулиан Ассанж, из беседы с авторами, июнь 2011 г.

«детонатором» (так называет себя Ассанж)…

Atika Shubert. WikiLeaks Editor Julian Assange Dismisses Reports of Internal Strife // CNN, 22 октября 2010 г., http://articles.cnn.com/2010-10-22/us/wikileaks.interview_1_julian-assange-wikileaks-afghan-war-diary?_s=PM:US.

Информаторы голосуют ногами…
Джулиан Ассанж, из беседы с авторами, июнь 2011 г.

утратила контроль над своим основным сайтом…
James Cowie. WikiLeaks: Moving Target // Renesys (блог), 7 декабря 2010 г., http://www.renesys.com/blog/2010/12/wikileaks-moving-target.shtml.

зеркальных сайтов…
Ravi Somaiya. Pro-Wikileaks Activists Abandon Amazon Cyber Attack // BBC, 9 декабря 2010 г., http://www.bbc.com/news/technology-11957367.

Алексея Навального, блогера и борца с коррупцией из России…
Matthew Kaminski. The Man Vladimir Putin Fears Most // Wall Street Journal, 3 марта 2012 г., http://online.wsj.com/article/SB10001424052970203986604577257321601811092.html; Russia Faces to Watch: Alexei Navalny // BBC, 12 июня 2012 г., http://www.bbc.co.uk/news/world-europe-18408297.

пожертвования на ведение ее операционной деятельности посредством PayPal…
Tom Parfitt. Alexei Navalny: Russia's New Rebel Who Has Vladimir Putin in His Sights // Guardian (Manchester), 15 января 2012 г., http://www.guardian.co.uk/theguardian/2012/jan/15/alexei-navalny-profile-vladimir-putin.

обнародования им в 2010 году документов…
Russia Checks Claims of $4bn Oil Pipeline Scam // BBC, 17 ноября 2010 г., http://www.bbc.co.uk/news/world-europe-11779154.

Партия жуликов и воров…

Tom Parfitt. Russian Opposition Activist Alexei Navalny Fined for Suggesting United Russia Member Was Thief // Telegraph (London), 5 июня 2012 г., http://www.telegraph.co.uk/news/worldnews/europe/russia/9312508/Russian-opposition-activist-Alexei-Navalny-fined-for-suggesting-United-Russia-member-was-thief.html; Stephen Ennis. Profile: Russian Blogger Alexei Navalny // BBC, 7 августа 2012 г., http://www.bbc.co.uk/news/world-europe-16057045.

задерживали, помещали под арест, устраивали за ним слежку, возбуждали уголовные дела…
Ellen Barry. Rousing Russia with a Phrase // New York Times, 9 декабря 2011 г., http://www.nytimes.com/2011/12/10/world/europe/the-saturday-profile-blogger-aleksei-navalny-rouses-russia.html. Robert Beckhusen. Kremlin Wiretaps Dissident Blogger—Who Tweets the Bug // Danger Room (blog), Wired, 8 августа 2012 г., http://www.wired.com/dangerroom/2012/08/navalny-wiretap/. Navalny Charged with Embezzlement, Faces up to 10 Years // RT (Moscow), версия от 1 августа 2012 г., http://rt.com/politics/navalny-charged-travel-ban-476/.

знают о нем в стране…
Parfitt. Alexei Navalny: Russia's New Rebel Who Has Vladimir Putin in His Sights // http://www.guardian.co.uk/theguardian/2012/jan/15/alexei-navalny-profile-vladimir-putin.

запрещено показывать на федеральных телеканалах…
Kaminski. The Man Vladimir Putin Fears Most, http://online.wsj.com/article/SB10001424052970203986604577257321601811092.html.

Михаила Ходорковского…
Mikhail Khodorkovsky // New York Times, версия от 8 августа 2012 г., http://topics.nytimes.com/top/reference/timestopics/people/k/mikhail_b_khodorkovsky/index.html; Andrew E. Kramer. Amid Political Prosecutions, Russian Court Issues Ruling Favorable to Oil Tycoon // New York Times, 1 августа 2012 г., http://www.nytimes.com/2012/08/02/world/europe/russian-court-issues-favorable-ruling-to-oil-tycoon.html. На момент выхода этой

книги Ходорковский остается в тюрьме. Ходят слухи, что президент Владимир Путин может сократить его 13-летний срок.

Бориса Березовского…
Svetlana Kalmykova. Oligarch Berezovsky Faces New Charges // Voice of Russia (Moscow), 29 мая 2012 г., http://english.ruvr.ru/2012_05_29/76399306/.

плохо смонтированной фотографии…
Russian Blogger Navalny Unmasks 'Kremlin' Photo Smear // BBC, 10 января 2012 г., http://www.bbc.co.uk/news/world-europe-16487469.

официальные обвинения в злоупотреблениях…
Ellen Barry. Russia Charges Anticorruption Activist in Plan to Steal Timber // New York Times, 31 июля 2012 г., http://www.nytimes.com/2012/08/01/world/europe/aleksei-navalny-charged-with-embezzlement.html.

Эти обвинения в преступлении, максимальное наказание за которое…
Там же.

персональные данные 150 тысяч пользователей Sony, украденные хакерской группровкой LulzSec…
Mathew J. Schwartz. Sony Hacked Again, 1 Million Passwords Exposed // InformationWeek, 3 июня 2011 г., http://www.informationweek.com/security/attacks/sony-hacked-again-1-million-passwords-ex/229900111.

Ассанж сказал нам, что на самом деле редактирует материалы лишь для того, чтобы снизить международное давление на организацию…
Джулиан Ассанж, из беседы с авторами, июнь 2011 г.

«нулевую терпимость»…
Charlie Savage. Holder Directs U.S. Attorneys to Track Down Paths of Leaks // New York Times, 8 июня 2012 г., http://www.nytimes.com/2012/06/09/us/politics/holder-directs-us-attorneys-to-investigate-leaks.html?pagewanted=all.

твитов, в которых он в режиме реального времени сообщил об операции по уничтожению…

Reed Stevenson, Reuters. Sohaib Athar Captures Osama bin Laden Raid on Twitter // Huffington Post, дата первой публикации 2 мая 2011 г., версия от 2 июля 2011 г., http://www.huffingtonpost.com/2011/05/02/osama-bin-laden-raid-twitter-sohaib-athar_n_856187.html.

Вот один из твитов…
Там же; твиты Сохаиба Атара, 1 мая 2011 г., 00:58, https://twitter.com/ReallyVirtual/status/64780730286358528. (Пять твитов Сохаиба Атара, размещенных в ночь операции по ликвидации бен Ладена: 1) «Над Абботтабадом в 1 ночи летает вертолет (такое нечасто бывает)» (его первый твит на эту тему); 2) «Улетай, вертолет, пока я не достал свою гигантскую мухобойку :-/»; 3) «Сильный взрыв в Абботтабаде, звенят стекла, надеюсь, ничего страшного не начнется:-S»; 4) «@m0hcin один из немногих, кто не спит, говорит, что один из вертолетов не пакистанский...»; 5) «Раз у талибов нет вертолетов (вероятно) и говорят, что он “не наш”, должно быть, в #abbottabad непростая ситуация».) См. Rik Myslewski. Pakistani IT Admin Leaks bin Laden Raid on Twitter // Register, 2 мая 2011 г., http://www.theregister.co.uk/2011/05/02/bin_laden_raid_tweeted/.

доступ в сеть там, где сегодня отсутствуют свободные СМИ, затруднен…
Обратите внимание на низкие значения проникновения мобильной связи в нижней части списка стран, отсортированного по убыванию индекса свободы прессы, у таких государств, как Эритрея и Северная Корея, в Mobile-Cellular Telephone Subscriptions Per 100 Inhabitants // International Telecommunication Union (ITU), ICT Data and Statistics (IDS), ссылка по состоянию на 15 октября 2012 г., http://www.itu.int/ITUD/ict/statistics/ и Press Freedom Index 2011/2012 // Reporters Without Borders (RSF), ссылка по состоянию на 15 октября 2012 г. http://en.rsf.org/press-freedom-index-2011-2012,1043.html.

полевых командиров из Восточного Конго…
ICC/DRC: Second Trial of Congolese Warlords // Human Rights Watch, News, 23 ноября 2009 г., http://www.hrw.org/news/2009/11/23/iccdrc-second-trial-congolese-warlords; Marlise Simons. International Criminal Court Issues First Sentence // New York Times, 10 июля 2012

г., http://www.nytimes.com/2012/07/11/world/europe/international-criminal-court-issues-first-sentence.html.

законом «О переписке президента»…
Presidential Records Act (PR A) of 1978 // National Archives, Presidential Libraries, Laws and Regulations, ссылка по состоянию на 12 октября 2012 г. http://www.archives.gov/presidential-libraries/laws/1978-act.html; Presidential Records // National Archives, Basic Laws and Authorities, ссылка по состоянию на 12 октября 2012 г. http://www.archives.gov/about/laws/presidential-records.html.

Хамза Кашгари разместил в твиттере воображаемый диалог с пророком Мухаммедом…
Mike Giglio. Saudi Writer Hamza Kashgari Detained in Malaysia over Muhammad Tweets // Daily Beast, 10 февраля 2012 г., http://www.thedailybeast.com/articles/2012/02/08/twitter-aflame-with-fatwa-against-saudi-writer-hamza-kashgari.html.

Через шесть часов после публикации Кашгари удалил твиты…
Asma Alsharif and Amena Bakr. Saudi Writer May Face Trial over Prophet Mohammad // Reuters, 13 февраля 2012 г., http://www.reuters.com/article/2012/02/13/us-saudi-blogger-idUSTRE81C13720120213.

создании группы в Facebook…
Liz Gooch and J. David Goodman. Malaysia Detains Saudi over Twitter Posts on Prophet // New York Times, 10 февраля 2012 г., http://www.nytimes.com/2012/02/11/world/asia/malaysia-detains-saudi-over-twitter-posts-on-prophet.html.

Он бежал в Малайзию, но спустя три дня был депортирован…
Ellen Knickmeyer. Saudi Tweeter Is Arrested in Malaysia // Wall Street Journal, 10 февраля 2012 г., http://online.wsj.com/article/SB10001424052970204626045772135536 13859184.html;

Nadim Kawach. Malaysia Deports Saudi over Twitter Posts // Emirates 24/7, 11 февраля 2012 г., http://www.emirates247.com/news/region/malaysia-deports-saudi-over-twitter-posts-2012-02-11-1.442363.

обвинение в богохульстве…
Saudi Writer Kashgari Deported // Freedom House, News and Updates, ссылка по состоянию на 12 октября 2012 г. http://www.freedomhouse.org/article/saudi-writer-kashgari-deported;
Saudi Arabia: Writer Faces Apostasy Trial // Human Rights Watch (HRW), News, 13 февраля 2012 г., http://www.hrw.org/news/2012/02/13/saudi-arabia-writer-faces-apostasy-trial.

извинился сразу, а потом еще раз в августе 2012 года…
Laura Bashraheel. Hamza Kashgari's Poem from Prison // Saudi Gazette (Jeddah), версия от 21 августа 2012 г., http://www.saudigazette.com.sa/index.cfm?method=home.regcon&contentid=20120821133653.

была убита известная актриса…
The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record», Electronic Privacy Information Center, ссылка по состоянию на 13 октября 2012 г. http://epic.org/privacy/drivers/.

обнародования сведений о том, какие видеофильмы брал в прокате покойный судья Роберт Борк…
Existing Federal Privacy Laws», Center for Democracy and Technology, ссылка по состоянию на 13 октября 2012 г. https://www.cdt.org/privacy/guide/protect/laws.php#vpp.

закон был применен в Техасе…
Harris v. Blockbuster // Electronic Privacy Information Center, ссылка по состоянию на 13 октября 2012 г. http://epic.org/amicus/blockbuster/default.html;
Cathryn Elaine Harris, Mario Herrera, and Maryam Hosseiny v. Blockbuster, Inc., Settlement, District Court for the Northern District of

Texas Dallas Division, Civil Action No. 3:09-cv-217-M, http://www.scribd.com/doc/28540910/Lane-v-Facebook-Blockbuster-Settlement.

участники сирийской оппозиции и сотрудники международных неправительственных организаций…
Ben Brumfield. Computer Spyware Is Newest Weapon in Syrian Conflict // CNN, 17 февраля 2012 г. http://articles.cnn.com/2012-02-17/tech/tech_web_computer-virus-syria_1_opposition-activists-computer-viruses-syrian-town?_s=PM:TECH.

Иностранные специалисты-компьютерщики…
Там же.

Одна сотрудница неправительственной организации загрузила такой файл…
Там же.

крушение высокоскоростного поезда…
China Train Crash: Signal Design Flaw Blamed // BBC, 28 июля 2011 г., http://www.bbc.co.uk/news/world-asia-pacific-14321060.

сообщений в «Вейбос»…
Michael Wines and Sharon LaFraniere. In Baring Facts of Train Crash, Blogs Erode China Censorship // New York Times, 28 июля 2011 г., http://www.nytimes.com/2011/07/29/world/asia/29china.html?pagewanted=all.

просчеты в проекте…
Sharon LaFraniere. Design Flaws Cited in Deadly Train Crash in China // New York Times, 28 декабря 2011 г., http://www.nytimes.com/2011/12/29/world/asia/design-flaws-cited-in-china-train-crash.html;
China Bullet Train Crash ‘Caused by Design Flaws’ // BBC, 28 декабря 2011 г., http://www.bbc.co.uk/news/world-asia-china-16345592.

вскоре после аварии власти разослали в СМИ специальные директивы…
David Bandurski. History of High-Speed Propaganda Tells All // China Media Project, 25 июля 2011 г., http://cmp.hku.hk/2011/07/25/14036/?utm_source=twitterfeed&utm_medium=twitter.

В Сомали, например, телекоммуникационные компании…
Abdinasir Mohamed and Sarah Childress. Telecom Firms Thrive in Somalia Despite War, Shattered Economy // Wall Street Journal, 11 мая 2010 г., http://online.wsj.com/article/SB10001424052748704608104575220570113266984.html.

правонарушения в киберпространстве трактовались как «посягательство на движимое имущество»…
Eric J. Sinrod. Perspective: A Cyberspace Update for Hoary Legal Doctrine // CNET, 4 апреля 2007 г., http://news.cnet.com/A-cyberspace-update-for-hoary-legal-doctrine/2010-1030_3-6172900.html.

использованию мобильных платформ и традиционной для арабских стран системы перевода денежных средств «хавала»…
Andrew Quinn. Cell Phones May Be New Tool vs. Somalia Famine // Reuters, 21 сентября 2011 г., Africa edition, http://af.reuters.com/article/topNews/idAFJOE78K00L20110921.

появились новые возможности…
Sahra Abdi. Mobile Transfers Save Money and Lives in Somalia // Reuters, 3 марта 2010 г., http://www.reuters.com/article/2010/03/03/us-somalia-mobiles-idUSTRE6222BY20100303.

мобильная связь намного более широко распространена, чем компьютеры и доступ в интернет…
Сравните количество абонентов сотовой связи и пользователей интернета в 2010 г. в таких странах, как Экваториальная Гвинея, Мали, Нигер и т. д. в Mobile-Cellular Subscriptions и Fixed (Wired) Internet Subscriptions // International Telecommunication Union (ITU), ICT Data

and Statistics (IDS), ссылка по состоянию на 13 октября 2012 г. http://www.itu.int/ITU-D/ict/statistics/.

многие используют мобильные телефоны как стереосистемы…
Michael Byrne. Inside the Cell Phone File Sharing Networks of Western Africa (Q+A) // Motherboard, 3 января 2012 г., http://motherboard.vice.com/2012/1/3/inside-the-cell-phone-file-sharing-networks-of-western-africa-q-a.

Более интересные возможности…
Dena Cassella. What Is Augmented Reality (AR): Augmented Reality Defined, iPhone Augmented Reality Apps and Games and More // Digital Trends, 3 ноября 2009 г., http://www.digitaltrends.com/mobile/what-is-augmented-reality-iphone-apps-games-flash-yelp-android-ar-software-and-more/.

Project Glass…
Babak Parviz, Steve Lee, Sebastian Thrun. Project Glass // Google, 4 апреля 2012 г., https://plus.google.com/+projectglass/posts;
Nick Bilton. Google Begins Testing Its Augmented-Reality Glasses // Bits (blog), New York Times, 4 апреля 2012 г., http://bits.blogs.nytimes.com/2012/04/04/google-begins-testing-its-augmented-reality-glasses/.

аналогичные устройства разрабатываются и другими компаниями…
Todd Wasserman. Apple Patent Hints at Google Glass Competitor // Mashable, 5 июля 2012 г., http://mashable.com/2012/07/05/apple-patent-google-glass/;
Molly McHugh. Google Glasses Are Just the Beginning: Why Wearable Computing Is the Future // Digital Trends, 6 июля 2012 г., http://www.digitaltrends.com/computing/google-glasses-are-just-the-beginning-why-wearable-computing-is-the-future/#ixzz29PI4PWK4.

принятия законов, обязывающих операторов…
Declan McCullagh. FBI: We Need Wiretap-Ready Web Sites—Now // CNET, 4 мая 2012 г., http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/; Charlie Savage. As Online Communications Stymie Wiretaps, Lawmakers Debate Solutions // New

York Times, 17 февраля 2011 г., http://www.nytimes.com/2011/02/18/us/18wiretap.html.

Napster, пионер в области пиринговых файлообменных сетей, был отключен…
Matt Richtel. Technology; Judge Orders Napster to Police Trading // New York Times, 7 марта 2001 г., http://www.nytimes.com/2001/03/07/business/technology-judge-orders-napster-to-police-trading-=pm.

способна блокировать передачу 99,4% таких материалов…
Matt Richtel. NapsterAppeals an Order to Remain Closed Down // *New York Times*, 13 июля 2001 г., http://www.nytimes.com/2001/07/13/business/technology-napster-appeals-an-order-to-remain-closed-down.html;
Lawrence Lessig. Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity. New York: Penguin Press, 2004, p. 73–74, http://www.free-culture.cc/freeculture.pdf.

абонентам, находящимся в зоне доступа…
Beware: Dangers of Bluetooth in Saudi... // Emirates 24/7, 1 декабря 2010 г., http://www.emirates247.com/news/region/beware-dangers-of-bluetooth-in-saudi-2010-12-01-1.323699;
Associated Press (AP). In Saudi Arabia, a High-Tech Way to Flirt // MSNBC, 11 августа 2005 г., http://www.msnbc.msn.com/id/8916890/ns/world_news-mideast_n_africa/t/saudi-arabia-high-tech-way-flirt/#.UJBU0sVG-8A.

Etisalat разослал почти 150 тысячам владельцев BlackBerry…
Margaret Coker and Stuart Weinberg. RIM Warns Update Has Spy ware // Wall Street Journal, 23 июля 2009 г., http://online.wsj.com/article/SB124827172417172239.html;
John Timmer. UAE Cellular Carrier Rolls Out Spyware as a 3G ‘Update’ // Ars Technica, 23 июля 2009 г., http://arstechnica.com/business/2009/07/mobile-carrier-rolls-out-spyware-as-a-3g-update/.

обязательное обновление системы…
UAE Spyware Blackberry Update // Digital Trends, 22 июля 2009 г., http://www.digitaltrends.com/mobile/uae-spyware-blackberry-update/.

RIM, производитель BlackBerry, дистанцировалась…
George Bevir. Etisalat Accused in Surveillance Patch Fiasco // Arabian Business, 21 июля 2009 г., http://www.arabianbusiness.com/etisalat-accused-in-surveillance-patch-fiasco-15698.html; см. также Adam Schreck, Associated Press (AP). United Arab Emirates, Saudi Arabia to Block BlackBerry over Security Fears // Huffington Post, 1 августа 2010 г., http://www.huffingtonpost.com/2010/08/01/uae-saudi-arabia-blackberry-ban_n_666581.html.

в ОАЭ и в соседней Саудовской Аравии раздались призывы ввести полный запрет…
Margaret Coker, Tim Falconer, Phred Dvorak. U.A.E. Puts the Squeeze on BlackBerry // Wall Street Journal, 2 августа 2010 г., http://online.wsj.com/article/SB10001424052748704702304575402493300698912.html;
Kayla Webley. UAE, Saudi Arabia Ban the Blackberry // Time, 5 августа 2010 г., http://www.time.com/time/specials/packages/article/0,28804,2008434_2008436_2008440,00.html; Saudi Arabia Begins Blackberry Ban, Users Say // BBC, 6 августа 2010 г., http://www.bbc.co.uk/news/world-middle-east-10888954.

Так же поступила Индия…
Bappa Majumdar and Devidutta Tripathy. Setback for BlackBerry in India; Saudi Deal Seen // Reuters, 11 августа 2010 г., India edition, http://in.reuters.com/article/2010/08/11/idINIndia-50769520100811.

Результатами беспорядков стали пятеро погибших…
Laura Davis. The Debate: Could the Behaviour Seen at the Riots Ever Be Justified? // Notebook (блог), Independent (London), 8 августа 2012

г., http://blogs.independent.co.uk/2012/08/08/the-debate-could-the-behaviour-seen-at-the-riots-ever-be-justified/.

ущерб в размере 300 млн фунтов стерлингов ($475 млн)…
John Benyon. England's Urban Disorder: The 2011 Riots // Political Insight, 28 марта 2012 г., http://www.politicalinsightmagazine.com/?p=911;
A Little Bit of History Repeating // Inside Housing, 27 июля 2012 г., http://www.insidehousing.co.uk/tenancies/a-little-bit-of-history-repeating/6522947.article.

призвала BlackBerry приостанавливать по ночам оказание услуг…
Sky News Newsdesk, Twitter, 9 августа 2011 г., 5:32, https://twitter.com/SkyNewsBreak/status/100907315603054592;
Bill Ray. Tottenham MP Calls for BlackBerry Messenging Suspension // Register, 9 августа 2011 г., http://www.theregister.co.uk/2011/08/09/bbm_suspension/.

«когда мы знаем, что люди замышляют насилие, беспорядки или преступления»…
PM Statement on Disorder in England // Number 10 (официальный сайт премьер-министра Великобритании), 11 августа 2011 г., http://www.number10.gov.uk/news/pm-statement-on-disorder-in-england/.

«дать полиции инструмент для отслеживания людей…
Rich Trenholm. Cameron Considers Blocking Twitter, Facebook, BBM after Riots // CNET, 11 августа 2011 г., http://crave.cnet.co.uk/software/cameron-considers-blocking-twitter-facebook-bbm-after-riots-50004693/;
Olivia Solon. Cameron Suggests Blocking Potential Criminals from Social Media // Wired UK, 11 августа 2011 г., http://www.wired.co.uk/news/archive/2011-08/11/david-cameron-social-media.

заявил об их готовности сотрудничать с правоохранительными органами…
Social Media Talks About Rioting ‘Constructive’ // BBC, 25 августа 2011 г., http://www.bbc.co.uk/news/uk-14657456.

биткоины…
Биткоин — это результат самого успешного на сегодняшний день эксперимента по созданию электронной валюты; проведение онлайн-платежей предполагает использование пиринговых сетей и цифровых подписей.
Курс биткоина сильно колеблется: вначале за единицу давали 3 цента, а уже через год — $29,57. Эта валюта хранится в электронных кошельках, ею можно расплачиваться за множество виртуальных и реальных товаров и услуг. По данным одного исследования, на черном онлайн-рынке «Шелковый путь», где люди с помощью анонимных каналов покупают наркотики, биткоины являются единственным средством платежа. Ежегодный оборот этого рынка составляет примерно $22 млн. См. Andy Greenberg. Black Market Drug Site ‘Silk Road’ Booming: $22 Million in Annual Sales // Forbes, 6 августа 2012 г., http://www.forbes.com/sites/andygreenberg/2012/08/06/black-market-drug-site-silk-road-booming-22-million-in-annual-mostly-illegal-sales/; Nicolas Christin. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace» (working paper, INI/CyLab, Carnegie Mellon, Pittsburgh, PA, 1 августа 2012 г.), http://arxiv.org/pdf/1207.7139v1.pdf.

непонятно, как можно добиться того…
Бруно Феррари, из беседы с авторами, ноябрь 2011 г.

не являются демократиями, или являются ими только формально…
Arch Puddington. Freedom in the World 2012: The Arab Uprisings and Their Global Repercussions, Freedom House, ссылка по состоянию на 15 октября 2012 г. http://www.freedomhouse.org/sites/default/files/FIW202012%20Booklet_0.pdf.

с самым низким в мире уровнем проникновения интернета…
См. низкие значения проникновения мобильной связи и интернета в странах с наиболее репрессивными режимами в мире, например таких, как Экваториальная Гвинея, Эритрея и Северная Корея, по данным доклада Worst of the Worst 2012: The World's Most Repressive Societies, Freedom House, ссылка по состоянию на 15 октября 2012 г. http://www.freedomhouse.org/sites/default/files/Worst20of%20the%20Worst%202012%20final20report.pdf,
Mobile-Cellular Telephone Subscriptions Per 100 Inhabitants. Percentage of Individuals Using the Internet // International Telecommunication Union (ITU), ICT Data and Statistics (IDS), ссылка по состоянию на 15 октября 2012 г., http://www.itu.int/ITU-D/ict/statistics/.

«Сегодняшние диктаторы и авторитарные правители гораздо умнее…
William J. Dobson. The Dictator's Learning Curve: Inside the Global Battle for Democracy. New York: Doubleday, 2012, 4.

Добсон перечисляет множество средств…
Там же.

сознательно и искусно созданные проекты…
Там же, с. 8.

автократии мира столкнутся с ситуацией…
См. низкие значения проникновения интернета в странах с наиболее репрессивными режимами в мире, например таких, как Экваториальная Гвинея, Эритрея и Северная Корея, по данным доклада Worst of the Worst 2012: The World's Most Repressive 274, примечания к с. 77–80 Societies, Freedom House, ссылка по состоянию на 15 октября 2012 г., http://www.freedomhouse.org/sites/default/files/Worst%20of%20the%20Worst%202012%20final%20report.pdf,
Percentage of Individuals Using the Internet // International Telecommunication Union (ITU), ICT Data and Statistics (IDS), ссылка по состоянию на 15 октября 2012 г., http://www.itu.int/ITU-D/ict/statistics/.

команда исследователей из Университета Карнеги–Меллон продемонстрировала результаты исследования…
Alessandro Acquisti, Ralph Gross, Fred Stutzman. Faces of Facebook: Privacy in the Age of Augmented Reality // Heinz College and CyLab, Carnegie Mellon University (презентация на конференции 2011 Black Hat Security Conference, Лас-Вегас, 3–4 августа 2011 г.), http://media.blackhat.com/bh-us-11/Acquisti/BH_US_11_Acquisti_Faces_of_Facebook_Slides.pdf.; Declan McCullagh. Face-Matching with Facebook Profiles: How It Was Done // CNET, 4 августа 2011 г., http://news.cnet.com/8301-31921_3-20088456-281/face-matching-with-facebook-profiles-how-it-was-done/.

запущенной в 2009 году…
UIDAI Background // Unique Identification Authority of India, ссылка по состоянию на 13 октября 2012 г. http://uidai.gov.in/about-uidai.html.

известной в Индии под названием «Аадаар» («основание», «поддержка»)…
Aadhaar Concept // Unique Identification Authority of India, ссылка по состоянию на 13 октября 2012 г. http://uidai.gov.in/aadhaar.html.

уникальный 12-значный номер…
What Is Aadhaar? // Unique Identifi cation Authority of India, ссылка по состоянию на 13 октября 2012 г. http://uidai.gov.in/what-is-aadhaar-number.html.

биометрические данные человека, в том числе его отпечатки пальцев и сканированное изображение сетчатки глаза…
Sunil Dabir and Umesh Ujgare. Aadhaar: The Numbers for Life // News on Air (New Delhi), ссылка по состоянию на 13 октября 2012 г. http://www.newsonair.nic.in/A_ADHA_AR-UID-Card-THE-NUMBERS-FOR-LIFE.asp.

счет в банке, привязанный к своему UID-номеру…

Surabhi Agarwal and Remya Nair. UID-Enabled Bank Accounts in 2–3 Months // Mint with the Wall Street Journal (New Delhi), 17 мая 2011 г. http://www.livemint.com/Politics/Go6diBWitIaus61Xud70EK/UIDenabled-bank-accounts-in-23-months.html;
Reform by Numbers // Economist, 14 января 2012 г., http://www.economist.com/node/21542814.

меньше 3% индийцев зарегистрированы для уплаты подоходного налога…
Salaried Taxpayers May Be Spared Filing Returns // Business Standard (New Delhi), 19 января 2011 г., http://business-standard.com/india/news/salaried-taxpayers-may-be-spared-filing-returns/422225/.

закона «Об удостоверениях личности» 2006 года…
Identity Cards Act 2006 // The National Archives (United Kingdom), Browse Legislation, ссылка по состоянию на 15 октября 2012 г., http://www.legislation.gov.uk/ukpga/2006/15/introduction.

недавно избранное коалиционное правительство страны в 2010 году приняло решение от нее отказаться…
Alan Travis. ID Cards Scheme to Be Scrapped Within 100 Days // Guardian (Manchester), 27 мая 2010 г., http://www.guardian.co.uk/politics/2010/may/27/theresa-may-scrapping-id-cards;
Identity Cards Scheme Will Be A xed ‘Within 100 Days’ // BBC, 27 мая 2010 г., http://news.bbc.co.uk/2/hi/8707355.stm.

необходимо получить от индивидуума явное и информированное согласие…
Opinion 15/2011 on the Definition of Consent // Article 29 Data Protection Working Party, European Commission, версия от 13 июля 2011 г., http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

От стран-участниц требуется…

EU Directive 95/46/EC—The Data Protection Directive: Chapter III Judicial Remedies, Liability and Sanctions // Data Protection Commissioner, http://www.dataprotection.ie/viewdoc.asp?DocID=94.

Назад к тексту

Глава 3. Будущее государства

YouTube в Иране…
Gwen Ackerman and Ladane Nasseri. Google Confirms Gmail and YouTube Blocked in Iran Since Feb. 10 // Bloomberg, 13 февраля 2012 г., http://www.bloomberg.com/news/2012-02-13/google-confirms-gmail-and-youtube-blocked-in-iran-since-feb-10.html.

Рекомендуем вышедшую в 2006 г. книгу Джека Голдсмита и Тима Ву «Кто контролирует интернет?»…
Jack Goldsmith and Tim Wu. Who Controls the Internet? Illusions of a Borderless World. New York: Oxford University Press, 2006.

большинство пользователей в виртуальном мире, как правило, не покидают свою культурную среду…
Мнение авторов, основанное на десятилетнем опыте работы в Google и двух годах в совете директоров компании.

отсутствуют некоторые понятия, например «Фалуньгун»…
Mark McDonald. Watch Your Language! (In China, They Really Do) // Rendezvous (blog), International Herald Tribune, the global edition of the New York Times, 13 марта 2012 г., http://rendezvous.blogs.nytimes.com/2012/03/13/watch-your-language-and-in-china-they-do/.

после неоднозначного визита…
Наблюдение председателя совета директоров Google Эрика Шмидта.

на службе у властей находится почти 300 тысяч «онлайн-комментаторов»…
Nate Anderson. 280,000 Pro-China Astroturfers Are Running Amok Online // Ars Technica, 26 марта 2010 г., http://arstechnica.com/tech-policy/news/2010/03/280000-pro-china-astroturfers-are-running-amok-online.ars;

Rebecca MacKinnon. China, the Internet, and Google, заметки, подготовленные для Комиссии Конгресса США по Китаю (официально не передавались), 1 марта 2010 г., http://rconversation.blogs.com/MacKinnonCECC_Mar1.pdf;
David Bandurski. China's Guerrilla War for the Web // Far Eastern Economic Review, июль 2008 г. http://www.feer.com/essays/2008/august/chinas-guerrilla-war-for-the-web. Примечание: впервые значение «280 000 человек» было указано в 2008 г., а затем подтверждено в 2010 г.

В выпущенном в 2010 году официальном правительственном докладе…
Полный текст: The Internet in China, IV. Basic Principles and Practices of Internet Administration (8 июня 2010 г.), Chinese Government's Official Web Portal, http://english.gov.cn/2010-06/08/content_1622956_6.htm.

блокировало работу YouTube…
Tom Zeller, Jr. YouTube Banned in Turkey after Insults to Ataturk // The Lede (блог), New York Times, 7 марта 2007 г., http://thelede.blogs.nytimes.com/2007/03/07/youtube-banned-in-turkey-after-insults-to-ataturk/.

YouTube согласилась блокировать показ видеоролика для турецкой аудитории…
Jeffrey Rosen. Google's Gatekeepers // New York Times Magazine, 28 ноября 2008 г., http://www.nytimes.com/2008/11/30/magazine/30google-t.html?partner=permalink&exprod=permalink.

около восьми тысяч сайтов…
Ayla Albayrak. Turkey Dials Back Plan to Expand Censorship // Wall Street Journal, 6 августа 2011 г., http://online.wsj.com/article/SB10001424053111903885604576490253692671470.html.

четыре уровня цензуры…
Sebnem Arsu. Internet Filters Set Off Protests Around Turkey // New York Times, 15 мая 2011

г., http://www.nytimes.com/2011/05/16/world/europe/16turkey.html?_r=3&.

тысячи людей более чем в тридцати турецких городах…
Ayla Albayrak. Turkey Dials Back Plan to Expand Censorship // Wall Street Journal, 6 августа 2011 г.

более агрессивную фильтрацию…
New Internet Filtering System Condemned as Backdoor Censorship // Reporters Without Borders, 2 декабря 2011 г., http://en.rsf.org/turquie-new-internet-filtering-system-02-12-2011,41498.html.

«Репортеры без границ»…
Там же.

Когда одна из турецких газет сообщила…
Internet Filters Block Evolution Website for Children in Turkey // Hurriyet (Istanbul), 8 декабря 2011 г., http://www.hurriyetdailynews.com/internet-filters-block-evolution-website-for-children-in-turkey.aspx?pageID=238&nID=8709&NewsCatID=374;
Sara Reardon. Controversial Turkish Internet Censorship Program Targets Evolution Sites // Science, 9 декабря 2011 г., http://news.sciencemag.org/scienceinsider/2011/12/controversial-turkish-internet-c.html.

Например, в Южной Корее закон «О национальной безопасности»…
Countries Under Surveillance: South Korea // Reporters Without Borders, ссылка по состоянию на 21 октября 2012 г. http://en.rsf.org/surveillance-south-korea,39757.html.

были заблокированы около сорока сайтов…
Там же.

закрыт десяток аккаунтов…
Lee Tae-hoon. Censorship on Pro-NK Websites Tight // Korea Times, 9 сентября 2010

г., http://www.koreatimes.co.kr/www/news/nation/2010/12/113_72788.html
.

на территории страны блокируются все сайты…
Europe // OpenNet Initiative, ссылка по состоянию на 21 октября 2012 г. http://opennet.net/research/regions/europe;
Germany // OpenNet Initiative, ссылка по состоянию на 21 октября 2012 г. http://opennet.net/research/profiles/germany.

несмотря на обещание никогда не подвергать интернет цензуре…
Clara Chooi. Najib Repeats Promise of No Internet Censorship // Malaysian Insider (Kuala Lumpur), 24 апреля 2011 г., http://www.themalaysianinsider.com/malaysia/article/najib-repeats-promise-of-no-internet-censorship.

на законодательном уровне — в законе «О гарантиях»…
Benefits // MSC Malaysia, ссылка по состоянию на 21 апреля 2012 г., http://www.mscmalaysia.my/why_msc_malaysia.

заблокировала доступ к файлообменным сайтам…
Ricky Laishram. Malayasian Government Blocks the Pirate Bay, MegaUpload and Other File Sharing Websites // Techie Buzz, 9 июня 2011 г., http://techie-buzz.com/tech-news/malayasian-government-blocks-websites.html.

Малайзийской комиссии по телекоммуникациям и мультимедиа говорилось…
Wong Pek Mei. MCMC Wants Block of 10 Websites That Allow Illegal Movie Downloads // The Star (Petaling Jaya), 10 июня 2011 г., http://thestar.com.my/news/story.asp?file=/2011/6/10/nation/20110610161330&sec=nation.

«Мы уважаем сделанный каждой из этих стран выбор собственного пути развития…
Сухбаатар Батболд (бывший премьер-министр Монголии), из беседы с авторами, ноябрь 2011 г.

первой страной в мире, на законодательном уровне установившей сетевой нейтралитет, стала Чили…
Tim Stevens. Chile Becomes First Country to Guarantee Net Neutrality, We Start Thinking About Moving // Engadget, 15 июля 2010 г., http://www.engadget.com/2010/07/15/chile-becomes-first-country-to-guarantee-net-neutrality-we-star/.

почти половина 17-миллионного населения Чили…
См. данные о населении и количестве интернет-пользователей в 2011 г. в Midyear Population and Density—Custom Region—Chile, 2011 // U.S. Census Bureau, International Data Base, ссылка по состоянию на 21 октября 2012 г. http://www.census.gov/population/international/data/idb/informationGateway.php и Percentage of Individuals Using the Internet // International Telecommunication Union (ITU), ICT Data and Statistics (IDS), ссылка по состоянию на 21 октября 2012 г. http://www.itu.int/ITU-D/ict/statistics/.

«халяльного интернета»…
Neal Ungerleider. Iran Cracking Down Online with ‘Halal Internet’ // Fast Company, 18 апреля 2011 г., http://www.fastcompany.com/1748123/iran-cracking-down-online-halal-internet.

запуск неотвратимо приближается…
Neal Ungerleider. Iran’s ‘Second Internet’ Rivals Censorship of China’s ‘Great Firewall’ // Fast Company, 23 апреля 2012 г., http://www.fastcompany.com/1819375/irans-second-internet-rivals-censorship-chinas-great-firewall.

«одобренные государством видеоролики»…
David Murphy. Iran Launches ‘Mehr,’ Its Own YouTube-like Video Hub, http://www.pcmag.com/article2/0,2817,2413014,00.asp.

на первом этапе национальный «чистый» интернет…
Christopher Rhoads and Farnaz Fassihi. Iran Vows to Unplug Internet // Wall Street Journal, версия от 19 декабря 2011

г., http://online.wsj.com/article/SB10001424052748704889404576277391449002016.html;
Nick Meo. Iran Planning to Cut Internet Access to Rest of World // Telegraph (London), 28 апреля 2012 г., http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9233390/Iran-planning-to-cut-internet-access-to-rest-of-world.html.

введенному в 2012 году запрету на иностранное противовирусное ПО…
S. Isayev and T. Jafarov. Iran Bans Import of Foreign Computer Security Software // Trend, 20 февраля 2012 г., http://en.trend.az/regions/iran/1994160.html.

Глава министерства экономики Ирана в интервью государственному агентству новостей выразил надежду…
Rhoads and Fassihi. Iran Vows to Unplug Internet, http://online.wsj.com/article/SB10001424052748704889404576277391449002016.html.

Нечто подобное обещал построить и Пакистан…
2Request for Proposal: National URL Filtering and Blocking System // National ICT R&D Fund, ссылка по состоянию на 21 октября 2012 г. http://ictrdf.org.pk/RFP-%20URL%20Filtering%20%26%20Blocking.pdf;
Ungerleider. Iran's 'Second Internet' Rivals Censorship of China's 'Great Firewall', http://www.fastcompany.com/1819375/irans-second-internet-rivals-censorship-chinas-great-firewall;
Danny O'Brien. Pakistan's Excessive Internet Censorship Plans // Committee to Protect Journalists (CPJ), 1 марта 2012 г., http://www.cpj.org/internet/2012/03/pakistans-excessive-net-censorship-plans.php.
Стоит заметить, что на момент написания книги пакистанская программа была положена «на полку». См. Shahbaz Rana. IT Ministry Shelves Plan to Install Massive URL Blocking System // The Express Tribune (Karachi) (блог) на сайте International Herald Tribune, 19 марта 2012 г., http://tribune.com.pk/story/352172/it-ministry-shelves-plan-to-install-massive-url-blocking-system/.

75-процентной долей Koryolink, единственного оператора сотовой связи в Северной Корее…
Mobile Phones in North Korea: Also Available to Earthlings // Economist, 11 февраля 2012 г., http://www.economist.com/node/21547295.

ежедневная северокорейская газета Rodong Sinmun рассылает ее абонентам новости в формате SMS…
Там же.

оплачивать свои телефонные счета в евро…
Там же; David Matthew. Understanding the Growth of KoryoLink // NK News, 15 декабря 2011 г., http://www.nknews.org/2011/12/understanding-koryo-link/.

количество абонентов сотовой связи увеличилось в три раза…
Mobile Phones in North Korea: Also Available to Earthlings // Economist, 11 февраля 2012 г.

Валовая прибыль Koryolink…
Там же.

Ericsson и Nokia Siemens Networks…
Steve Stecklow, Farnaz Fassihi and Loretta Chao. Chinese Tech Giant Aids Iran // Wall Street Journal, 27 октября 2011 г., http://online.wsj.com/article/SB10001424052970204644504576651503577823210.html?_nocache=1346874829284&user=welcome&mg=id-wsj.

Huawei активно продвигал свою продукцию…
Там же.

компания Zaeim Electronic Industries Co, также является фаворитом…
Там же.

Huawei утверждает, что продает Zaeim только «коммерческие продукты для широкого использования»…
Там же.

Huawei выпустила пресс-релиз…
Huawei. Statement Regarding Inaccurate and Misleading Claims About Huawei's Commercial Operations in Iran, пресс-релиз, 4 ноября 2011 г., http://www.huawei.com/en/about-huawei/newsroom/press-release/hw-104191.htm.

«добровольно ограничивает» свои операции…
Huawei. Statement Regarding Huawei's Commercial Operations in Iran, пресс-релиз, 9 декабря 2011 г., http://www.huawei.com/en/about-huawei/newsroom/press-release/hw-104866-statement-commercialoperations.htm.

«полностью выполнять все законы об интеллектуальной собственности…»
Ху Цзиньтао, выступление перед группой руководителей крупных корпораций во время саммита Азиатско-Тихоокеанского экономического сотрудничества (АПЕК) в 2011 г.

только в 2009 году американские компании недополучили примерно $3,5 млрд…
2010 Report to Congress on China's WTO Compliance, United States Trade Representative (декабрь 2010 г.),
5, http://www.ustr.gov/webfm_send/2460.

79% конфискованной в США контрафактной продукции, нарушающей чьи-либо авторские права…
Там же, с. 92.

Подобные проблемы существуют в России, Индии и Пакистане…
2011 Special 301 Report, United States Trade Representative, см. Section II: Country Reports Priority Watch List, 25, 28,
30, http://www.ustr.gov/webfm_send/2841.

Израиль и Канаду…
Там же, с. 27, 29.

определение кибероружия, данное бывшим руководителем американского ведомства по борьбе с терроризмом Ричардом Кларком…
Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It. New York: Ecco, 2010, 6.

В октябре 2012 года министр обороны США Леон Панетта выступил с предупреждением…
Elisabeth Bumiller and Thom Shanker. Panetta Warns of Dire Threat of Cyberattack on U.S. // New York Times, 11 октября 2012 г., http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?hp&_r=1&.

«Война есть не что иное, как продолжение государственной политики иными средствами»…
Carl von Clausewitz. On War. Baltimore: Penguin Books, 1968.

«намного труднее понять, кто же нанес вам удар»…
Крейг Манди, из беседы с авторами в ноябре 2011 г.

Манди называет тактику кибершпионажа «оружием массового разрушения»…
Craig Mundie. Information Security in the Digital Decade». Remarks at the American Chamber of Commerce in Bangkok, Thailand, 20 октября 2003 г., http://www.microsoft.com/en-us/news/exec/craig/10-20security.aspx.

пока выявленный в 2012 году вирус Flame не отобрал у него этот титул…
Resource 207: Kaspersky Lab Research Proves That Stuxnet and Flame Developers Are Connected // Kaspersky Lab, 11 июня 2012 г., http://www.kaspersky.com/about/news/virus/2012/

Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected.

заставил газовые центрифуги резко изменять скорость вращения…
David E. Sanger. Obama Order Sped Up Wave of Cyberattacks Against Iran // New York Times, 1 июня 2012 г., http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r =1&ref =davidesanger&pagewanted=all.

какой-нибудь служащий завода по незнанию пронес его на USB-накопителе…
Там же.

признал даже президент страны Махмуд Ахмадинежад…
Julian Borger and Saeed Kamali Dehghan. Attack on Iranian Nuclear Scientists Prompts Hit Squad Claims // Guardian (Manchester), 29 ноября 2010 г., http://www.guardian.co.uk/world/2010/nov/29/iranian-nuclear-scientists-attack-claims.

«вырвался на волю»…
Sanger. Obama Order Sped Up Wave of Cyber-attacks Against Iran, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&ref=davidesanger&pagewanted=all.

ссылки на даты и библейские истории…
Elinor Mills. Stuxnet: Fact vs. Theory // CNET, 5 октября 2010 г., http://news.cnet.com/8301-27080_3-20018530-245.html.

писали не менее тридцати человек…
Michael Joseph Gross. A Declaration of Cyber-War // Vanity Fair, апрель 2011 г., http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104

первый вариант Stuxnet…

Elinor Mills. Shared Code Indicates Flame, Stuxnet Creators Worked Together // CNET, 11 июня 2012 г., http://news.cnet.com/8301-1009_3-57450292-83/shared-code-indicates-flame-stuxnet-creators-worked-together/.

Анонимный источник в администрации президента Обамы…
Sanger. Obama Order Sped Up Wave of Cyberattacks Against Iran, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&ref=davidesanger&pagewanted=all.

и правда думаете, я вам расскажу…
Меир Даган, из беседы с авторами, июнь 2012 г.

назывался «Олимпийские игры», затем перешел «по наследству» к следующему президенту…
Sanger. Obama Order Sped Up Wave of Cyberattacks Against Iran, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&ref=davidesanger&pagewanted=all.

После завершения разработки и тестирования червя…
Там же.

Ларри Константин, профессор Университета Мадейры в Португалии, усомнился в данных Сангера…
Larry Constantine, interview by Steven Cherry. Stuxnet: Leaks or Lies? // Techwise Conversations (podcast), IEEE Spectrum, 4 сентября 2012 г., http://spectrum.ieee.org/podcast/computing/embedded-systems/stuxnet-leaks-or-lies.

Как сказал Сангеру бывший директор ЦРУ Майкл Хэйден…
Sanger. Obama Order Sped Up Wave of Cyberattacks Against Iran, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&ref=davidesanger&pagewanted=all.

По словам Сангера, официальные лица США отрицали, что Flame являлся частью проекта «Олимпийские игры»…
Там же.

специалисты из «Лаборатории Касперского…
Resource 207: Kaspersky Lab Research Proves That Stuxnet and Flame Developers Are Connected, http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Prove_that_Stuxnet_and_Flame_Developers_are_Connected;
Mills. hared Code Indicates Flame, Stuxnet Creators Worked Together, http://news.cnet.com/8301-1009_3-57450292-83/shared-code-indicates-flame-stuxnet-creators-worked-together/.

обнаружить один модуль под названием Resource 207…
Resource 207: Kaspersky Lab Research Proves That Stuxnet and Flame Developers Are
Connected, http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected.

руководитель исследовательской группы "Лаборатории Касперского"…
Mills. Shared Code Indicates Flame, Stuxnet Creators Worked Together, http://news.cnet.com/8301-1009_3-57450292-83/shared-code-indicates-flame-stuxnet-creators-worked-together/.

дипломатических баталий, развернувшихся в 2007 году после заявления правительства Эстонии…
Bronze Soldier Installed at Tallinn Military Cemetery // RIA Novosti (Moscow), 30 апреля 2007
г., http://en.rian.ru/world/20070430/64692507.html.

множество известных эстонских сайтов…

Ian Traynor. Russia Accused of Unleashing Cyberwar to Disable Estonia // Guardian (Manchester), 16 мая 2007 г., http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

Эстонию часто называют самой цифровой страной на Земле…
Joshua Davis. Hackers Take Down the Most Wired Country in Europe // Wired, 21 августа 2007 г., http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

Урмас Паэт прямо обвинил во всем Кремль…
Doug Bernard. New Alarm Bells, and Old Questions, About the Flame Virus and Cyber-War // VOA (блог), 30 мая 2012 г., http://blogs.voanews.com/digital-frontiers/tag/cyber-war/.

Эксперты НАТО и Евросоюза не смогли найти свидетельства…
Estonia Has No Evidence of Kremlin Involvement in Cyber Attacks // RIA Novosti (Moscow), 9 июня 2007 г., http://en.rian.ru/world/20070906/76959190.html.

были выведены из строя сайты министерства обороны и правительства Грузии…
John Markoff. Georgia Takes a Beating in the Cyberwar with Russia // Bits (blog), New York Times, 11 августа 2008 г., http://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia/;
John Markoff. Before the Gunfire, Cyber-attacks // New York Times, 12 августа 2008 г., http://www.nytimes.com/2008/08/13/technology/13cyber.html.

хакеры из России выбрали в качестве мишени киргизских интернет-провайдеров…
Gregg Keizer. Russian ‘Cybermilitia’ Knocks Kyrgyzstan Offline // Computerworld, 28 января 2009 г., http://www.computerworld.com/s/article/9126947/Russian_cybermilitia_knocks_Kyrgyzstan_offline.

на несколько дней отключив 80% абонентов широкополосного доступа страны…
Christopher Rhoads. Kyrgyzstan Knocked Offline // Wall Street Journal, 28 января 2009 г., http://online.wsj.com/article/SB123310906904622741.html.

Кто-то считает, что целью атаки…
Там же; Kyrgyzstan to Close US Airbase, Washington Says No Plans Made // Hurriyet (Istanbul), 17 января 2009 г., http://www.hurriyet.com.tr/english/world/10796846.asp?scr=1.

В конце 2009 года специалисты Google обнаружили подозрительный трафик в своей сети…
David Drummond. A New Approach to China // Google Blog, 12 января 2010 г., http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

принять решение об изменении своего подхода к бизнесу в Китае…
David Drummond. A New Approach to China, an Update // Google Blog, 22 марта 2010 г., http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

Пентагон выпустил директиву о создании Кибернетического командования США (USCybercom)…
U.S. Cyber Command // U.S. Strategic Command, версия декабря 2011 г., http://www.stratcom.mil/factsheets/cyber_command/.

Роберт Гейтс провозгласил киберпространство «пятой областью» военных операций…
Misha Glenny. Who Controls the Internet? // Financial Times Magazine (London), 8 октября 2010 г., http://www.ft.com/cms/s/2/3e52897c-d0ee-11df-a426-00144feabdc0.html#axzz1nYp7grM6; Susan P. Crawford. When We Wage Cyber war, the Whole Web Suffers // Bloomberg, 25 апреля 2012 г., http://www.bloomberg.com/news/2012-04-25/when-we-wage-cyberwar-the-whole-web-suffers.html.

годовой бюджет нового «киберпромышленного комплекса» в диапазоне $80–150 млрд…
Ron Deibert and Rafal Rohozinski. The New Cyber Military-Industrial Complex // Globe and Mail (Toronto), 28 марта 2011 г., http://www.theglobeandmail.com/commentary/the-new-cyber-military-industrial-complex/article573990.

После разгрома здания египетской службы государственной безопасности…
Там же; Eli Lake. British Firm Offered Spy Software to Egypt // Washington Times, 25 апреля 2011 г., http://www.washingtontimes.com/news/2011/apr/25/british-firm-offered-spy-software-to-egypt/?page=all#pagebreak.

китайскую телекоммуникационную компанию привлекли…
WikiLeaks cable. Subject: stifled potential: fiber-optic cable lands in tanzania, Origin: Embassy Dar Es Salaam (Tanzania), Cable time: Fri. 4 Sep 2009 04:48 UTC, http://www.cablegatesearch.net/cable.php?id=09DARESSALAAM585.

Sichuan Hongda объявила…
Fumbuka Ng'wanakilala. China Co Signs $3 Bln Tanzania Coal, Iron Deal // Reuters, 22 сентября 2011 г., http://www.reuters.com/article/2011/09/22/tanzania-china-mining-idUSL5E7KM1HU20110922.

соглашение с Китаем на сумму $1 млрд…
China, Tanzania Sign $1 Bln Gas Pipeline Deal: Report // Reuters, 30 сентября 2011 г., Africa edition, http://af.reuters.com/article/investingNews/idAFJOE78T08T20110930?pageNumber=1&virtualBrandChannel=0.

На долю государственных компаний в Китае приходится 80% капитализации…
Emerging-Market Multinationals: The Rise of State Capitalism // Economist, 21 января 2012 г., http://www.economist.com/node/21543160.

$150 млн на создание проекта «электронного правительства» Ганы…
Andrea Marshall. China's Mighty Telecom Footprint in Africa // eLearning Africa News Portal, 21 февраля 2011 г., http://www.elearning-africa.com/eLA_Newsportal/china%E2%80%99s-mighty-telecom-footprint-in-africa/.

исследовательский госпиталь в Кении…
East Africa: Kenya, China in Sh8 Billion University Hospital Deal // AllAfrica, 22 апреля 2011 г., http://allafrica.com/stories/201104250544.html.

«Африканский техноград» в Хартуме…
John G. Whitesides. Better Diplomacy, Better Science // China Economic Review, 1 января 1970 г., http://www.chinaeconomicreview.com/content/better-diplomacy-better-science.

четыре основных производителя…
Мнение авторов.

Это уже называют «новой холодной войной»:
Michael Riley and Ashlee Vance. Cyber Weapons: The New Arms Race // Bloomberg BusinessWeek, 20 июля 2011 г., http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html. Как видите, не мы придумали термин «холодная кибервойна».

в результате трех волн DDoS-атак были выведены из строя крупные правительственные сайты…
Kim Zetter. Lawmaker Wants 'Show of Force' Against North Korea for Website Attacks // Wired, 10 июля 2009 г., http://www.wired.com/threatlevel/2009/07/show-of-force/.

сеть участвовавших в атаке компьютеров, или ботнетов, была родом из Северной Кореи…

Choe Sang-Hun and John Markoff. Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea // New York Times, 9 июля 2009
г., http://www.nytimes.com/2009/07/10/technology/10cyber.html?_r=1;
Associated Press (AP). U.S. Officials Eye N. Korea in Cyberattack // USA Today, 9 июля 2009
г., http://usatoday30.usatoday.com/news/washington/2009-07-08-hack ing-washington-nkorea_N.htm.

обвинили в произошедшем Пхеньян…
Choe and Markoff. Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea // New York Times, 9 июля 2009 г..

республиканский конгрессмен потребовал…
Zetter. Lawmaker Wants 'Show of Force' Against North Korea for Website Attacks // Wired, 10 июля
2009 г.

признаков причастности к нападению правительства Северной Кореи или любой другой страны найти не удалось…
Lolita C. Baldor, Associated Press (AP). US Largely Ruling Out North Korea in 2009 Cyber Attacks // USA Today, 6 июля 2010
г., http://usatoday30.usatoday.com/tech/news/computersecurity/2010-07-06-nkorea-cyber-attacks_N.htm.

Один из вьетнамских специалистов заявил, что атака началась в Великобритании…
Martyn Williams. UK, Not North Korea, Source of DDOS Attacks, Researcher Says // IDG News Service and Network World, 14 июля 2009
г., http://www.networkworld.com/news/2009/071409-uk-not-north-korea-source.html?ap1=rcb.

в Южной Корее продолжали настаивать…
N. Korean Ministry Behind July Cyber Attacks: Spy Chief // Yonhap News, 30 октября 2009

г., http://english.yonhapnews.co.kr/northkorea/2009/10/30/0401000000AEN20091030002200315.HTML.

от полупроводников и автомобилей до реактивных технологий…
Michael Riley and Ashlee Vance. Inside the Chinese Boom in Corporate Espionage // Bloomberg BusinessWeek, 15 марта 2012 г., http://www.businessweek.com/articles/2012-03-14/inside-the-chinese-boom-in-corporate-espionage.

Ост-Индская компания наняла одного шотландского ботаника…
Famous Cases of Corporate Espionage // Bloomberg BusinessWeek, 20 сентября 2011 г., http://images.businessweek.com/slideshows/20110919/famous-cases-of-corporate-espionage #slide3.

китайская супружеская пара из Мичигана…
Ed White, Associated Press (AP). Shanshan Du, Ex-GM Worker, Allegedly Tried to Sell Hybrid Car Secrets to Chinese Companies // Huffington Post, 23 июля 2010 г., http://www.huffingtonpost.com/2010/07/23/shanshan-du-ex-gm-worker_n_656894.html.

сотрудник ведущего производителя красок и облицовочных материалов Valspar Corporation…
Cyber Espionage: An Economic Issue», China Caucus (blog), Congressional China Caucus, 9 августа 2011 г., http://forbes.house.gov/chinacaucus/blog/?postid=268227;
Foreign Spies Stealing U.S. Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011, Office of the National Counterintelligence Executive, (октябрь 2011 г.), 3, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

ученый-химик из DuPont…
Economic Espionage // Office of the National Counterintelligence Executive, ссылка по состоянию на 22 октября 2012

г. http://www.ncix.gov/issues/economic/index.php.

Основное условие: если ваша сеть заражена…
Крейг Манди, из беседы с авторами, ноябрь 2011 г.

Манди считает…
Там же.

10 млн строк кода…
DARPA. DARPA Increases Top Line Investment in Cyber Research by 50 Percent over next Five Years // Новостной бюллетень, 7 ноября 2011 г., http://www.darpa.mil/NewsEvents/Releases/2011/11/07.aspx; Spencer Ackerman. Darpa Begs Hackers: Secure Our Networks, End 'Season of Darkness' // Danger Room (блог), Wired, 7 ноября 2011 г., http://www.wired.com/dangerroom/2011/11/darpa-hackers-cybersecurity/.

«приходилось выступать за технологические изменения»…
Регина Даган, из беседы с авторами, июль 2012 г.

собрав объединенную команду из специалистов по компьютерной безопасности…
Cheryl Pellerin, American Forces Press Service. DARPA Goal for Cybersecurity: Change the Game», U.S. Air Force, 20 декабря 2010 г., http://www.af.mil/news/story.asp?id=123235799.

Назад к тексту

Глава 4. Будущее революций

молодо население многих государств, недавно получивших доступ в сеть…
См. низкие значения проникновения интернета в 2011 г. для Эфиопии, Пакистана и Филиппин в Percentage of Individuals Using the Internet // International Telecommunication Union (ITU), ICT Data and Statistics (IDS), ссылка по состоянию на 16 октября 2012 г. http://www.itu.int/ITU-D/ict/statistics/, и данные о количестве молодых жителей этих стран за 2011 г. в Mid-Year Population by Five Year Age Groups and Sex— Custom Region—Ethiopia, Pakistan, Philippines // U.S. Census Bureau, International Data Base, ссылка по состоянию на 16 октября 2012 г. http://www.census.gov/population/international/data/idb/region.php.

более активная роль женщин…
Courtney C. Radsch. Unveiling the Revolutionaries: Cyberactivism and the Role of Women in the Arab Uprisings // James A. Baker III Institute for Public Policy, Rice University, May 17, 2012;
Jeff Falk. Social Media, Internet Allowed Young Arab Women to Play a Central Role in Arab Spring, 24 мая 2012 г., Rice University, News and Media, http://news.rice.edu/2012/05/24/social-media-and-the-internet-allowed-young-arab-women-to-play-a-central-role-in-the-arab-spring-uprisings-new-rice-study-says-2/;
Women and the Arab Spring: Taking Their Place?, International Federation for Human Rights, ссылка по состоянию на 4 ноября 2012 г., http://www.europarl.europa.eu/document/activities/cont/201206/20120608AT T46510/20120608ATT46510EN.pdf;
Lauren Bohn. Women and the Arab Uprisings: 8 ‘Agents of Change’ to Follow // CNN, 3 февраля 2012 г., http://www.cnn.com/2012/02/03/world/africa/women-arab-uprisings/index.html.

небольшие группы протестующих собираются практически каждое утро…

Министры переходного правительства, из беседы с авторами в Триполи, январь 2012 г.

в сообщении «Аль-Джазира» на английском языке были приведены данные о множестве погибших демонстрантов…
Fresh Protests Erupt in Syria // Al Jazeera, версия от 8 апреля 2011 г., http://www.aljazeera.com/news/middleeast/2011/04/201148104927711611.html.

«Аль-Джазира» на арабском, как ни странно…
David Pollock. Al Jazeera: One Organization, Two Messages // Washington Institute, Policy Analysis, 28 апреля 2011 г., http://www.washingtoninstitute.org/policy-analysis/view/aljazeera-one-organization-two-messages.

этот дисбаланс отражает политическую зависимость катарского телеканала от Ирана…
Там же.

упомянули об одинаковых проблемах…
Активисты «жасминовой революции», из беседы с авторами, январь 2012 г.

аккаунт в Twitter, созданный старшекурсником…
Stephan Faris. Meet the Man Tweeting Egypt's Voices to the World // Time, 1 февраля 2011 г., http://www.time.com/time/world/article/0,8599,2045489,00.html.

размещал там последние известия…
Там же.

@Jan25voices был основным источником информации о восстании…
Там же.

Он курировал один из самых заметных источников информации…

Andy Carvin, interview by Robert Siegel. The Revolution Will Be Tweeted // NPR, 21 февраля 2011 г., http://www.npr.org/2011/02/21/133943604/The-Revolution-Will-Be-Tweeted.

в Бенгази был сформирован Переходный национальный совет (ПНС)…
AntiGaddafi Figures Say Form National Council // Reuters, 27 февраля 2011 г., Africa edition, http://af.reuters.com/article/idAFWEB194120110227.

известные оппозиционеры, видные члены правительства, перешедшие на сторону восставших…
Dan Murphy. The Members of Libya's National Transitional Council // Christian Science Monitor, 2 сентября 2011 г., http://www.csmonitor.com/World/Backchannels/2011/0902/The-members-of-Libya-s-National-Transitional-Council;
David Gritten. Key Figures in Libya's Rebel Council // BBC, 25 августа 2011 г., http://www.bbc.co.uk/news/world-africa-12698562.

Население не прекращало протесты…
Tunisia's Leaders Resign from Ruling Party // NPR, January 20, 2011, http://www.npr.org/2011/01/20/133083002/tunisias-leaders-resign-from-ruling-party;
Christopher Alexander. Apres Ben Ali: Deluge, Democracy, or Authoritarian Relapse? // Middle East Channel (блог), Foreign Policy, 24 января 2011 г., http://mideast.foreignpolicy.com/posts/2011/01/24/apres_ben_ali_deluge_democracy_or_authoritarian_relapse.

«жертвой министерства внутренних дел»…
Премьер-министр Туниса Хамади Джебали, из беседы с авторами, январь 2012 г.

Али Лараеда, который провел 14 лет в тюрьме…
David D. Kirkpatrick. Opposition in Tunisia Finds Chance for Rebirth // New York Times, 20 января 2011

г., http://www.nytimes.com/2011/01/21/world/africa/21islamist.html?pagewanted=all;
Tarek Amara and Mariam Karouny. Tunisia Names New Government, Scraps Secret Police // Reuters, 8 марта 2011 г., http://in.mobile.reuters.com/article/worldNews/idINIndia-55387920110307?irpc=984.

«Трудно представить, чтобы де Голль или Черчилль могли появиться…»
Генри Киссинджер, из беседы с авторами, декабрь 2011 г.

«Если вы революционеры, покажите нам, на что способны…»
Mahmoud Salem. Chapter's End! // Rantings of a Sandmonkey (блог), 18 июня 2012 г., http://www.sandmonkey.org/2012/06/18/chapters-end/.

Он убеждал уличных активистов принимать участие в управлении страной…
Mahmoud Salem. For the Light to Come Back // Rantings of a Sandmonkey (блог), 30 марта 2012 г., http://www.sandmonkey.org/2012/03/30/for-the-light-to-come-back/.

книга Тины Розенберг «Вступите в клуб: как мнение группы может изменить мир»…
Более подробный анализ книги Join the Club: How Peer Pressure Can Transform the World см. в Saul Austerlitz. Power of Persuasion: Tina Rosenberg's Join the Club // review, The National (Abu Dhabi), 25 февраля 2011 г., http://www.thenational.ae/arts-culture/books/power-of-persuasion-tina-rosenbergs-join-the-club#full;
Jeffrey D. Sachs. Can Social Networking Cure Social Ills? // review, New York Times, 20 мая 2011 г., http://www.nytimes.com/2011/05/22/books/review/book-review-join-the-club-by-tina-rosenberg.html?pagewanted= all;
Thomas Hodgkinson. Join the Club by Tina Rosenberg—Review // Guardian (Manchester), 1 сентября 2011 г., http://www.guardian.co.uk/books/2011/sep/02/join-club-tina-rosenberg-review;

Steve Weinberg. C’mon, Everyone’s Doing It // review, Bookish (blog), Houston Chronicle, 27 марта 2011 г., http://blog.chron.com/bookish/2011/03/cmon-everyones-doing-it-a-review-of-tina-rosenbergs-new-book/.

Возможно, самая убедительная иллюстрация…
Tina Rosenberg. Join the Club: How Peer Pressure Can Transform the World. New York: W. W. Norton and Co., 2011.

на примере бывших сербских активистов, обучающих своих молодых коллег по всему миру…
Там же, с. 278–282, 332–336.

площадь Тахрир — место, где началась революция, — демонстранты несколько раз оккупировали снова…
Egypt Anti-Military Protesters Fill Tahrir Square // BBC, 22 июня 2012 г., http://www.bbc.co.uk/news/world-middle-east-18547371;
Aya Batrawy, Associated Press (AP). Egypt Protests: Thousands Gather in Tahrir Square to Demonstrate Against Military Rule // Huffington Post, 20 апреля 2012 г., http://www.huffingtonpost.com/2012/04/20/egypt-protests-tahrir-square_n_1439802.html;
Gregg Carlstrom and Evan Hill. Scorecard: Egypt Since the Revolution // Al Jazeera, версия от 24 января 2012 г., http://www.aljazeera.com/indepth/interactive/2012/01/201212271176135598.html;
Egypt Protests: Death Toll Up in Cairo’s Tahrir Square // BBC, 20 ноября 2011 г., http://www.bbc.co.uk/news/world-africa-15809739.

иранскому режиму в ходе протестов 2009 года, начавшихся после выборов…
Christopher Rhoads, Geoffrey A. Fowler, and Chip Cummins. Iran Cracks Down on Internet Use, Foreign Media // Wall Street Journal, 17 июня 2009 г., http://online.wsj.com/article/SB124519888117821213.html.

отдало распоряжение отключить интернет и мобильную связь…

James Cowie. Egypt Leaves the Internet // Renesys (блог), 27 января 2011 г., http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml.

В блокировке интернет-провайдеров было сделано всего одно исключение…
James Cowie. Egypt Returns to the Internet // Renesys (блог), 2 февраля 2011 г., http://www.renesys.com/blog/2011/02/egypt-returns-to-the-internet.shtml.

четырех основных национальных интернет-провайдеров…
Cowie. Egypt Leaves the
Internet, http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml.

оказание услуг мобильной связи было приостановлено…
Associated Press (AP). Vodafone: Egypt Ordered Cell Phone Service Stopped // Huffington Post, 28 февраля 2011 г., http://www.huffingtonpost.com/2011/01/28/vodafone-egypt-service-dropped_n_815493.html.

Утром крупнейшая из телекоммуникационных компаний Vodafone Egypt выступила с заявлением…
Statements—Vodafone Egypt // Vodafone, 28 января 2011 г., http://www.vodafone.com/content/index/media/press_statements/statement_on_egypt.html.

оптоволоконные кабели, размещенные в одном из каирских зданий…
James Glanz and John Markoff. Egypt Leaders Found ‘Off ’ Switch for Internet // New York Times, 15 февраля 2011 г., http://www.nytimes.com/2011/02/16/technology/16internet.html?pagewanted=all&_r=0.

государственная компания Telecom Egypt физически отрежет их от телекоммуникационной инфраструктуры…
Там же.

такой шаг не имел прецедентов в истории…
Parmy Olson. Egypt Goes Dark, Cuts Off Internet and Mobile Networks // Forbes, 28 января 2011 г., http://www.forbes.com/sites/parmyolson/2011/01/28/egypt-goes-dark/.

ударило по тому, что полагали важным 100% жителей…
Витторио Колао, из беседы с авторами, август 2011 г.

Оно могло нам не нравиться…
Там же, см. также Statements—Vodafone Egypt // Vodafone, 28 января 2011 г. — 3 февраля 2011 г., http://www.vodafone.com/content/index/media/press_statements/statement_on_egypt.html.

централизованно разослать SMS всем своим абонентам…
Statements—Vodafone Egypt // Vodafone, 3 февраля 2011 г., http://www.vodafone.com/content/index/media/press_statements/statement_on_eg.ypt.html;
Jonathan Browning. VodafoneSays It Was Instructed to Send Pro-Mubarak Messages to Customers // Bloomberg, 3 февраля 2011 г., http://www.bloomberg.com/news/2011-02-03/vodafone-ordered-to-send-egyptian-government-messages-update1-.html.

сообщения стали чересчур политизированными, причем односторонними…
Витторио Колао, из беседы с авторами, август 2011 г.

Vodafone Group PLC, материнская компания, выступила с заявлением…
Там же.

French Data Network организовала интернет-доступ…
Jonathan Browning. Google, Twitter Offer Egyptians Option to Tweet // Bloomberg, 1 февраля 2011 г., http://www.bloomberg.com/news/2011-01-31/egyptians-turn-to-dial-up-service-to-get-around-government-s-web-shutdown.html.

Google запустила услугу передачи твитов по телефону…
Ujjwal Singh and AbdelKarim Mardini. Some Weekend Work That Will (Hopefully) Enable More Egyptians to Be Heard // Google Blog, 31 января 2011 г., http://googleblog.blogspot.com/2011/01/some-weekend-work-that-will-hopefully.html.

мы решили, что это нужно обсудить:
Витторио Колао, из беседы с авторами, август 2011 г.

египетская полиция нравов использовала троллей в чатах и форумах…
In a Time of Torture: The Assault on Justice in Egypt's Crackdown on Homosexual Conduct, Human Rights Watch (HRW):
2004, http://www.hrw.org/en/reports/2004/02/29/time-torture.

полиция нравов провела облаву в плавучем ночном клубе…
Там же;
Egypt: Egyptian Justice on Trial—The Case of the Cairo 52 // International Gay and Lesbian Human Rights Commission, 15 октября 2001 г., http://www.iglhrc.org/cgi-bin/iowa/article/takeaction/partners/692.html.

к китайской версии акции протеста…
Andrew Jacobs. Chinese Government Responds to Call for Protests // New York Times, February 20,
2011, http://www.nytimes.com/2011/02/21/world/asia/21china.html?_r=1.

ополчились на участниц кампании…
Rights Group Decries Flogging Sentence for Female Saudi Driver // CNN, 27 сентября 2011 г., http://articles.cnn.com/2011-09-27/middleeast/world_meast_saudi-arabia-flogging_1_flogging-sentence-women2drive-saudi-woman?_s=PM:MIDDLEEAST.

Когда стало известно об этом приговоре…
Там же;
Amnesty International (AI). Flogging Sentence for Saudi Arabian Woman After Driving 'Beggars Belief', пресс-релиз, 27 сентября 2011

г., https://www.amnesty.org/en/for-media/press-releases/flogging-sentence-saudi-arabian-woman-after-driving-%E2%80%9Cbeggars-belief%E2%80%9D-2011-0.

заставила правительство отменить свое решение…
Saudi King Revokes Flogging of Female Driver // CNN, 29 сентября 2011 г., http://www.cnn.com/2011/09/28/world/meast/saudi-arabia-flogging/index.html.

с запретом сатирического короткометражного фильма…
Принц аль-Валид бин Талал аль-Сауд, из беседы с авторами, февраль 2011 г.;
Faisal J. Abbas. Monopoly: The Saudi Short-Film Which Went a Long Way // Huffington Post, 9 сентября 2011 г., http://www.huffingtonpost.com/faisal-abbas/monopoly-the-saudi-shortf_b_969540.html.

Фильм под названием «Монополия» (Monopoly) появился на YouTube…
Принц аль-Валид бин Талал аль-Сауд, из беседы с авторами, февраль 2011 г. Фильм появился и в Facebook, и на YouTube. Принц говорил о Facebook.

собрал более миллиона просмотров…
Там же.

а по количеству просмотров роликов на YouTube — в мире…
Saudi Arabia Ranks First in You-Tube Views // Al Arabiya, 22 мая 2012 г., http://english.alarabiya.net/articles/2012/05/22/215774.html;
Simon Owens. Saudi Satire Ignites YouTube’s Massive Growth in Middle East // U.S. News, 30 мая 2012 г., http://www.usnews.com/news/articles/2012/05/30/saudi-satire-ignites-youtubes-massive-growth-in-middle-east.

наиболее динамичный мобильный рынок на Земле…
African Mobile Observatory 2011: Driving Economic and Social Development Through Mobile Services, Groupe Speciale Mobile (GSM), 9,

ссылка по состоянию на 17 октября 2011 г., http://www.gsma.com/publicpolicy/wp-content/uploads/2012/04/africamobileobservatory2011-1.pdf.

«Интернет хорош как средство для “выпускания пара”…»
Премьер-министр Ли Сяньлун, из беседы с авторами, ноябрь 2011 г.

в молодости все люди хотят быть частью какого-то классного движения…
Уверенность премьер-министра Ли Сяньлуна в том, что молодые люди хотят быть «классными», поддерживает Тина Розенберг, анализируя стратегию движения «Отпор», которое использовало эту же потребность молодежи и обучало своим методам представителей оппозиционных групп во всем мире. Примеры «фактора классности» движения «Отпор» см. в Rosenberg, Join the Club, p. 223–224, 229, 256–258, 260, 276.

«карригейт»…
Shamim Adam. Singapore Curry Protest Heats Up Vote with Facebook Campaign // Bloomberg, 19 августа 2011 г., http://www.bloomberg.com/news/2011-08-18/singapore-curry-protest-heats-up-vote.html;
Singaporeans to Launch Largest ‘Protest’ over ‘Currygate’ Incident // TR Emeritus (blog), 21 августа 2011 г., http://www.tremeritus.com/2011/08/21/singaporeans-to-launch-largest-protest-over-currygate-incident/.

«Китайский эмигрант и сингапурец индийского происхождения поссорились из-за карри…»
Премьер-министр Ли Сяньлун, из беседы с авторами, ноябрь 2011 г.

почти миллиард жителей…
Michael Kan, International Data Group (IDG) News Service. China’s Internet Population Reaches 538 Million // 19 июля 2012 г., PCWorld, http://www.pcworld.com/article/259482/chinas_internet_population_reaches_538_million.html;

к моменту выхода книги в Китае проживали более 1,3 млрд человек, поэтому оставалось предоставить доступ к сети еще 800 млн. Мы учли прогнозы относительно темпов роста населения в ближайшие десять лет и увеличили эту оценку почти до миллиарда человек. По данным доклада Комитета защиты журналистов за 2012 г., наиболее жесткая цензура применяется в Эритрее, на втором месте — Северная Корея.

«Происходящее в Китае полностью не контролирует никто…»
Премьер-министр Ли Сяньлун, из беседы с авторами, ноябрь 2011 г.

«История революций — это история долго копившегося недовольства…»
Генри Киссинджер, из беседы с авторами, декабрь 2011 г.

Назад к тексту

Глава 5. Будущее терроризма

уязвимость перед кибертерроризмом…
С точки зрения тактики есть много общего между кибертерроризмом и действиями хакеров, отличаются они обычно только мотивами. Террористы, скорее, ближе к наркоторговцам.

американские патрули больше всего боятся самодельных бомб…
Капитан армии США, служащий в Ираке, из беседы с авторами, ноябрь 2009 г.

СВУ образца 2009 года были дешевле и совершеннее…
Там же.

когда-то казавшиеся сложными и неоправданно дорогими…
Впервые один из авторов услышал об этом во время совместного выступления с Джонатаном Пауэрсом в Высшей школе международной политики имени Джона Хопкинса в 2005 г. Позднее это подтвердили многочисленные рассказы гражданских и военных участников кампании в Ираке.

назвал «феноменом творца»…
Энди Рубин, из беседы с авторами, февраль 2012 г.

твиттер сомалийской повстанческой группировки «Аль-Шабааб»…
Will Oremus. Twitter of Terror // Slate, 23 декабря 2011 г., http://www.slate.com/articles/technology/technocracy/2011/12/al_shabaab_twitter_a_somali_militant_group_unveils_a_new_social_media_strategy_for_terrorists_.html.

недавнее убийство Анвара аль-Авлаки, радикального американского проповедника…
Profile: Anwar al-Awlaki // Anti-Defamation League (ADL), версия ноября 2011 г., http://www.adl.org/main_Terrorism/anwar_al-awlaki.htm.

многие и состоявшиеся, и потенциальные террористы называли его своим вдохновителем…
Pierre Thomas, Martha Raddatz, Rhonda Schwartz and Jason Ryan. Fort Hood Suspect Yells Nidal Hasan's Name in Court // ABC Blotter, 29 июля 2011 г., http://abcnews.go.com/Blotter/fort-hood-suspect-naser-jason-abdo-yells-nidal-hasan/story?id =14187568#.UIIwW8VG-8C;
Bruce Hoffman. Why al Qaeda Will Survive // Daily Beast, 30 октября 2011 г., http://www.thedailybeast.com/articles/2011/09/30/al-awlaki-s-death-nothing-more-than-a-glancing-blow-al-qaeda-stronger-than-everest.html.

наиболее нетерпимо настроенные к Западу, религиозные деятели Саудовской Аравии…
Принц аль-Валид бин Талал аль-Сауд, из беседы с авторами, февраль 2012 г.

Мы разместили пропагандистские материалы у офисов Motorola…
Маджид Наваз, из беседы с авторами, февраль 2012 г.

внимание охранников одной из колумбийских тюрем в Медельине привлекла одиннадцатилетняя девочка…
Colombia Catches Girl 'Smuggling 74 Mobiles into Jail // BBC, 6 февраля 2011 г., http://www.bbc.co.uk/news/world-latin-america-12378390.

В Бразилии заключенные выдрессировали почтовых голубей…
Pigeons Fly Mobile Phones to Brazilian Prisoners // Telegraph (London), 30 марта 2009
г., http://www.telegraph.co.uk/news/newstopics/howaboutthat/5079580/Pigeons-fly-mobile-phones-to-Brazilian-prisoners.html.

местный бандит заплатил какому-то подростку…
Associated Press (AP). Police: Brazilian Teen Used Bow and Arrow to Launch Illegal Cell Phones over Prison Walls // Fox News, 2 сентября 2010 г., http://www.foxnews.com/world/2010/09/02/police-brazilian-teen-used-bow-arrow-launch-illegal-cell-phones-prison-walls/.

стоимость контрабандного смартфона…
Бывший член лос-анджелесской банды, из беседы с авторами, апрель 2012 г.

Афганистан, где уровень проникновения связи один из самых низких в мире…
Mobile-Cellular Subscriptions; Percentage of Individuals Using the Internet // International Telecommunication Union (ITU), ICT Data and Statistics (IDS), ссылка по состоянию на 19 октября 2012 г., http://www.itu.int/ITU-D/ict/statistics/.

ежегодно гибли десятки тысяч политзаключенных…
Авторы узнали об этом на встрече с участием персонала тюрьмы в феврале 2009 г. (материалы не являются секретными).

«нервный центр» афганских террористов…
Rod Nordland and Sharifullah Sahak. Afghan Government Says Prisoner Directed Attacks // New York Times, 10 февраля 2011 г., http://www.nytimes.com/2011/02/11/world/asia/11afghan.html?_r=1&scp=3&sq=pul%20e%20charki&st=cse.

В 2008 году в Третьем блоке произошел бунт заключенных…
Джаред узнал о террористической ячейке, существовавшей в «Пуль-э-Чарки», во время встреч и интервью, которые он провел в тюрьме в феврале 2009 г. (материалы не являются секретными);
см. также Joshua Philipp. Corruption Turning Afghan Prisons into Taliban Bases: Imprisoned Taliban Leaders Coordinate Attacks from Within Prison Walls // Epoch Times, 29 августа 2011 г., http://www.theepochtimes.com/n2/world/corruption-turning-afghan-prisons-into-taliban-bases-60910.html.

В ответ на шутливую просьбу дать номер телефона Аджи…
Мулла Акбак Аджи, из беседы с Джаредом Коэном, февраль 2009 г.

Вскоре после этого последовала серия хакерских атак…

Anonymous (Internet Group) // New York Times, версия от 8 марта 2012 г., http://topics.nytimes.com/top/reference/timestopics/organizations/a/anonymous_internet_group/index.html.

отомстить всем…
Sean-Paul Correll. Operation: Payback Broadens to Operation Avenge Assange // Pandalabs (блог), 6 декабря 2010 г., http://pandalabs.pandasecurity.com/operationpayback-broadens-to-operation-avenge-assange/;
Mathew Ingram. WikiLeaks Gets Its Own 'Axis of Evil' Defense Network // GigaOM (блог), 8 декабря 2010 г., http://gigaom.com/2010/12/08/wikileaks-gets-its-own-axis-of-evil-defence-network/.

Началось международное расследование…
U.S. Department of Justice. Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks // Национальный пресс-релиз, 19 июля 2011 г., http://www.fbi.gov/news/pressrel/press-releases/sixteen-individuals-arrested-in-the-united-states-for-alleged-roles-in-cyber-attacks;
Andy Greenberg. Fourteen Anonymous Hackers Arrested for 'Operation Avenge Assange,' LulzSec Leader Claims He's Not Affected // Forbes, 19 июля 2011 г., http://www.forbes.com/sites/andygreenberg/2011/07/19/anonymous-arrests-continue-lulzsec-leader-claims-hes-not-affected/;
Hackers Arrested in US, NL and UK // Radio Netherlands Worldwide, 20 июля 2011 г., http://www.rnw.nl/english/bulletin/hackers-arrested-us-nl-and-uk.

известно из его электронного письма в New York Times…
Somini Sengupta. Hacker Rattles Security Circles // New York Times, 11 сентября 2011 г., http://www.nytimes.com/2011/09/12/technology/hacker-rattles-internet-security-circles.html?pagewanted=all&_r=0.

Comodohaker действительно смог подделать 500 сертификатов интернет-безопасности…
Там же.

была взломана переписка…
Там же.

По его словам, он атаковал…
Там же.

заявлял, что «ненавидит Израиль»…
I Will Finish Israel Off Electronically: Ox-Omar // Emirates 24/7, 22 января 2012 г., http://www.emirates247.com/news/world/i-will-finish-israel-off-electronically-ox-omar-2012-01-22-1.438856.

файл с данными о 400 тысячах кредитных карт…
Chloe Albanesius. Hackers Target Israeli Stock Exchange, Airline Web Sites // PC Magazine, 16 января 2012 г., http://www.pcmag.com/article2/0,2817,2398941,00.asp.

они дублировали друг друга…
Isabel Kershner. Cyberattack Exposes 20,000 Israeli Credit Card Numbers and Details About Users // New York Times, 6 января 2012 г., http://www.nytimes.com/2012/01/07/world/middleeast/cyberattack-exposes-20000-israeli-credit-card-numbers.html.

утверждал, что входит в группировку хакеров-ваххабитов…
Jonathon Blakeley. Israeli Credit Card Hack // deLiberation, 5 января 2012 г., http://www.deliberation.info/israeli-credit-card-hack/.

«Можно будет повеселиться…»
Ehud Kenan. Saudi Hackers Leak Personal Information of Thousands of Israelis // YNet, 3 января 2012 г., http://www.ynetnews.com/articles/0,7340,L-4170465,00.html.

была нарушена работа израильской авиакомпании El Al и фондовой биржи…
Isabel Kershner. 2 Israeli Web Sites Crippled as Cyberwar Escalates // New York Times, 16 января 2012

г., http://www.nytimes.com/2012/01/17/world/middleeast/cyber-attacks-temporarily-cripple-2-israeli-web-sites.html.

если Израиль извинится за «геноцид» против палестинцев…
Yaakov Lappin. 'I Want to Harm Israel,' Saudi Hacker Tells 'Post' // Jerusalem Post, 16 января 2012 г., http://www.jpost.com/NationalNews/Article.aspx?id=253893; Saar Haas. 'OxOmar' Demands Israeli Apology // YNet, 16 января 2012 г., http://www.ynetnews.com/articles/0,7340,L-4176436,00.html?utm_source=dlvr.it&utm_medium=twitter.

«удостоился чести стать мишенью кибертеррористов»…
Страница Дэнни Аялона в Facebook, посты от 13 и 16 января 2012 г., ссылка по состоянию на 20 октября 2012 г., https://www.facebook.com/DannyAyalon.

DARPA одобрило заключение восьми контрактов…
Austin Wright. With Cyber Fast Track, Pentagon Funds Hacker Research // Politico, 7 декабря 2011 г., http://www.politico.com/news/stories/1211/70016.html.

«демократических инноваций с использованием краудсорсинга»
Statement by Dr. Regina E. Dugan, submitted to the Subcommittee on Terrorism, Unconventional Threats and Capabilities of the House Armed Services Committee, United States House of Representatives, 23 марта 2010 г., www.darpa.mil/Work Area/DownloadAsset.aspx?id =542.

хакеры и члены группы Anonymous — все как один злодеи…
Регина Даган, из беседы с авторами, июль 2012 г.

отсутствие интернета на его вилле…
Mark Mazzetti and Helene Cooper. Detective Work on Courier Led to Breakthrough on bin Laden // New York Times, 2 мая 2011 г., http://www.nytimes.com/2011/05/02/world/asia/02reconstruct-capture-osama-bin-laden.html;

Bob Woodward. Death of Osama bin Laden: Phone Call Pointed U.S. to Compound—and to ‘The Pacer’ // Washington Post, 6 мая 2011 г., http://www.washingtonpost.com/world/national-security/death-of-osama-bin-laden-phone-call-pointed-us-to-compound-and-to-the-pacer/2011/05/06/AFnSVaCG_story.html.

Но когда бойцы шестого отряда «морских котиков» захватили дом…
Joby Warrick. Al-Qaeda Data Yield Details of Planned Plots // Washington Post, 5 мая 2011 г., http://www.washingtonpost.com/world/national-security/al-qaeda-data-yields-details-of-planned-plots/2011/05/05/AFFQ3L2F_story.html.;
Woodward. Death of Osama bin Laden, http://www.washingtonpost.com/world/national-security/death-of-osama-bin-laden-phone-call-pointed-us-to-compound-and-to-the-pacer/2011/05/06/AFnSVaCG_story.html.

теракт в Мумбаи…
Hari Kumar. India Says Pakistan Aided Planner of Mumbai Attacks // New York Times, 27 июня 2012 г., http://www.nytimes.com/2012/06/28/world/asia/india-says-pakistan-aided-abu-jindal-in-mumbai-attacks.html;
Harmeet Shah Singh. India Makes Key Arrest in Mumbai Terror Plot // CNN, 26 июня 2012 г., http://articles.cnn.com/2012-06-26/asia/world_asia_india-terror-arrest_1_fahim-ansari-ujjwal-nikam-sabauddin-ahmed?_s=PM:ASIA;
Mumbai Attacks ‘Handler’ Arrested in India // Agence France-Presse (AFP), 25 июня 2012 г., http://www.google.com/hostednews/afp/article/ALeqM5gydBxOITFOjQ_gQjs278EF2DTvIQ?docId=CNG.1ec8f11cdfb59279e03f13dafbcd927a.01.
Чтобы лучше понять роль, которую в теракте 2008 г. в Мумбаи сыграли технологии, мы встретились с Пракашем Шуклой, старшим вице-президентом и техническим директором компании Taj Hotels Resorts and Palaces, которая управляет отелем Taj Mahal. По его словам, «из просмотра записей с камер видеонаблюдения было очевидно, что эти люди никогда в отеле не были. Однако они совершенно точно

знали, как по нему передвигаться, где что находится и т. д. Старая часть отеля была построена более ста лет назад, у нас даже нет поэтажных планов. Но благодаря нашему сайту в сочетании с картами Google можно очень хорошо представить его устройство. Еще на сайте указано расположение номеров премиум-класса: они находятся на верхних этажах здания. Террористам было очень легко спланировать нападения на такие известные цели, как Taj, Oberoi, железнодорожный вокзал и т. д. Все это плюс разведка Дэвида Хедли, которую он провел в Индии, дало террористам очень хорошее представление о месте проведения теракта. Начав действовать, они сразу направились в старое крыло (с номерами премиум-класса) и начали подниматься на верхние этажи. У них были спутниковые радиотелефоны. Они совершили несколько денежных переводов при помощи электронных платежных систем и использовали индийские предоплаченные SIM-карты».

Крупномасштабные теракты в отелях приведут к изменениям в системе безопасности всей отрасли гостеприимства. Шукла рассказал, что «отели идут по пути авиакомпаний. В нашей отрасли вводятся те же меры, что и в аэропортах: проверка багажа и паспортов. В частности, с Taj четыре года работала группа израильских специалистов, консультируя нас по вопросам создания системы безопасности, которая предотвратила бы подобные атаки. В 2008 г. у нас имелась охрана, но она не была вооружена. Теперь мы знаем, что полиция повела себя неадекватно ситуации — к тому моменту, когда прибыли коммандос и группа спецназа, с момента начала теракта прошло более двенадцати часов. Новая архитектура безопасности состоит из нескольких компонентов. Проверка: всех гостей из списка прибывающих проверяют, их фамилии сообщают в службу безопасности; по прибытии проверяют документы; сотрудников службы безопасности обучили внимательно следить за всеми, кто входит в отель; сканируется весь багаж; регулярно проводятся тренировки и отрабатывается поведение в случае чрезвычайной ситуации; персонал следит за обстановкой; часть вооруженных сотрудников службы безопасности одеты в штатское; все они проходят месячную стажировку в Израиле, где учатся обращаться с огнестрельным оружием и разрешать конфликты. На реализацию всех

этих мер мы потратили довольно значительные средства и знаем, что наш отель представляет собой более трудную цель, чем конкуренты, так что более-менее мы уверены в том, что нападение не повторится. Однако ситуация меняется. Развиваемся не только мы, но и наши враги, поэтому нам приходится внедрять инновации и постоянно совершенствовать систему безопасности».

террористы полагались на базовые общедоступные технологии…
Jeremy Kahn. Mumbai Terrorists Relied on New Technology for Attacks // New York Times, 8 декабря 2008 г., http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html; Damien McElroy. Mumbai Attacks: Terrorists Monitored British Websites Using BlackBerry Phones // Telegraph (London), 28 ноября 2008 г., http://www.telegraph.co.uk/news/worldnews/asia/india/3534599/Mumbai-attacks-Terrorists-monitored-coverage-on-UK-websites-using-BlackBerry-phones-bombay-india.html.

по «электронным следам»…
Global Lessons from the Mumbai Terror Attacks // Investigative Project on Terrorism (IPT), 25 ноября 2009 г., http://www.investigativeproject.org/1539/global-lessons-from-the-mumbai-terror-attacks.

об одном из высокопоставленных руководителей «Аль-Каиды»…
Член шестого отряда «морских котиков» США, из беседы с авторами, февраль 2012 г.

была похищена канадская журналистка Аманда Линдаут…
Canadian Amanda Lindhout Freed in Somalia // CBC (Ottawa), версия от 25 ноября 2009 г., http://www.cbc.ca/news/world/story/2009/11/25/amanda-lindhout-free.html.

похитители…
Аманда Линдаут, из беседы с авторами, июль 2012 г.

По некоторым оценкам, 90% обладателей мобильных телефонов во всем мире…
Technology/Internet Trends, 18 октября 2007 г., Morgan Stanley (China Mobile 50K Survey), 7. Размещено в Scribd, http://www.scribd.com/doc/404905/Mary-Meeker-Explains-The-Internet.

в компьютере, принадлежавшем Усаме бен Ладену, нашли большое количество порнофильмов…
Scott Shane. Pornography Is Found in bin Laden Compound Files, U.S. Officials Say // New York Times, 13 мая 2011 г., http://www.nytimes.com/2011/05/14/world/asia/14binladen.html.

Секретариата общественной безопасности в Мехико…
Venu Sarakki et al.. Mexico's National Command and Control Center Challenges and Successes // 16th International Command and Control Research and Technology Symposium in Quebec, Canada, 21–23 июня 2011 г., http://www.dtic.mil/dtic/tr/fulltext/u2/a547202.pdf.

Идея заключалась в том, чтобы собрать все «транзакционные» данные…
Dr. John Poindexter. Overview of the Information Awareness Office // Заметки для конференции DARPATech 2002, 2 августа 2002 г., см. сайт Федерации американских ученых (FAS), http://www.fas.org/irp/agency/dod/poindexter.html.

законопроект о полном исключении расходов на ее реализацию…
Department of Defense Appropriations Act, 2004, S.1382, 108th Cong. (2003), см. раздел 8120; Department of Defense Appropriations Act, 2004, H.R.2658, 108th Cong. (2003) (представлен на подпись президенту), см. раздел 8131.

некоторые его проекты нашли пристанище…
Associated Press (AP). U.S. Still Mining Terror Data // Wired, 23 февраля 2004 г., http://www.wired.com/politics/law/news/2004/02/62390;

Michael Hirsh. Wanted: Competent Big Brothers // Newsweek and Daily Beast, 8 февраля 2006 г., http://www.thedailybeast.com/newsweek/2006/02/08/wanted-competent-big-brothers.html.

По оценкам специалистов, 52% населения Земли моложе 30 лет…
Mid-Year Population by Five Year Age Groups and Sex—World, 2011 // U.S. Census Bureau, International Data Base, ссылка по состоянию на 20 октября 2012 г., http://www.census.gov/population/international/data/idb/informationGateway.php.

победить терроризм смогут только две вещи…
Генерал Стэнли Маккристал, из интервью Сюзанне Кебл Killing the Enemy Is Not the Best Route to Success // Der Spiegel, 11 января 2010 г., http://www.spiegel.de/international/world/spiegel-interview-with-general-stanley-mcchrystal-killing-the-enemy-is-not-the-best-route-to-success-a-671267.html.

Ежедневно просматривается более четырех миллиардов роликов…
Alexei Oreskovic. Exclusive: YouTube Hits 4 Billion Daily Video Views // Reuters, 23 января 2012 г., http://www.reuters.com/article/2012/01/23/us-google-youtube-idUSTRE80M0TS20120123.

Назад к тексту

Глава 6. Будущее конфликтов, войн и иностранного военного вмешательства

«удерживают нас от насилия и заставляют сотрудничать с другими и проявлять альтруизм»…
Steven Pinker, The Better Angels of Our Nature: Why Violence Has Declined. New York: Viking, 2011, XXV.

«мир начинает выглядеть иначе…»
Там же, XXVI.

умышленно лишают примерно 2,2 млн этнических цыган…
Amnesty International (AI). Romania Must End Forced Evictions of Roma Families // пресс-релиз, 26 января 2010 г., http://www.amnesty.org/en/for-media/press-releases/romania-must-end-forced-evictions-roma-families-20100126.
Точно так же цыган преследуют во всей Восточной Европе и все чаще — в Западной тоже. В июле 2010 г. президент Николя Саркози возглавил кампанию по депортации цыган на их родину, в Болгарию и Румынию. В течение месяца было закрыто более 50 нелегальных лагерей, и к сентябрю депортировано свыше тысячи цыган. См. France Sends Roma Gypsies Back to Romania // BBC, 20 августа 2010 г., http://www.bbc.co.uk /news/world-europe-11020429;
France: Renewed Crackdown on Roma: End Discriminatory Roma Camp Evictions and Removals // Human Rights Watch (HRW), News, 10 августа 2010 г., http://www.hrw.org/news/2012/08/10/france-renewed-crackdown-roma; French Ministers Fume After Reding Rebuke Over Roma // BBC, 15 сентября 2010 г., http://www.bbc.co.uk/news/world-europe-11310560.

«Экстремистским группам и фанатикам-одиночкам запугивать своих жертв через интернет гораздо проще…
Кристиан Пиччолини, из беседы с авторами, апрель 2012 г.

Юлий Цезарь…

Julius Caesar. The Gallic Wars / translation by John Warrington with a preface by John Mason Brown and an introduction by the translator. Norwalk, Conn.: Easton Press, 1983; see also Dr. Neil Faulkner. The Official Truth: Propaganda in the Roman Empire // BBC, History, версия от 17 февраля 2011 г., http://www.bbc.co.uk/history/ancient/romans/romanpropaganda_article_01.shtml.

«Видео: израильский пилот ждет, чтобы район покинули мирные жители…»
Twitter-аккаунт @IDFspokesperson, 19 ноября 2012 г.

Неда Ага-Солтан:
Nazila Fathi. In a Death Seen Around the World, a Symbol of Iranian Protests // New York Times, 22 июня 2009 г., http://www.nytimes.com/2009/06/23/world/middleeast/23neda.html.

Эти ролики иранцы передавали друг другу…
Thomas Erdbrink. In Iran, a Woman Named Neda Becomes Opposition Icon in Death // Washington Post, 23 июня 2009 г., http://www.washingtonpost.com/wp-dyn/content/article/2009/06/22/AR2009062203041.html.

направляло в офисы радиостанций полицию…
Информация получена Джаредом Коэном при подготовке его книги One Hundred Days of Silence: America and the Rwanda Genocide. Lanham: Rowman & Littlefi eld Publishers, 2007; см. также Alison Liebhafsky. Des Forges, Leave None to Tell the Story: Genocide in Rwanda. New York: Human Rights Watch, 1999.

имена и адреса прятавшихся тутси передавали по радио…
The Media and the Rwanda Genocide / Allan Thompson, ed., with a statement by Kofi Annan. London: Pluto Press, 2007, p. 49, http://www.internews.org/sites/default/files/resources/TheMedia&TheRwandaGenocide.pdf.

практически «лежал» сайт службы по связям с общественностью НАТО…
Dan Verton. Serbs Launch Cyberattack on NATO // Federal Computer Week, 4 апреля 1999 г., http://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx.

По сведениям Тома Доуни, которые он привел в своей нашумевшей статье…
Tom Downey. China's Cyberposse // New York Times Magazine, 3 марта 2010 г., http://www.nytimes.com/2010/03/07/magazine/07Human-t.html.

страшный видеоролик…
Там же.

убийцу обнаружили…
Там же.

понадобилось всего шесть дней…
Там же.

закон (отмененный месяц спустя Конституционным советом страны)…
Scott Sayare. French Council Strikes Down Bill on Armenian Genocide Denial // New York Times, 28 февраля 2012 г., http://www.nytimes.com/2012/02/29/world/europe/french-bill-on-armenian-genocide-is-struck-down.html.

«расистским и дискриминационным»…
Turkey PM Says French Bill on Genocide Denial 'Racist' // BBC, 24 января 2012 г., http://www.bbc.co.uk/news/world-europe-16695133.

в точке сингулярности…
P. W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century. New York: Penguin Press, 2009, 102.

миссия DARPA…

DARPA. About, ссылка по состоянию на 9 октября 2012 г., http://www.darpa.mil/About.aspx; DARPA. Our Work, ссылка по состоянию на 9 октября 2012 г., http://www.darpa.mil/our_work/.

скучной, грязной и опасной работы…
Singer, Wired for War, 63.

компания iRobot, которая изобрела робот-пылесос Roomba…
Там же, 21–23.

Двух роботов PackBot использовали в 2011 г. на АЭС в Фукусиме…
Amar Toor. iRobot Packbots Enter Fukushima Nuclear Plant to Gather Data, Take Photos, Save Lives // Engadget, 18 апреля 2011 г., http://www.engadget.com/2011/04/18/irobot-packbots-enter-fukushima-nuclear-plant-to-gather-data-ta/.

Foster-Miller, выпускает конкурента PackBot…
Singer, Wired for War, 26.

Еще существуют беспилотные летательные аппараты…
Описание беспилотников Predator, Raven и Reaper см. в Singer, Wired for War, 32–35, 37, 116.

31% всех военных самолетов…
Spencer Ackerman and Noah Shachtman. Almost 1 in 3 U.S. Warplanes Is a Robot // Danger Room (blog), Wired, 9 января 2012 г., http://www.wired.com/dangerroom/2012/01/drone-report/.

на долю роботов будет приходиться больше операций с использованием огнестрельного оружия…
Гарри Уинго, из беседы с авторами, апрель 2012 г.

роботы SWORDS…
Singer, Wired for War, 29–32; Noah Shachtman. First Armed Robots on Patrol in Iraq (Updated) // Danger Room (блог), Wired, 2 августа 2007 г., http://www.wired.com/dangerroom/2007/08/httpwwwnational/.

как будут выглядеть боевые подразделения…
Военнослужащий отряда «морских котиков», из беседы с авторами, февраль 2012 г.

стратегический вопрос для них…
Питер Уоррен Сингер, из беседы с авторами, апрель 2012 г.

объединенной тактической системы радиосвязи…
Bob Brewin. Pentagon Shutters Joint Tactical Radio System Program Office // Nextgov, 1 августа 2012 г., http://www.nextgov.com/mobile/2012/08/pentagon-shutters-joint-tactical-radio-system-program-office/57173/;
Matthew Potter, Defense Procurement News. Joint Program Executive Office Joint Tactical Radio System (JPEO JTRS) Stands Down and Joint Tactical Networking Center (JTNC) Opens, пресс-релиз, 1 октября 2012 г., http://www.defenseprocurementnews.com/2012/10/01/joint-program-executive-office-joint-tactical-radio-system-jpeo-jtrs-stands-down-and-joint-tactical-networking-center-jtnc-opens-press-release/.

Такого рода вещи недопустимы…
Питер Уоррен Сингер, из беседы с авторами, апрель 2012 г.

В каком-то смысле армии помог спрос…
Там же.

Даже Венесуэла присоединилась к этому клубу…
Brian Ellsworth. Venezuela Says Building Drones with Iran's Help // Reuters, 14 июня 2012 г., http://www.reuters.com/article/2012/06/14/us-venezuela-iran-drone-idUSBRE85D14N20120614.

«Да, мы делаем это…»
Robert Beckhusen. Iranian Missile Engineer Oversees Chavez's Drones // Danger Room (blog), Wired, 18 июня 2012 г., http://www.wired.com/dangerroom/2012/06/mystery-cargo/.

побочные эффекты технологических новинок…
Регина Даган, из беседы с авторами, июль 2012 г.

все уже используют…
Питер Уоррен Сингер, из беседы с авторами, апрель 2012 г.

аренду БПЛА для слежки и разведки…
Singer, Wired for War, 265.

В 2009 году она подписала контракт с ЦРУ об оснащении бомбами…
James Risen and Mark Mazzetti. C.I.A. Said to Use Outsiders to Put Bombs on Drones // New York Times, 20 августа 2009 г., http://www.nytimes.com/2009/08/21/us/21intel.html.

Компании, обладающие недвижимостью, применяют беспилотники…
Somini Sengupta. Who Is Flying Drones over America? // Bits (блог), New York Times, 14 июля 2012 г., http://bits.blogs.nytimes.com/2012/07/14/who-is-flying-drones-over-america/.

в Университете Канзаса можно получить диплом…
Jefferson Morley. Drones Invade Campus // Salon, 1 мая 2012 г., http://www.salon.com/2012/05/01/drones_on_campus/.

«битва за контроль»…
Peter Warren Singer, quoted by Noah Shachtman. Insurgents Intercept Drone Video in King-Size Security // Danger Room (блог), Wired, 17 декабря 2009 г., http://www.wired.com/dangerroom/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/.

RQ-170 Sentinel…
Scott Peterson. Downed U.S. Drone: How Iran Caught the ‘Beast’ // Christian Science Monitor, 9 декабря 2011 г., http://www.csmonitor.com/World/Middle-East/2011/1209/Downed-US-drone-How-Iran-caught-the-beast.

«приземлиться там, где захотели…»
Scott Peterson and Payam Faramarzi. Exclusive: Iran Hijacked U.S. Drone, Says Iranian Engineer // Christian Science Monitor, 15 декабря 2011 г., http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video.

известна как «спуфинг…
Adam Rawnsley. Iran's Alleged Drone Hack: Tough, but Possible // Danger Room (блог), Wired, 16 декабря 2011 г., http://www.wired.com/dangerroom/2011/12/iran-drone-hack-gps/.

$6 млн…
Dan Murphy. Obama Taking Heat for Asking for U.S. Drone Back? Pay Little Heed // Christian Science Monitor, 15 декабря 2011 г., http://www.csmonitor.com/World/Backchannels/2011/1215/Obama-taking-heat-for-asking-for-US-drone-back-Pay-little-heed.

в результате утечек информации из правительства появились подробные статьи…
Daniel Klaidman. Drones: How Obama Learned to Kill // 28 мая 2012 г., Newsweek and Daily Beast, http://www.thedailybeast.com/newsweek/2012/05/27/drones-the-silent-killers.html;
Jo Becker and Scott Shane. Secret 'Kill List' Proves a Test of Obama's Principles and Will // New York Times, 29 мая 2012 г., http://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html;
David E. Sanger. Obama Order Sped Up Wave of Cyberattacks Against Iran // New York Times, 1 июня 2012 г., http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html;
Charlie Savage. Holder Directs U.S. Attorneys to Track Down Paths of Leaks // New York Times, 8 июня 2012 г., http://www.nytimes.com/2012/06/09/us/politics/holder-directs-us-attorneys-to-investigate-leaks.html?pagewanted=all.

с боснийской кампании 1990-х годов…
Siobhan Gorman, Yochi J. Dreazen and August Cole. Insurgents Hack U.S. Drones // Wall Street Journal, 17 декабря 2009 г., http://online.wsj.com/article/SB126102247889095011.html.

оказался изъятый у шиитских повстанцев в Ираке ноутбук…
Там же.

когда во время Первой мировой войны на полях сражений появился танк…
Питер Уоррен Сингер, из беседы с авторами, апрель 2012 г.

боролся с советскими танками…
Абдул Рахим Вардак, из беседы с авторами, июнь 2012 г.

«Наземные роботы, которых наши солдаты используют…»
Питер Уоррен Сингер, из беседы с авторами, апрель 2012 г.

Как бы поступили вы…
Там же.

«Обязанность защищать»…
Jayshree Bajoria. Libya and the Responsibility to Protect // Counsel on Foreign Relations, аналитический обзор, 24 марта 2011 г., http://www.cfr.org/libya/libya-responsibility-protect/p24480.

о храбром американце по имени Фред…
Ливийские министры, из беседы с авторами, июнь 2012 г.

одним из самых активных участников международных миротворческих миссий является Бангладеш…
Ranking of Military and Police Contributions to U.N. Operations // United Nations Peacekeeping, Resources, 31 августа 2012 г., http://www.un.org/en/peacekeeping/contributors/2012/august12_2.pdf.

Назад к тексту

Глава 7. Будущее возрождения страны

небольшая GSM-сеть для чиновников…
Apple’s iPhone and Afghanistan’s Taliban // Cellular-News (London), 13 февраля 2009 г., http://www.cellular-news.com/story/36027.php.

Саддам Хусейн полностью запретил мобильные телефоны…
W. David Gardner. For Sale: Iraq’s Cell-Phone Franchises // InformationWeek, 27 июля 2005 г., http://www.informationweek.com/news/166403218.

Стороны противостояния пользовались самыми простыми средствами связи…
Служащие ливийского министерства связи и информации, из беседы с авторами, июнь 2012 г.

с региональным оператором MTC-Vodafone…
Post-War Telecommunications Developments in Iraq // Office of Technology and Electronic Commerce, Research by Country/Region, ссылка по состоянию на 18 октября 2012 г. http://web.ita.doc.gov/ITI/itiHome.nsf/6502bd9adeb499b285256cdb00685f77/e781b255ae7a4f9a85256d9c0068abd9?OpenDocument.

MCI, получил одобрение на работу в Багдаде…
Там же.

вышки появились по всей стране…
Один из руководителей CPA, из беседы с авторами, январь 2011 г.

она находится на подъеме…
Iraq—Telecoms, Mobile, Broadband and Forecasts: Executive Summary, BuddeComm, ссылка по состоянию на 18 октября 2012 г., http://www.budde.com.au/Research/Iraq-Telecoms-Mobile-Broadband-and-Forecasts.html.

ООН организовала сеть сотовой связи…
Press Briefing by the U.N. Offices for Pakistan and Afghanistan // United Nations, News Centre, 16 января 2001 г., http://www.un.org/apps/news/infocus/afghanistan/infocusnews.asp?NewsID=136&sID=4.

в Афганистане было четыре крупных оператора…
Afghanistan—Telecoms, Mobile, Internet and Forecasts: Executive Summary, BuddeComm, ссылка по состоянию на 18 октября 2012 г. http://www.budde.com.au/Research/A fghanistan-Telecoms-Mobile-Internet-and-Forecasts.html.
По данным этого источника, в 2011 г. в Афганистане было 17,6 млн абонентов сотовой связи, при этом четыре крупнейших оператора «имели долю не менее 20% каждый». Отсюда мы сделали нашу консервативную оценку «примерно 15 млн».

связь заработала довольно быстро…
Tim Large. Cell Phones and Radios Help Save Lives After Haiti Earthquake // Reuters, 25 января 2010 г., http://www.reuters.com/article/2010/01/25/us-haiti-telecoms-idUSTRE60O07M20100125.

По сообщениям двух крупнейших сотовых операторов страны, Digicel и Voila…
Suzanne Choney. Firms Scramble to Repair Haiti Wireless Service // MSNBC, версия от 22 января 2010 г., http://www.msnbc.msn.com/id/34977823/ns/world_news-haiti/t/firms-scramble-repair-haiti-wireless-service/#.UIBq5MVG-8B.

восстановите вышки сотовой связи, включите связь…
Кэмерон Хьюм, из беседы с Джаредом Коэном, январь 2010 г.

А еще организовать охрану вышек…
Suzanne Choney. Firms Scramble to Repair Haiti Wireless Service // MSNBC, версия от 22 января 2010

г., http://www.msnbc.msn.com/id/34977823/ns/world_news-haiti/t/firms-scramble-repair-haiti-wireless-service/#.UIBq5MVG-8B.

Оперативное восстановление связи компанией Vodafone…
Statements—Vodafone Egypt // Vodafone, 29 января 2011 г. и 2 февраля 2011
г., http://www.vodafone.com/content/index/media/press_statements/statement_on_egypt.html.

«наши люди ночевали в технических центрах…»
Витторио Колао, из беседы с авторами, август 2012 г.

Roshan — не только крупнейший мобильный оператор в стране, но и лидер по объему инвестиций и уплаченных налогов…
Western Union and Roshan to Introduce International Mobile Money Transfer Service in Afghanistan // Roshan, News, 27 февраля 2012 г., http://www.roshan.af/Roshan/Media_Relations/News/News_Details/12-02-27/Western_Union_and_Roshan_to_Introduce_International_Mobile_Money_Transfer_service_in_Afghanistan.aspx.

Она дает работу тысячам афганцев…
Там же.

8% акций газеты New York Times…
Russell Adams. Carlos Slim Boosts Stake in New York Times Again // Wall Street Journal, 6 октября 2011 г., http://online.wsj.com/article/SB10001424052970203388804576615123528159748.html.

«Думаю, что тогда я был не столько ливанцем, сколько гражданином мира…»
Карлос Слим Хелу, из беседы с авторами, сентябрь 2011 г.

Возросшая популярность мобильных телефонов…

Abdi Sheikh and Ibrahim Mohamed. Somali Mobile Phone Firms Thrive Despite Chaos // Reuters, 3 ноября 2009 г., Africa edition, http://af.reuters.com/article/investingNews/idAFJOE5A20DB20091103;
Abdinasir Mohamed and Sarah Childress. Telecom Firms Thrive in Somalia Despite War, Shattered Economy // Wall Street Journal, 11 мая 2010 г., http://online.wsj.com/article/SB10001424052748704608104575220570113266984.html.

функционируют во всех трех регионах…
Somalia—Telecommunications Overview // Infoasaid, ссылка по состоянию на 18 октября 2012 г. http://infoasaid.org/guide/somalia/telecommunications-overview.

В Сомали всего один коммерческий банк…
Mohamed Odowa. Rebuilding Trust in Somali Commercial Banking // Somalia Report, 15 мая 2012 г., http://www.somaliareport.com/index.php/post/3347/Rebuilding_Trust_in_Somali_Commercial_Banking; Dinfin Mulupi. Opening a Bank in Somalia? Not a Crazy Idea, Says Businessman // How We Made It in Africa (Cape Town), 18 июня 2012 г., http://www.howwemadeitinafrica.com/why-we-decided-to-open-a-bank-in-somalia/17530/.

благодаря услуге мобильного перевода…
Sahra Abdi. Mobile Transfers Save Money and Lives in Somalia // Reuters, 3 марта 2010 г., http://www.reuters.com/article/2010/03/03/us-somalia-mobiles-idUSTR E6222BY20100303.

сотовый оператор из Бахрейна попытался расширить…
Cynthia Johnston, Reuters. U.S. Authority Tells Batelco to End Iraq Cellular Service // Arab News (Jeddah), 27 июля 2003 г., http://www.arabnews.com/node/234902.

Проникновение мобильной связи в Сомали гораздо выше…
Представители правительства Сомали, из беседы с авторами, октябрь 2012 г. Следует заметить, что официальная сомалийская статистика

иногда показывает меньшие значения.

Пираты на сомалийском побережье…
Jama Deperani. Somali Pirate Rules and Regulations // Somalia Report, 8 октября 2011 г., http://www.somaliareport.com/index.php/post/1706.

В докладе Совета безопасности ООН, опубликованном в 2012 году…
Security Council Committee on Somalia and Eritrea Adds One Individual to List of Individuals and Entities, United Nations Security Council SC/10545, 17 февраля 2012 г., http://www.un.org/News/Press/docs/2012/sc10545.doc.htm.

список из десяти функций государства…
Ashraf Ghani and Clare Lockhart, Fixing Failed States: A Framework for Rebuilding a Fractured World. New York: Oxford University Press, 2008, p. 124–166.

были созданы три комиссии…
Work Package 7 on Reparations, Report of Workshop II: The Interactions between Mass Claims Processes and Cases in Domestic Courts, Impact of International Courts on Domestic Criminal Procedures in Mass Atrocity Cases (DOMAC) and Amsterdam Center for International Law, 18 июня 2010 г. См. раздел Питера ван дер Ауверарта в Panel Three: Iraq Reparation Schemes, с. 27–31, http://www.domac.is/media/domac/Workshop-II-report-Final.pdf.

Параллельно появился специальный орган…
Там же, см. Discussion of the Cassation Commission, с. 28 и 30.

Однако, несмотря на благие намерения…
Там же, с. 29–31.

Представители сомалийской диаспоры…
France Lamy. Mapping Towards Crisis Relief in the Horn of Africa // Google Maps, 12 августа 2011 г., http://google-latlong.blogspot.com/2011/08/mapping-towards-crisis-relief-in-horn.html.

Журналистка Наоми Клейн…
Naomi Klein. The Shock Doctrine: The Rise of Disaster Capitalism. New York: Metropolitan Books/Henry Holt, 2007.

погибли сотни тысяч человек…
Paul Farmer Examines Haiti 'After the Earthquake' // NPR, 12 июля 2011 г., http://www.npr.org/2011/07/12/137762573/paul-farmer-examines-haiti-after-the-earthquake.

Власти страны утверждают…
Haiti // New York Times, версия от 26 августа 2012 г., http://topics.nytimes.com/top/news/international/countriesandterritories/haiti/index.html.

из попавшего в распоряжение СМИ американского правительственного доклада…
Emily Troutman. US Report Queries Haiti Quake Death Toll, Homeless // Agence France-Presse (AFP), 27 мая 2011 г., http://www.google.com/hostednews/afp/article/ALeqM5jELhQRaWNNs56GOlifagC5F4DSZg?docId=CNG.699dc08a5f873f53071a317e008a7a5b.3a1.

кампании «SMS-помощи»…
Lindsey Ellerson. Obama Administration Texting Program Has Raised $5 Million for Red Cross Haiti Relief // ABC News, 14 января 2010 г., http://abcnews.go.com/blogs/politics/2010/01/obama-administration-texting-program-has-raised-5-million-for-red-cross-haiti-relief/.

было собрано свыше $43 млн.…
Elizabeth Woyke. Yes, You Can Still Donate Money to Haiti via Your Cellphone // Forbes, 12 января 2011 г., http://www.forbes.com/sites/elizabethwoyke/2011/01/12/yes-you-can-still-donate-money-to-haiti-via-your-cellphone/.

«Телеком без границ»…

Adele Waugaman. Telecoms Sans Frontieres' Emergency Response, доклад в Госдепартаменте США, посвященный землетрясению в Гаити, 9 июля 2010 г., United Nations Foundation and Vodafone Foundation, http://www.unfoundation.org/assets/pdf/haiti-earthquake-tsf-emergency-response-1.pdf; Tom Foremski, Telecoms Sans Frontieres—How a Simple Phone Call Helps in Haiti // Silicon Valley Watcher, 4 февраля 2010 г., http://www.siliconvalleywatcher.com/mt/archives/2010/02/telecoms_sans_f.php.

AlertNet, проект фонда Thompson Reuters Foundation…
Thomson Reuters. Thomson Reuters Foundation Launches Free Information Service for Disaster-Struck Population in Haiti: Text Your Location to 4636 to Register // пресс-релиз, 17 января 2010 г., http://thomsonreuters.com/content/press_room/corporate/TR_Foundation_launches_EIS.

Финансовая помощь от институциональных доноров…
Jose de Cordoba. Aid Spawns Backlash in Haiti // Wall Street Journal, 12 ноября 2010 г., http://online.wsj.com/article/SB10001424052702304023804575566743115456322.html;
Ingrid Arnesen. In Haiti, Hope Is the Last Thing Lost // Wall Street Journal, 12 января 2011 г., http://online.wsj.com/article/SB10001424052748704515904576076031661824012.html.

сотни тысяч жителей Гаити…
William Booth. NGOs in Haiti Face New Questions about Effectiveness // Washington Post, 1 февраля 2011 г., http://www.washingtonpost.com/wp-dyn/content/article/2011/02/01/AR2011020102030.html.

специалистами, которые извлекли из него важные уроки…
See Paul Farmer, Haiti After the Earthquake. New York: PublicAffairs, 2012.

модель работы международных благотворительных организаций, вероятно, изменится…
О росте количества НКО см. Jessica T. Mathews. Power Shift // Foreign Affairs, январь/февраль 1997 г., http://www.foreignaffairs.com/articles/52644/jessica-t-mathews/power-shift.

70% собранных пожертвований были направлены на «производственные нужды»…
Aly Weisman. Invisible Children Respond to #StopKony Viral Video Criticisms // The Wire, Business Insider, 8 марта 2012 г., http://www.businessinsider.com/invisible-children-respond-to-stopkony-viral-video-criticisms-2012-3.

странный случай…
Sarah Grieco. Invisible Children Co-founder Detained: SDPD // NBC 7 San Diego, 17 марта 2012 г., http://www.nbcsandiego.com/news/local/jason-russell-san-diego-invisible-children-kony-2012-142970255.html.

Системы мониторинга и оценки, которые помогают повысить ответственность и выявить недостатки благотворительных организаций, уже появились…
В первую категорию попадают GuideStar, Charity Navigator, GiveWell, CharityWatch, Philanthropedia, GreatNonprofits и другие организации. Их основная цель заключается в том, чтобы доноры делали более информированные пожертвования. Методы разные: от простого аккумулирования налоговой отчетности различных НКО (GuideStar) до сбора и обработки данных благотворительных организаций с последующим анализом результатов их усилий (GiveWell). И хотя это необыкновенно ценная информация, мы подозреваем, что пользуется этим меньшинство фондов и частных лиц — те, кто жертвует значительные суммы. Доклад под названием Money for Good подтверждает наши опасения: оказалось, что только 35% людей изучают вопрос, прежде чем сделать пожертвование, да и те в основном задают вопросы самой организации. См. Money for Good II: Driving Dollars to the Highest Performing Nonprofits, Summary Report

2011 // Hope Consulting, ноябрь 2011 г., с. 9–10, http://www.guidestar.org/ViewCmsFile.aspx?ContentID =4040. Есть еще «зонтичные» благотворительные организации вроде InterAction, но у них в лучшем случае пара сотен членов, притом что в этой сфере работают десятки тысяч НКО.

Ярким примером является работа проекта Ushahidi…
Jason Palmer. Social Networks and the Web Offer a Lifeline in Haiti // BBC, 15 января 2010 г., http://news.bbc.co.uk/2/hi/8461240.stm;
How Does Haiti Communicate after the Earthquake? // BBC, 20 января 2010 г., http://news.bbc.co.uk/2/hi/technology/8470270.stm.

волонтеры Ushahidi из США…
James F. Smith. Tufts Map Steered Action amid Chaos // Boston Globe, 5 апреля 2010 г., http://www.boston.com/news/world/latinamerica/articles/2010/04/05/tufts_project_delivered_aid_to_quake_victims/?page=1;
Jessica Ramirez. 'Ushahidi' Technology Saves Lives in Haiti and Chile // Newsweek and Daily Beast, 3 марта 2010 г., http://www.thedailybeast.com/newsweek/blogs/techtonic-shifts/2010/03/03/ushahidi-technology-saves-lives-in-haiti-and-chile.html.

«Крыша обрушилась, но я еще жив»…
Ramirez. 'Ushahidi' Technology Saves Lives in Haiti and Chile, http://www.thedailybeast.com/newsweek/blogs/techtonic-shifts/2010/03/03/ushahidi-technology-saves-lives-in-haiti-and-chile.html.

Roshan запустила пилотную программу…
Eltaf Najafi zada and James Rupert. Afghan Police Paid by Phone to Cut Graft in Anti-Taliban War // Bloomberg, 13 апреля 2011 г., http://www.bloomberg.com/news/2011-04-13/afghan-police-now-paid-by-phone-to-cut-graft-in-anti-taliban-war.html.

Если кому-то нужна срочная помощь, он ее получит…
Поль Кагаме, из беседы с авторами, сентябрь 2011 г.

его размер оценивается в $1 млрд в год…
Aditi Malhotra. The Illicit Trade of Small Arms // Geopolitical Monitor (Toronto), Backgrounder, 19 января 2011 г., http://www.geopoliticalmonitor.com/the-illicit-trade-of-small-arms-4273/.

в Мали, в руках воинственных туарегов…
Michel Moutot, Agence France-Presse (AFP). West's Intervention in Libya Tipped Mali into Chaos: Experts // Google News, 5 апреля 2012 г., http://www.google.com/hostednews/afp/article/ALeqM5hJtUvEGQfS0X5Lip5M2Z7MOJIgkw?docId=CNG.90655ad2d0483083880b2914c0ec5599.251.

демилитаризацию десятков тысяч бывших солдат…
Reintegration Program: Reflections on the Reintegration of Ex-Combatants, Multi-Country Demobilization and Reintegration Program (MDRP), сентябрь — октябрь 2008 г., http://www.mdrp.org/PDFs/MDRP_DissNote5_0908.pdf.

«Мы считаем, что те, кто воевал, смогут изменить свою жизнь, только если мы дадим им инструменты»…
Поль Кагаме, из беседы с авторами, сентябрь 2011 г.

больше $380 млн…
Frederick Womakuyu. South Sudan: Nation Embarks on Disarming Ex-Combatants // AllAfrica, 12 июля 2011 г., http://allafrica.com/stories/201107130081.html.

200 тысяч человек…
Там же.

В Колумбии очень успешно реализуется программа разоружения, демобилизации и реабилитации…
Наблюдения авторов в ходе двух посещений программы в Колумбии.

«группам борцов за права человека и торжество правосудия стоит разработать…»
Найджел Сноад, из беседы с авторами, март 2012 г.

Десятки преступников…
Report of the International Criminal Court, Sixty-Sixth Session, United Nations General Assembly, 19 августа 2011 г., 6–7, http://www.icc-cpi.int/NR/rdonlyres/D207D618-D99D-49B6-A1FC-A1A221B43007/283906/ICC2011AnnualReporttoUNEnglish1.pdf.

прежде чем начнется рассмотрение их дела…
Susana SaCouto, Katherine Cleary et al. Expediting Proceedings at the International Criminal Court // American University, Washington College of Law, War Crimes Research Office, International Criminal Court, Legal Analysis and Education Project, июнь 2011 г., http://www.wcl.american.edu/warcrimes/icc/documents/1106report.pdf.

новые власти страны…
Reconciliation After Violent Conflict: A Handbook, International Institute for Democracy and Electoral Assistance (International IDEA), 2003. See section by Peter Uvin. The Gacaca Tribunals in Rwanda, 116–117, ссылка по состоянию на 19 октября 2012 г., http://www.idea.int/publications/reconciliation/upload/reconciliation_full.pdf.

В «гакакских» трибуналах…
Там же.

Назад к тексту

Заключение

это эволюционный процесс…
Ray Kurzweil. The Age of Spiritual Machines: When Computers Exceed Human Intelligence. New York: Viking, 1999, 32.

Каждые два дня…
M. G. Siegler. Eric Schmidt: Every 2 Days We Create as Much Information as We Did up to 2003 // TechCrunch, 4 августа 2010 г.

лишь два миллиарда человек…
The World in 2010: ICT Facts and Figures // ITU News, декабрь 2010 г., http://www.itu.int/net/itunews/issues/2010/10/04.aspx.

из семи…
U.S. & World Population Clocks // U.S. Cesus Bureau, ссылка по состоянию на 26 октября 2012 г., http://www.census.gov/main/www/popclock.html.

Назад к тексту

[1] Гордон Мур — основатель корпорации Intel. *Прим. ред.*

[2] Слово «смартфон» (англ. *smart phone*) дословно переводится как «умный», «интеллектуальный» телефон. *Прим. перев.*

[3] Chief Executive Officer (англ.) — высшая исполнительная должность в компании. В принятой в России иерархии аналог генерального директора. *Прим. ред.*

[4] Неврологическое заболевание, проявляющееся длительной болью и онемением пальцев рук. Развивается при монотонных сгибательно-разгибательных движениях кисти. *Прим. ред*

[5] «Особое мнение» — фантастический триллер Стивена Спилберга. *Прим. ред*.

[6] Шведский музыкальный сервис. *Прим. ред*.

[7] Слава южнокорейской звезды K-попа Psy достигла планетарных масштабов практически мгновенно после того, как созданный исполнителем видеоролик на его песню Gangnam Style побил рекорд по количеству просмотров за три месяца. *Прим. авт. Далее особо отмечаются только примечания редактора и переводчика, примечания автора даны без оговорки.*

[8] В американских и европейских больницах роботизированные хирургические комплексы уже используются в ходе операций.

[9] Статуи Будды, входившие в комплекс буддийских монастырей в Бамианской долине (Афганистан), в 2001 году были разрушены талибами как памятники язычества. *Прим. ред.*

[10] Выходила на русском языке: Левитт С., Дабнер С. Фрикономика. М. : Манн, Иванов и Фербер, 2011. *Прим. ред*.

[11] Большинство таких методов относятся к группе инструментов поисковой оптимизации (SEO). Чаще всего, чтобы повлиять на механизм ранжирования результатов выдачи поисковых систем, используют создание позитивного контента, содержащего целевые слова (например, имя человека), многочисленных ссылок на него и частое обновление содержимого. В результате поисковые «пауки», скорее всего, будут идентифицировать этот материал как популярный и новый, тем самым сдвигая ниже в результатах поиска старые и менее релевантные материалы. На рейтинг также может влиять использование популярных ключевых слов и обратных ссылок на «раскрученные» сайты. Все это вполне законно и морально приемлемо. Однако у поисковой оптимизации есть и оборотная сторона — «черная SEO», которая включает в себя попытки манипулирования рейтингом при помощи незаконных или аморальных методов, скажем, причинение вреда чужому контенту (к примеру, путем привязки его с помощью ссылок к подозрительным сайтам, в частности содержащим детскую порнографию), добавление скрытого текста или маскировка сайта (это когда поисковым роботам показывают одну его версию, а конечным пользователям — другую).

[12] Считается, что впервые эту максиму сформулировал Стюарт Брэнд, основатель и редактор Whole Earth Catalog, в ходе Первой хакерской конференции, состоявшейся в 1984 г.

[13] Подробнее о Джулиане Ассанже и WikiLeaks можно прочитать в книге: Ассанж Д. Неавторизованная биография. М. : Альпина Бизнес Букс, 2012.

[14] Хотя в программистском сообществе термин «хакер» означает человека, создающего что-то быстро и спонтанно, мы используем здесь это слово в его привычном значении — «взломщик компьютерных систем».

[15] Вот один из твитов, которые написал в Twitter пакистанский IT-консультант Сохаиб Атхар в ночь операции по уничтожению бен Ладена: «Над Абботтабадом в час ночи летает вертолет (такое нечасто бывает)».

[16] Уотергейтский скандал — политический скандал в США (1972–1974), вызванный раскрытием попытки установить подслушивающую аппаратуру в отеле «Уотергейт», где располагалась штаб-квартира Демократической партии, и закончившийся досрочной отставкой президента страны республиканца Р. Никсона. *Прим. ред*.

[17] Упреждающий анализ — молодая наука на стыке статистики, глубинного исследования данных и компьютерного моделирования. По сути, речь идет об использовании имеющихся данных для составления полезных прогнозов будущего. Например, специалисты по упреждающему анализу могут, имея данные о пассажиропотоке нью-йоркского метро, предсказать, сколько поездов потребуется выпустить на линии в каждый конкретный день с учетом времени года, уровня безработицы и прогноза погоды. *Прим. ред.*

[18] Впервые на практике этот закон был применен в Техасе в 2008 г., когда одна женщина подала коллективный судебный иск против компании Blockbaster, без разрешения передавшей информацию о приобретенных и просмотренных ею фильмах рекламодателю. Дело закончилось мировым соглашением.

[19] В США уже были случаи, когда правонарушения в киберпространстве трактовались как «посягательство на движимое имущество».

[20] Технология носимых устройств отчасти похожа на недавно возникшую тактильную технологию, но это не одно и то же. Тактильными называются устройства, воздействующие на органы осязания пользователя, часто путем вибрации или нажатия. В носимых устройствах часто используются тактильные элементы, но не только они (например, светящаяся в темноте велосипедная куртка), и не все тактильные устройства являются носимыми.

[21] William J. Dobson. The Dictator’s Learning Curve. New York, 2012. *Прим. ред.*

[22] Интернет-Балканы, как мы их называем, — не то же самое, что интранеты. В интранетах используются те же интернет-протоколы, но в рамках сети одной организации или местного сообщества, а не сети из множества сетей. Корпоративные интранеты часто защищены от несанкционированного доступа извне при помощи межсетевых экранов и других средств безопасности.

[23] Несколько внешне незначительных инцидентов говорят о том, что власти могут время от времени изменять маршрутизацию DNS и без колебаний делают это. Уже много раз, набрав адрес Google, некоторые пользователи мистическим образом попадали на сайт ее китайского конкурента www.Baidu.com.

[24] Мы различаем «кибератаку» и «кибертерроризм» в зависимости от того, кто за ними стоит — индивидуум или организация, а также по их мотивам. Однако и то и другое может проявляться одинаково, например в случае экономического шпионажа.

[25] Когда мы спросили бывшего руководителя израильской разведки Меира Дагана об этом сотрудничестве, единственное, что он ответил, — «вы и правда думаете, я вам расскажу?»

[26] Ларри Константин, профессор Университета Мадейры в Португалии, усомнился в данных Сангера в интервью, которое он 4 сентября 2012 г. дал Стивену Черри, заместителю главного редактора IEEE Spectrum, журнала Института инженеров по электротехнике и электронике США, заявив, что Stuxnet физически не мог распространяться так, как это описывал Сангер (поскольку червь мог перемещаться лишь по локальной компьютерной сети, но не по интернету). Мы считаем, что аргумент Константина силен настолько, что заслуживает как минимум обсуждения.

[27] В конечном счете в ходе одной из таких кибератак китайские власти обязательно будут пойманы за руку. Конечно, если этот случай рассмотрит Совет безопасности ООН, никакую резолюцию принять не удастся, учитывая имеющееся у Китая право вето, однако понятно, что геополитические последствия будут серьезными.

[28] Здесь нужно сделать важное уточнение. Для проведения DoS- или DDoS-атак чаще всего неважно, находятся ли взломанные компьютеры внутри сети, ставшей целью злоумышленников, или вне ее. Но это важно в случае промышленного шпионажа, когда целью является сбор информации: в таких случаях компьютеры должны быть внутри сети.

[29] Tina Rosenberg. Join the Club: How Peer Pressure Can Transform the World. New York — London, 2011. *Прим. ред*.

[30] В ходе выделения характеристик автоматически идентифицируется наличие, отсутствие или состояние интересующих исследователя характеристик выбранного набора данных. В данном случае ключевыми характеристиками могут быть уровень качества текста, частота появления эмоциональных слов и количество упомянутых автором людей, что позволяет выявить степень его независимости.

[31] В этом посте компании Renesys, специализирующейся на анализе интернета, был приведен поразительный график практически мгновенного отключения египетских интернет-провайдеров от глобальной сети.

[32] В блокировке интернет-провайдеров было сделано всего одно исключение — для компании Noor Group, оказывавшей услуги нескольким крупным организациям вроде Египетской фондовой биржи и Египетского кредитного бюро. Она работала без ограничений еще три дня.

[33] Египетский режим славился своей жестокостью по отношению к подпольному гей-сообществу. Известен случай, когда полиция нравов провела облаву в плавучем ночном клубе Queen Boat и арестовала 55 человек, в результате несколько десятков из них обвинили в хулиганстве и отправили за решетку.

[34] От weibo — так китайцы называют микроблоги. *Прим. ред*.

[35] Томас Джефферсон (1743–1826) — один из отцов-основателей США и авторов Декларации независимости. *Прим. ред.*

[36] Кибертеррористы скрывают свои следы, действуя через несколько компьютеров-посредников. Источником атаки жертвам кажутся промежуточные звенья (зачастую это взломанные домашние и офисные компьютеры в разных точках мира). Первое звено цепи отследить довольно трудно: для этого нужно пробиться через множество промежуточных звеньев. Более того, хакер может запустить на какой-то из взятых им под контроль машин Tor-маршрутизатор, способный активно генерировать отвлекающий трафик из взломанной сети, тем самым маскируя действия взломщика.

[37] Может оказаться, что это не так легко выполнить. Все зависит от преступника. Когда был осужден Кевин Митник, известный хакер, он провел пять лет в тюрьме, а затем вышел досрочно, и на время испытательного срока ему было запрещено пользоваться интернетом и мобильным телефоном. Но он все же добился отмены этого ограничения через суд.

[38] Если платформы вроде WikiLeaks и группы хакеров имеют дело с информацией, засекреченной различными правительствами, они как минимум занимаются шпионажем или поощряют его.

[39] Как и многие другие, компания Google создает бесплатные инструменты, которые могут применять все желающие. Поэтому она постоянно ищет способы снизить риски того, что этими инструментами воспользуются с целью причинить вред другим.

[40] Steven Pinker. The Better Angels of Our Nature, 2011. *Прим. ред*.

[41] Если для израильских ультраортодоксальных сил будет сделано такое исключение по религиозным основаниям, не станет ли это прецедентом? А если следующими станут ультраконсервативные салафиты из Египта с требованием свести интернет к определенному набору сайтов?

[42] Полицейские называют это «эффектом CNN». Чаще всего его связывают с американским военным вмешательством в Сомали в 1992–1993 гг. Распространено мнение, что решение президента Джорджа Буша направить в страну войска было спровоцировано показанными по телевидению кадрами голодающих и отчаявшихся сомалийцев, но, когда 3 октября 1993 г. в Могадишо погибли 18 американских рейнджеров и двое
военнослужащих коалиционных сил из Малайзии, после чего тело одного из американцев протащили по улицам города, что также попало в телеэфир, военный контингент США был из Сомали выведен.

[43] Недавно заработал проект Storyful, который выполняет эту функцию для многих крупных новостных агентств. В нем работают бывшие журналисты, которые тщательно изучают материалы социальных сетей (например, проверяют, совпадает ли погода на размещенном в YouTube ролике с фактическими данными о погоде, зарегистрированными в этот день в городе, где предположительно он был снят).

[44] Peter Singer. Wired for War: The Robotics Revolution and Conflict in the 21st Century. New York, 2009. *Прим. ред*.

[45] Компьютерные фанаты не забудут роли этой организации в создании интернета. Правда, тогда она называлась «Агентство передовых исследований» (ARPA).

[46] Двух роботов PackBot использовали в 2011 г. на АЭС в Фукусиме, где произошла авария после землетрясения и цунами: они перемещались по разрушенному заводу, куда из-за высокого уровня радиации было слишком опасно входить спасателям, и собирали информацию при помощи видеокамер и специальных датчиков.

[47] Слова Сингера подтвердили несколько военнослужащих спецназа, с которыми мы разговаривали на эту тему.

[48] Тако — традиционное блюдо мексиканской кухни; состоит из кукурузной или пшеничной лепешки с разнообразной начинкой. *Прим. ред.*

[49] Эти трудности усугубляло то, что штаб-квартира миссии располагалась в бывшем дворце Саддама Хусейна, превращенном диктатором-параноиком в систему непроницаемых для электронных волн бункеров.

[50] Мы использовали список из десяти функций государства, приведенный в книге «Возрождение несостоятельных государств» Клэр Локхарт и Ашрафа Гани, основателей Института эффективности государства. (Fixing Failed States, by Clare Lockhart and Ashraf Ghani. New York, 2009. *Прим. ред*.)

[51] Журналистка Наоми Клейн в своей провокационной книге «Шоковая доктрина» (The Shock Doctrine) дала таким людям прозвище «эксплуататоры катастроф». Клейн утверждает, что защитники неолиберальных экономических принципов стремятся воспользоваться посткризисной ситуацией для насаждения идеи свободного рынка, обычно делая это в ущерб существующему экономическому порядку. По аналогии с «шоковой терапией», которая используется в психиатрии, эти фундаменталисты свободного рынка цепляются за возможность начать с, как им кажется, чистого листа и насильно изменить экономическую среду.

[52] Оценки количества погибших во время землетрясения в Гаити разнятся очень сильно. Власти страны утверждают, что погибло 316 000 человек, но из попавшего в распоряжение СМИ американского правительственного доклада известно, что это число находится в диапазоне от 46 190 до 84 961.

[53] Paul Farmer. Haiti After the Earthquake. New York, 2011. *Прим. ред.*

[54] Пробация — вид условного осуждения в США, когда осужденный на время испытательного срока, установленного судом, находится под надзором специальных органов. *Прим. ред*.

[55] Ray Kurzweil. The Age of Spiritual Machines: When Computers Exceed Human Intelligence. New York, 1999. *Прим. ред*.

[56] Эксабайт — единица измерения информации, равная 1018. *Прим. ред*.

Над книгой работали

Ответственный редактор *Юлия Потемкина*
Редактор *Татьяна Собко*
Дизайн *Сергей Хозин*
Верстка *Вячеслав Лукьяненко*
Корректоры *Лев Зелексон, Юлия Молокова*

ООО «Манн, Иванов и Фербер»
mann-ivanov-ferber.ru
facebook.com/mifbooks
Электронная версия книги
подготовлена компанией Webkniga, 2013
webkniga.ru

Максимально полезные книги от издательства «Манн, Иванов и Фербер»

Заходите в гости: http://www.mann-ivanov-ferber.ru/

Наш блог: http://blog.mann-ivanov-ferber.ru/

Мы в Facebook: http://www.facebook.com/mifbooks

Мы ВКонтакте: http://vk.com/mifbooks

Предложите нам книгу: http://www.mann-ivanov-ferber.ru/about/predlojite-nam-knigu/

Ищем правильных коллег: http://www.mann-ivanov-ferber.ru/about/job/

СОДЕРЖАНИЕ