Security Engineering: часть 14. Политика безопасности

Published: 02.07.2026 09:44 | Updated: 08.07.2026 10:45

Политика безопасности, террор и свобода: Анализ угроз и реакций общества

Эпоха чрезмерных реакций

Атаки 11 сентября 2001 года оказали глубокое влияние на мир информационной безопасности и глобальную политику. Как отметил Усама бен Ладен, «Аль-Каида» потратила на организацию атак около 500 тысяч долларов, тогда как США в результате самих событий и их последствий потеряли, по самым скромным оценкам, более 500 миллиардов долларов. Современный терроризм во многом работает за счет провоцирования государства на чрезмерные и иррациональные реакции.
Этот феномен порождает ряд критических вопросов для общества и инженеров по безопасности:

1. **Политический вопрос.** Уязвимы ли западные открытые общества с демократией и свободной прессой именно из-за своей открытости? Ответы на террористические угрозы часто приводят к авторитарным мерам: дактилоскопии в аэропортах, введению удостоверений личности, тотальной слежке и задержаниям без суда, что подрывает вековые традиции верховенства права.
2. **Экономический вопрос.** Колоссальные средства тратятся на меры безопасности с нулевой или минимальной эффективностью. Например, США потратили более 14 миллиардов долларов на досмотр пассажиров в аэропортах, не поймав ни одного террориста. При этом укрепление дверей в кабинах пилотов, которое могло бы устранить основную угрозу, обошлось бы в fraction (долю) от этой суммы, однако «невидимые» меры не приносят политических дивидендов.

3. **Проблема «военно-промышленного комплекса безопасности».** После 11 сентября возник стремительный рост корпораций, лоббирующих интересы в сфере безопасности, что напоминает оборонную промышленность времен Холодной войны.
4. **Манипуляция техническими аргументами.** Технические доводы часто используются для оправдания плохой политики. Например, в Великобритании срок задержания подозреваемых без суда увеличивали, аргументируя это необходимостью расшифровки данных с компьютеров. В реальности же проблема заключалась в банальной нехватке переводчиков с сомалийского языка, что можно было решить иначе.
5. **Эффект домино.** Политика в области киберпространства сместилась в сторону слежки, цензуры и экспортного контроля, что напрямую затрагивает гражданские свободы и приватность.

Терроризм: Эволюция и природа политического насилия

Исторический контекст

Политическое насилие не является новшеством; антропологи находят свидетельства племенных войн у ранних людей и шимпанзе. Террор использовался для подавления подданных еще майя, инками и Вильгельмом Завоевателем. В более поздней истории можно вспомнить Гая Фокса (Пороховой заговор 1605 года) или Ирландскую республиканскую армию (ИРА). Примечательно, что граница между террористом и государственным деятелем часто размыта. Многие лидеры, использовавшие насилие в борьбе за свои цели, впоследствии стали главами государств: Джерри Адамс, Менахем Бегин, Шарль де Голль, Джомо Кениата и Нельсон Мандела.

Причины политического насилия

Первая хорошая новость заключается в том, что общий тренд на террористическое насилие неуклонно снижается. Исследование Пола Коллиера и Анке Хеффлер, проведенное для Всемирного банка, проанализировало войны с 1960 по 1999 год, чтобы определить, что движет конфликтами: «обиды» (неравенство, отсутствие политических прав, этнические разделения) или «жажда наживы» (экономическая жизнеспособность повстанцев).

Данные убедительно показывают, что обиды играют незначительную роль. Восстания определяются тем, могут ли они быть финансово обеспечены. Как отмечал еще Цицерон: «Бесконечные деньги — это нервы войны».

- Кампания ИРА продолжалась благодаря поддержке Советского блока и ирландских эмигрантов в США. Когда этот поток иссяк, оружие было сложено.
- Конфликт в Сьерра-Леоне подпитывался «кровавыми алмазами».
- Восстание тамильских тигров в Шри-Ланке финансировалось диаспорой в США и Индии.
- «Аль-Каида» спонсировалась богатыми донорами из стран Персидского залива.

Вывод для безопасности: наиболее эффективный способ борьбы с повстанцами — перекрыть их финансовые потоки.

Психология политического насилия

Люди склонны игнорировать вероятности, когда в дело вступают эмоции (эвристика аффекта). Ужасающие события, такие как теракты, заставляют общество переоценивать риски.
Эксперимент, проведенный с 22 муниципальными судьями в Тусоне (штат Аризона), показал влияние «смертельной осведомленности» (mortality salience). Судьям предложили определить размер залога для проститутки, страдающей наркотической зависимостью. Половине судей beforehand задали вопросы, заставляющие их задуматься о собственной смерти. Результат: судьи, которым напомнили о смертности, назначили залог в среднем 455 долларов, тогда как контрольная группа — всего 50 долларов. Осознание конечности жизни заставляет людей строже придерживаться культурных норм и агрессивнее защищать свое мировоззрение. Атаки 11 сентября, напомнив о смерти, спровоцировали всплеск религиозности, патриотизма и, как обратную сторону, предрассудков.

Роль политических институтов

Почему правительства принимают иррациональные решения? Ответ дает «экономика общественного выбора» (public-choice economics), основанная Джеймсом Бьюкененом (лауреат Нобелевской премии). Политики стремятся максимизировать шансы на переизбрание, а чиновники — расширить свои империи и бюджеты.
Например, первоначальной реакцией Великобритании на 11 сентября было

увеличение бюджета MI5. Однако это не принесло «политического мяса» промышленному комплексу безопасности. В результате средства были перенаправлены на грандиозный и дорогостоящий проект внедрения национальных удостоверений личности. Аналогичным образом, вторжение в Ирак многие аналитики рассматривали как способ обеспечить загрузку Пентагона и оборонной промышленности, которые остались не у дел после успешной, но короткой войны в Афганистане.

Роль прессы

Средства массовой информации живут по принципу «If it bleeds, it leads» (Если это кровоточит, это идет на первую полосу). Редакторы хотят продавать больше газет и транслировать самые пугающие версии событий, тем самым усиливая панику и позволяя политикам диктовать повестку дня, держа оппонентов в обороне.

Демократический ответ и обучение общества

Несмотря на мрачные тенденции, демократические общества способны учиться на ошибках. Общественная реакция на взрывы в лондонском метро 7 июля 2005 года была гораздо более сдержанной по сравнению с реакцией на 11 сентября в США — во многом благодаря опыту четвертивековой борьбы с ИРА.
Историк Джон Мюллер показывает, как менялось отношение американских администраций к терроризму:

- **Джимми Картер** раздул кризис с заложниками в Иране, что дало ему первоначальный рост рейтингов, но в итоге стоило ему президентства.
- **Рональд Рейган** в основном игнорировал провокации, но поддался искушению в случае с ливанскими заложниками (скандал «Иран-контрас»), после чего быстро восстановил рейтинг, дистанцировавшись от ошибки.
- **Джордж Буш** использовал политику, основанную на страхе, что в конечном итоге привело к падению популярности.

Избиратели со временем видят сквозь страх. Политики, пытающиеся использовать терроризм для запугивания и получения голосов, в долгосрочной перспективе сталкиваются с общественным отторжением.

Наблюдение (Surveillance)

Одним из побочных эффектов событий 11 сентября 2001 года стало колоссальное увеличение масштабов технического наблюдения как путем прослушки, так и через интеллектуальный анализ коммерческих данных государственными агентствами. Недавние раскрытия фактов незаконного наблюдения в ряде стран, наряду с различиями в подходах США и Европы к конфиденциальности, политизировали эти вопросы. Прослушка и так была острой темой в 1990-х годах, и о ней были написаны миллионы слов.

История правительственной прослушки

Правители всегда пытались контролировать коммуникации. В классические времена курьеры проверялись на таможнях, а со Средних веков многие короли либо управляли почтовой монополией, либо предоставляли ее фаворитам. «Черные кабинеты» (Black Chambers) — службы перехвата и дешифровки почты раннего Нового времени — описаны в фундаментальной истории Дэвида Кана. Изобретение электронных коммуникаций вызвало ответную защитную реакцию. В большей части Европы телеграфная служба была создана как часть Почтового ведомства и всегда находилась в государственной собственности. Даже там, где это было не так, регулирование было настолько жестким, что рост отрасли сильно тормозился, что оставило Америку с явным конкурентным преимуществом. Множество национальных правил, которые иногда конфликтовали друг с другом, настолько раздражали всех, что в 1865 году был создан Международный телеграфный союз (ITU). Однако это не удовлетворило всех: в Британии телеграфная индустрия была национализирована Гладстоном в 1869 году.
Изобретение телефона еще больше усилило интерес правительства к слежке и сопротивление ей — как юридическое, так и техническое. В 1928 году Верховный суд США в деле Olmstead vs United States постановил, что прослушка не нарушает положения Четвертой поправки о незаконном обыске и конфискации, поскольку не было физического проникновения в жилище. Судья Брандейс знаменито выступил с особым мнением. В 1967 году суд изменил свою позицию в деле Katz vs United States, постановив, что поправка защищает людей, а не места. В следующем году Конгресс легализовал федеральную прослушку (в «Титуле III» Закона о всеобъемлющем контроле над преступностью и безопасности на улицах) после свидетельств о масштабах организованной преступности. В 1978 году, после расследования злоупотреблений администрации Никсона, Конгресс принял Закон о надзоре в сфере внешней

разведки (FISA), который регулирует прослушку в целях национальной безопасности. В 1986 году Закон о защите электронных коммуникаций (ECPA) ослабил положения о ордерах Титуля III.
К началу 1990-х годов распространение дерегулированных услуг — от мобильных телефонов до переадресации вызовов — начало подрывать способность властей осуществлять прослушку, чему также способствовали технические новшества, такие как канальная сигнализация и адаптивное эхоподавление в модемах. Поэтому в 1994 году был принят Закон о содействии правоохранительным органам в области связи (CALEA), который обязал все телекоммуникационные компании сделать свои сети доступными для прослушки способами, одобренными ФБР. К 1999 году в США было легально прослушано 2 450 000 линейных дней, что в среднем составляло чуть более 1350 одновременных прослушек, санкционированных судебными ордерами.

DES как инструмент политики

АНБ продвигало стандарт DES (с его 56-битным ключом) не просто как отраслевой стандарт, но и как целенаправленный политический инструмент. Идея заключалась в том, чтобы воспрепятствовать иностранным правительствам внедрять стойкую криптографию. АНБ создавало иллюзию, что обладает вычислительными мощностями для взлома DES, что вынуждало другие страны продолжать использовать уязвимые роторные машины, трафик которых АНБ могло свободно перехватывать и читать.

Растущие споры вокруг анализа трафика

Однако основная масса полицейской коммуникационной разведки в развитых странах поступает не от перехвата контента, а от анализа телефонных счетов и других данных о связях. Преступники идут на большие ухищрения, чтобы скрыть свои сигналы в безобидном трафике, используя такие методы, как одноразовые мобильные телефоны и взлом АТС, а полиция, в свою очередь, разрабатывает методы отслеживания сетей контактов.
Это не ново. Правители давно использовали свой контроль над почтовыми службами для отслеживания корреспондентов подозреваемых, даже если сами письма не вскрывались. Изобретение почтовых марок в 1840 году стало шагом вперед для конфиденциальности, так как оно сделало отправку письма анонимно намного проще. Некоторые страны настолько опасались угрозы подстрекательства и клеветы, что принимали законы, требующие указания обратного адреса на обратной стороне конверта. Развитие телеграфа, напротив, стало шагом вперед для слежки: поскольку сообщения регистрировались по

отправителю, получателю и количеству слов, можно было составлять сводки трафика, которые, как выяснилось, были эффективным индикатором экономической активности. Первая мировая война показала комбатантам ценность разведданных, которые можно было получить, прослушивая объем вражеского радиотрафика, даже если его не удавалось расшифровать. Последующие конфликты только закрепили это.
Анализ трафика продолжает обеспечивать основную массу полицейской коммуникационной разведки. Например, в США в 1998 году (последний год, за который были доступны сопоставимые статистические данные) было одобрено 1350 заявок на прослушку, в то время как было подано 4886 судебных повесток (плюс 4621 продление) на использование регистраторов вызовов (устройств, записывающих все номера, набранные с конкретной телефонной линии) и 2437 повесток (плюс 2770 продлений) на устройства ловушки и трассировки (которые записывают идентификатор вызывающей линии входящих вызовов, даже если вызывающий абонент пытается его заблокировать). Иными словами, повесток на получение данных о связях было более чем в десять раз больше, чем на прослушку контента. Более того, эти данные были еще более неполными, чем данные о прослушке. Тенденция последних лет — даже до 11 сентября — заключалась в переходе на использование повесток для получения детализации счетов в базах данных телефонных компаний, а не в получении данных регистраторов вызовов непосредственно с коммутатора (чему способствовал CALEA). Например, Bell Atlantic сообщила, что за период с 1989 по 1992 год она ответила на 25 453 повестки или судебных ордера на получение детализации счетов 213 821 своего клиента, в то время как NYNEX сообщила, что обработала 25 510 повесток, касающихся не установленного числа клиентов, только в 1992 году. В масштабах страны это предполагает, что, возможно, полмиллиона клиентов ежегодно подвергаются изъятию своих записей, и что данные о трафике собираются примерно в сто раз большем количестве случаев, чем применяется прослушка.

Незаконное наблюдение

В 2006 году выяснилось, что слухи были верны. Компания AT&T действительно передавала АНБ записи о звонках миллионов американцев; целью агентства было «создать базу данных каждого звонка, когда-либо совершенного в пределах национальных границ», чтобы оно могло картировать всю социальную сеть США для «Войны с террором». По всей видимости, эти данные теперь собирались для 200 миллионов клиентов AT&T, Verizon и BellSouth, трех крупнейших телефонных компаний страны. Программа началась вскоре после 11 сентября. Компания Qwest не сотрудничала, потому что ее генеральный

директор в то время, Джо Наччио, не верил утверждениям АНБ о том, что Qwest не нужен судебный ордер (или одобрение по FISA). АНБ оказывало давление на Qwest, угрожая лишить ее засекреченных контрактов, а юристы Qwest просили АНБ передать свое предложение в суд FISA. АНБ отказалось, заявив, что суд может с ними не согласиться.
Позже выяснилось, что АНБ оказывало давление на Qwest с целью передачи данных еще до 11 сентября. В октябре 2007 года демократические сенаторы получили дальнейшее подтверждение, когда Verizon призналась им, что передавала ФБР данные о звонках второго поколения своих клиентов по письмам национальной безопасности 720 раз с 2005 года; а в ноябре 2007 года Washington Post раскрыла, что АНБ прослушивало множество чисто внутренних телефонных звонков и данных о трафике, а также перехватывало трафик на узле пиринга AT&T в Сан-Франциско, чтобы получить доступ к интернет-трафику.
Записи телефонных и компьютерных услуг могут быть предоставлены другим органам, кроме правоохранительных, в соответствии с 18 USC 2703; так, например, видно, что Вирджиния и Мэриленд планируют использовать данные отслеживания мобильных телефонов для мониторинга заторов на Capital Beltway.
Использование данных о трафике в маркетинговых целях также прямо предусматривалось Конгрессом при принятии этого закона. Однако растущая доступность записей мобильных телефонов теперь сделала их доступными и для преступников, что позволяет гангстерам отслеживать цели и выяснять, не звонил ли кто-то из их сообщников в полицию.

Доступ к поисковым запросам и данным о местоположении

Одна проблема заключается в том, что данные о связях и контент становятся все более взаимосвязанными, поскольку то, что является контентом на одном уровне абстракции, часто является данными о связях на другом. Люди могут думать, что URL — это просто адрес страницы, которую нужно получить, но URL, такой как `http://www.google.com/search?q=marijuana+cultivation+UK`, содержит термины, введенные в поисковую систему, а также ее имя. Очевидно, что некоторые полицейские хотели бы получить список всех, кто отправил такой запрос. Не менее очевидно, что предоставление такого рода данных полиции в больших масштабах окажет охлаждающее воздействие на онлайн-дискурс.
В США Министерство юстиции отправило судебную повестку ряду поисковых систем с требованием передать два полных месяца поисковых запросов, а также все URL в их индексе, заявив, что эти данные нужны для подкрепления своих утверждений о том, что Закон о защите детей в интернете не нарушает конституцию и что фильтрация может быть эффективной против детской порнографии. AOL, Microsoft и Yahoo тихо подчинились, но Google воспротивился.

Судья постановил, что Министерство не получит поисковых запросов, а только случайную выборку из 50 000 URL, которые оно изначально запрашивало.
В Британии правительство пыталось определить URL как данные о трафике, когда оно проталкивало законопроект RIP через парламент, и новости о том, что полиция будет иметь неограниченный доступ к URL, которые вводит каждый пользователь (их кликам), вызвали общественный протест против «Большого Браузера», и определение коммуникационных данных было урезано. Для общего интернет-трафика это означает IP-адреса, но также включает адреса электронной почты. Все это может быть затребовано простым уведомлением от старшего полицейского.
С телефонной системой связаны еще более тонкие моменты. В Британии вся информация о местоположении мобильных телефонов считается данными о трафике, и чиновники получают ее легко; но в США Апелляционный суд постановил в 2000 году, что когда полиция получает ордер на местоположение мобильного телефона, достаточно указать соту, в которой он активен, и что требование триангуляции устройства (толкование, которого хотела полиция) нарушит конфиденциальность. Кроме того, даже информация о местоположении с точностью до соты не была бы доступна по более низким стандартам, применяемым к повесткам на регистраторы вызовов. Повестки также были признаны недостаточными для пост-отсеченных набранных цифр, так как нет способа заранее отличить цифры, набранные для маршрутизации вызовов, от цифр, набранных для доступа или предоставления информации. На практике это означает, что если подозреваемый заходит в магазин 7-Eleven и покупает телефонную карту на несколько долларов, полиция не может получить список его звонков без полного ордера на прослушку. Все, что они могут получить по повестке, — это цифры, которые он набирает для связи с оператором телефонной карты, а не цифры, которые он набирает позже для соединения.

Интеллектуальный анализ данных (Data Mining)

Анализ данных о звонках — это лишь один аспект гораздо более широкой проблемы: сопоставление данных правоохранительных органов, то есть обработка данных из множества источников. Самый ранний серьезный пример использования данных из нескольких источников, о котором знает общественность, произошел в Германии в конце 1970-х годов для поиска безопасных домов, используемых террористической группой Баадер-Майнхоф. Следователи искали арендованные квартиры с нерегулярными пиками потребления коммунальных услуг, за которые платили путем удаленного банковского перевода из серии различных мест. Это сработало: был получен список из нескольких сотен квартир, среди которых было несколько безопасных

домов. Инструменты для выполнения такого рода анализа теперь поставляются вместе с рядом продуктов, используемых для анализа трафика и управления крупными полицейскими расследованиями. Степень, в которой они используются, зависит от местного нормативного климата; в Великобритании были споры из-за доступа полиции к базам данных рецептов, выписанных фармацевтами, в то время как в США врачи обеспокоены тем, как часто личная медицинская информация вызывается повестками от страховых компаний следователями. Существуют также практические ограничения, накладываемые стоимостью понимания множества проприетарных форматов данных, используемых коммерческими и государственными обработчиками данных. Но для полиции стало обычным делом иметь доступ, по крайней мере, к данным коммунальных услуг, таким как счета за электричество, которые анализируются для поиска производителей марихуаны.

Наблюдение через провайдеров: Carnivore и его потомки

Одним из крупных недавних событий стало навязчивое наблюдение через интернет-провайдеров (ISP). Перехват интернет-трафика сложнее, чем раньше было с голосовой связью; существует множество препятствий, таких как временные IP-адреса, назначаемые большинству клиентов, и все более распределенный характер трафика. В старые времена (скажем, в 2002 году) у провайдера могли быть модемные стойки и локальная сеть, где можно было разместить устройство прослушки; теперь многие клиенты подключаются через DSL, и провайдеры используют коммутируемые сети, которые часто не имеют очевидного места для установки перехватчика.
Во многих странах есть законы, требующие от провайдеров содействия прослушке, и обычным способом сделать это у крупного провайдера является наличие уже установленного оборудования, которое разделяет целевую сеть так, что копии интересующих пакетов отправляются в отдельную засекреченную сеть с оборудованием для прослушки. Небольшие провайдеры часто не имеют таких возможностей. В конце 1990-х годов ФБР разработало систему под названием Carnivore, которую они могли привозить к небольшим провайдерам, когда требовалась прослушка; это был ПК с программным обеспечением, которое можно было настроить на запись электронной почты подозреваемого или его веб-серфинга, или любого другого трафика, указанного в ордере.
Она стала спорной в 2000 году, когда провайдер оспорил ее в суде; она использовалась для записи заголовков электронной почты как данных о трафике, без ордера на прослушку. В настоящее время у нас есть раскрытия по

FOIA о текущей сети прослушки ФБР, DCSNet, которая очень эффективна — позволяет агентам удаленно и почти мгновенно получать доступ к трафику и контенту от участвующих телефонных компаний.

Радиоэлектронная разведка зарубежных целей и ее эффективность

Основная масса коммуникационной разведки, будь то прослушка, анализ трафика или другие методы, проводится не в правоохранительных целях, а для внешней разведки. В США главным агентством, отвечающим за это, является Агентство национальной безопасности (АНБ), которое располагает огромными объектами и десятками тысяч сотрудников. В то время как правоохранительные органы имеют 150–200 активных прослушек в любой момент времени, АНБ полностью затмевает эти цифры. Ситуация аналогична в других странах; британский Government Communications Headquarters (GCHQ) имеет тысячи сотрудников и бюджет около миллиарда долларов, в то время как много лет один-единственный полицейский в Нью-Скотленд-Ярде занимался администрированием всех полицейских прослушек в Лондоне (и делал другие вещи тоже).

Информация постепенно просачивалась о масштабах и эффективности современных операций сигнальной разведки. Фундаментальная история Дэвида Кана заложила основу, описав многое из того, что происходило до начала Второй мировой войны. Анонимный бывший аналитик АНБ, позже идентифицированный как Перри Феллвок, раскрыл масштабы операций АНБ в 1972 году. «Сбор информации АНБ завершен», — писал он. «Он охватывает то, что делают иностранные правительства, что планируют делать, что делали в прошлом: какие армии куда двигаются и против кого; какие военно-воздушные силы куда двигаются и каковы их возможности. У АНБ действительно нет никаких ограничений. Его миссия простирается от вызова B-52 во Вьетнаме до мониторинга каждого аспекта советской космической программы».

В то время как мотивом Феллвока было противодействие войне во Вьетнаме, следующим крупным осведомителем стал британский взломщик кодов времен Второй мировой войны, Фредерик Уинтерботэм, который хотел написать мемуары о своих военных достижениях и, поскольку он умирал, не беспокоился о судебном преследовании. В 1974 году он раскрыл успех союзников в взломе немецких и японских шифровальных систем во время этой войны, что привело к появлению множества других книг о сигнальной разведке Второй мировой войны. После этого произошел медленный поток откровений от investigative journalists, довольно немногие из чьих источников были обеспокоены злоупотреблением объектами со стороны чиновников, отслеживающих

внутренние политические группы. Например, осведомитель Пег Ньюшам раскрыла, что АНБ незаконно прослушивало телефонный звонок, сделанный сенатором Стромом Термондом.
Джеймс Бэмфорд собрал довольно много информации об АНБ из открытых источников и, поговорив с бывшими сотрудниками, в то время как наиболее существенным недавним источником информации об организации и методах сигнальной разведки США и их союзников стала книга, собранная новозеландским журналистом Ники Хагером после того, как разведывательное сообщество Новой Зеландии не подчинилось приказу своего премьер-министра понизить уровень разведывательного сотрудничества с США.
Картина, которая emerged из этих источников, описывала всемирную систему сбора сигнальной разведки, Echelon, совместно управляемую США, Великобританией, Канадой, Австралией и Новой Зеландией. Данные, факсы и телефонные звонки собираются на большом количестве узлов, которые варьируются от международных коммуникационных кабелей, которые приземляются в странах-участницах (или перехватываются тайно под водой), до наблюдения за трафиком к и от коммерческих спутников связи и специальных спутников разведки, которые перехватывают трафик над враждебными странами, до пунктов прослушки в посольствах стран-участниц. Собранный трафик ищется в реальном времени компьютерами, известными как словари, согласно таким критериям, как телефонные номера или IP-адреса отправителя или получателя, а также поиск по ключевым словам в содержимом электронной почты. Эти критерии поиска вводятся аналитиками разведки стран-участниц; словари затем собирают трафик, удовлетворяющий им, и отправляют его обратно аналитику. Echelon, по всей видимости, работает очень похоже на Google, за исключением того, что вместо поиска веб-страниц он ищет трафик мировой телефонной и информационной сети в реальном времени.
Несмотря на то, что Echelon выглядит впечатляюще (и пугающе), следует учесть несколько моментов. Во-первых, сеть, построенная АНБ и его союзниками, была в основном нацелена на старый СССР, где человеческая разведка была затруднена, и сбор огромных объемов телефонных звонков давал хотя бы некоторое представление о том, что происходит. Но полученная в результате политическая и экономическая разведка оказалась слабой; Запад думал, что экономика России примерно в два раза больше, чем она была на самом деле, и был удивлен ее крахом после 1989 года. (Стимулы агентств преувеличивать угрозу очевидны). В любом случае, большая часть усилий была военной, направленной на понимание советских радаров и коммуникаций, а также на получение решающего преимущества в определении местоположения, подавлении и обмане. Без способности вести электронную войну современное

государство не может конкурировать в воздушных или морских боях или в танковых сражениях на земле. Поэтому неудивительно, что большинство персонала АНБ — военные, а его директором всегда был действующий генерал. По-прежнему много усилий тратится на понимание сигналов потенциальных противников.

Во-вторых, были некоторые успехи против террористов — в частности, арест предполагаемого организатора 11 сентября Халида Шейха Мохаммеда после того, как он использовал SIM-карту мобильного телефона из партии, купленной известным террористом в Швейцарии. Но электронная война против повстанцев в Ираке, оказалась непродуктивной. И давно ясно, что гораздо больше усилий следовало направить на человеческую разведку. В статье, опубликованной незадолго до 11 сентября, аналитик написал: «У ЦРУ, вероятно, нет ни одного по-настоящему квалифицированного говорящего по-арабски офицера ближневосточного происхождения, который мог бы правдоподобно сыграть мусульманского фундаменталиста, который вызвался бы провести годы своей жизни с паршивой едой и без женщин в горах Афганистана. Ради Бога, большинство оперативных офицеров живут в пригородах Вирджинии. Мы не занимаемся такими вещами». Другой выразился еще более прямолинейно: «Операции, которые включают диарею как образ жизни, не происходят». Сочетание дистанционной технической разведки и огромной огневой мощи соответствует личным интересам бюрократов и поставщиков оборудования, но это делает союзные силы неэффективными в борьбе с повстанцами, где враг смешивается с гражданским населением. Подобные извращенные стимулы препятствуют и военным. Например, Британия тратит миллиарды на два новых авианосца и на модернизацию ядерного сдерживания, но даже через шесть лет после 11 сентября мы не подготовили достаточно солдат, способных поддержать базовый разговор на арабском языке. Большие дебаты, которые сейчас назревают в Пентагоне, касаются не только разведки, но и того, как выработать более умный подход к борьбе с повстанцами в целом.

В-третьих, хотя другие страны могут жаловаться на сбор сигнальной разведки США, лицемерно с их стороны морализировать по этому поводу. Другие страны также проводят разведывательные операции и часто гораздо более агрессивны в проведении экономической и другой невоенной шпионской деятельности. Реальная разница между странами WASP и остальными заключается в том, что никто другой не построил «систему систем» Echelon. Действительно, в области сигнальной разведки, как и в других, могут действовать сетевые эффекты: ценность сети растет быстрее, чем ее размер, и чем больше вы перехватываете, тем дешевле это становится. Поэтому были предприняты попытки построить «европейский Echelon» с участием полиции и разведывательных агентств

континентальных европейских стран.
Зрелая точка зрения, заключается в том, что сигнальная разведка необходима для выживания нации, но потенциально опасна — так же, как и вооруженные силы, которым она служит. Вопрос не в том, должны ли существовать такие ресурсы, а в том, как они подотчетны. В США слушания сенатора Черча в 1975 году детально описали ряд злоупотреблений, таких как незаконный мониторинг граждан США. Сбор внешней разведки теперь регулируется законодательством США в форме 50 USC 1801–1811, который кодифицирует FISA. Это не идеально; как уже отмечалось, он является предметом ожесточенных споров между исполнительной и законодательной властью по поводу недавнего положения о том, что АНБ может прослушивать звонки в США, если одна из сторон, как полагают, не является гражданином США. Даже до этого количество ордеров FISA неуклонно росло после 11 сентября и превысило количество обычных ордеров на прослушку по Титулю III. Но, по крайней мере, Конгресс заинтересовался. И США повезло: в большинстве стран надзор за разведкой даже не обсуждается.
Наконец, плохая подотчетность обходится дороже, чем просто эрозия свободы и случайные политические злоупотребления. Существует также реальная операционная стоимость в распространении разведывательных бюрократий, которые оказываются в основном бесполезными, когда начинаются боевые действия. В Вашингтоне во время Холодной войны агентства ненавидели друг друга гораздо больше, чем они ненавидели русских. В Великобритании одной из самых ожесточенных разведывательных битв была не против ИРА, а между полицией и MI5 из-за того, кто будет ведущим в борьбе против ИРА. Существует множество отчетов о неэффективности разведки и внутренних склоках от хорошо осведомленных инсайдеров, таких как Р. В. Джонс. Именно в этом контексте бюрократических войн за сферы влияния, надо описать, которые стали формирующим опытом для многих правительств (и НПО) в вопросах политики наблюдения и технологий.

Крипто-войны (The Crypto Wars)

Политика в области технологий в 1990-х годах была доминирована ожесточенными дебатами о депонировании ключей (key escrow) — доктрине, согласно которой любой, кто шифрует данные, должен предоставить правительству копию ключа, чтобы гражданское использование криптографии не препятствовало сбору разведданных АНБ и другими. Хотя некоторые ограничения на криптографию существовали годами и раздражали как академических исследователей, так и гражданских пользователей, они попали на первые полосы газет в 1993 году, когда президент Клинтон поразил ИТ-

индустрию Стандартом шифрования с депонированием, более известным как чип Clipper. Это было предлагаемой заменой DES, со встроенной бэкдор-ключом, чтобы правительственные агентства могли расшифровывать любой трафик. АНБ пыталось продать эту программу кабинету президента Буша-старшего и потерпело неудачу, но новая администрация была рада помочь.
Мнение в США поляризовалось. Правительство утверждало, что, поскольку криптография предназначена для сохранения секретности сообщений, она может использоваться преступниками для предотвращения сбора доказательств полицией при прослушке, ИТ-индустрия (за несколькими исключениями) заняла противоположную точку зрения, что криптография была единственным средством защиты электронной коммерции и, таким образом, жизненно важна для будущего развития сети. Группы по защите гражданских свобод встали на сторону индустрии и заявили, что криптография станет критической технологией для конфиденциальности. К 1994 году АНБ пришло к выводу, что оно столкнулось с войной с Microsoft, которую Билл выиграет, поэтому оно передало руководство политикой ФБР, продолжая направлять вопросы из-за кулис.
Дебаты быстро переплелись с экспортным контролем над оружием, с помощью которого криптография традиционно контролировалась. Американским/software-фирмам не разрешалось экспортировать продукты, содержащие криптографию, которую было слишком сложно взломать (обычно это означало длину ключа более 40 бит). Автор программного обеспечения из США, Фил Циммерманн, был вызван на большое жюри за торговлю оружием после того, как программа, которую он написал — PGP — «сбежала» в интернет. Он немедленно стал народным героем и сделал состояние, так как его продукт захватил лидерство на рынке. Конфликт стал международным: Государственный департамент США пытался убедить другие страны тоже контролировать криптографию. Это стало одной из личных миссий вице-президента Гора (причина, по которой многие в Редмонде и Кремниевой долине внесли вклад в кампанию Буша в 2000 году). Результаты были смешанными. Некоторые страны с воспоминаниями об угнетающих режимах, такие как Германия и Япония, сопротивлялись американским уговорам. Другие, такие как Россия, воспользовались предлогом, чтобы принять суровые законы о контроле над криптографией. Франция дерзко нарушила традиционный запрет на негосударственное использование криптографии, Британия послушно перешла от либеральной политики невмешательства при Джоне Мейджоре в середине 1990-х годов к драконовскому закону при Тони Блэре. Закон о регулировании полномочий по расследованию (RIP) 2000 года дает полиции право требовать, чтобы я передал ключ или пароль, находящийся в моем распоряжении, а Закон об экспортном

контроле 2002 года предписывает мне получить лицензию на экспорт, если я отправляю любое криптографическое программное обеспечение за пределы Европы, использующее ключи длиннее 56 бит. О, и правительство также получило полномочия проверять иностранных аспирантов, изучающих опасные предметы, такие как информатика, и отказывать в визах тем, кого оно считает риском распространения.

Имели ли крипто-войны значение?

Когда дебаты о депонировании ключей разгорелись в Великобритании в 1994–1995 годах, была многими занята позиция, которая в то время была непопулярна как среди лоббистов за депонирование, так и среди противников. Сторонники депонирования утверждали, что, поскольку криптография обеспечивает конфиденциальность, а конфиденциальность может помочь преступникам, должен быть какой-то способ обойти ее. Противники депонирования утверждали, что, поскольку криптография необходима для конфиденциальности, не должно быть способа обойти ее. По существу все предпосылки этих аргументов были неверны. Большинство приложений криптографии (в реальном мире, в отличие от академического) касаются аутентификации, а не конфиденциальности; они помогают полиции, а не препятствуют ей. Что касается преступников, то им требуется незаметная связь — а шифрование телефонного звонка — это хороший способ привлечь к себе внимание агентств. Что касается конфиденциальности, то большинство нарушений происходит в результате злоупотребления санкционированным доступом со стороны инсайдеров. Наконец, гораздо более серьезная проблема для полицейских, расследующих электронные преступления, заключается в том, чтобы найти приемлемые доказательства, для чего хорошая аутентификация может быть полезной.

Это не значит, что у полиции нет нужды в прослушке. Хотя многие полицейские силы обходятся без нее довольно успешно, а некоторые из них, как мы видели, используют ее, и угроза прослушки может быть эффективным сдерживающим фактором, существуют случаи, когда она необходима. Отчет Уолша — старшего австралийского разведчика — дает достаточно сбалансированное рассмотрение этих вопросов. Он сравнил операционные merits прослушки, жучков и физического наблюдения и указал, что прослушка была либо самым дешевым, либо единственным методом расследования в некоторых обстоятельствах.

Тем не менее, главное достижение разведывательного сообщества в 1990-х годах, позже было выяснено, заключалось в том, чтобы свести к минимуму количество систем, использующих криптографию по умолчанию. Если бы значительная часть интернет-трафика была зашифрована, то

автоматизированный поиск по ключевым словам, выполняемый такими системами, как Echelon, был бы в значительной степени сорван. АНБ прекрасно осознавало, что многие новые сетевые системы быстро строились во время бума доткомов, и если бы криптография не была встроена в них с самого начала, то, скорее всего, было бы слишком дорого внедрять ее позже. Поэтому каждый год АНБ удерживало линию на контроле над криптографией, что означало десятки систем, открытых для перехвата на десятилетия вперед. В этих терминах политика была успешной: лишь незначительная часть мирового сетевого трафика зашифрована, за некоторыми исключениями, такими как контент, защищенный DRM, Skype, несколько веб-страниц, защищенных TLS, оппортунистическое шифрование TLS между почтовыми серверами, трафик SSH, корпоративные VPN и онлайн-компьютерные игры. Все остальное в значительной степени открыто для перехвата — включая массы высокочувствительной электронной почты между компаниями.

Отчет Уолша и европейский спор о типах ключей

Отчет Уолша — старшего австралийского разведчика — дал сбалансированную оценку этих проблем. Он пришел к выводу, что нет убедительных причин для раннего регулирования криптографии, но рекомендовал разрешить полиции и спецслужбам взламывать компьютеры подозреваемых для получения доказательств (например, устанавливая на них шпионское ПО).
В Европе эти дебаты привели к расколу при обсуждении «Евроклиппера» (Euroclipper). Немецкое правительство требовало, чтобы депонированию (эскроу) подлежали только ключи конфиденциальности. Великобритания же настаивала на том, чтобы депонировались и ключи цифровых подписей. Британская позиция опиралась на военную доктрину, где обман и дезинформация считаются не менее важными, чем прослушка, в то время как немцы опирались на полицейскую доктрику, требующую сохранения доказательной базы и недопущения подделки подписей.

Скандал с Crypto AG и Хансом Бюлером

Одним из самых известных примеров негласного контроля стал случай со швейцарской компанией Crypto AG, которая была ведущим поставщиком шифровального оборудования для правительств, не имевших собственных технологий. В 1992 году её продавец Ханс Бюлер был арестован в Иране. Он заявил, что компания тайно контролировалась спецслужбами США и

Великобритании (GCHQ), а в её устройства годами встраивались бэкдоры, известные в профессиональной среде как «красные нити» (red threads), позволявшие спецслужбам читать трафик.

Экспортный контроль

Основным побочным эффектом крипто-войн стало введение гораздо более жесткого экспортного контроля, чем раньше, особенно в Европе. Приведем краткую сводку законодательства о криптографии.
Международные соглашения о контроле над вооружениями (КОКОМ и Вассенаарские договоренности) обязывают большинство правительств вводить экспортный контроль над криптографическим оборудованием, и последние реализуются в Европейском Союзе регламентом ЕС, обязывающим государства-члены контролировать и лицензировать экспорт товаров двойного назначения — товаров, которые имеют как гражданское, так и военное применение. Криптоаналитические продукты подпадают под военный режим, тогда как подавляющее большинство программного обеспечения, которое просто использует криптографию для защиты, подпадает под товары двойного назначения.
Но национальные реализации различаются. Законодательство Великобритании не контролировало экспорт нематериальных активов до 2002 года, поэтому криптографическое программное обеспечение можно было экспортировать в электронном виде, бельгийское правительство выдает лицензии почти на все, а Швейцария остается крупным экспортером криптографического оборудования.

Цензура

«Дебаты о политике шифрования, стали репетицией в 1990-х еще более масштабной битвы, которая велась вокруг анонимности, цензуры и авторского права». И хотя вопросы авторского права и DRM в значительной степени стабилизировались, цензура за последние годы стала гораздо более острой проблемой.
Цензура осуществляется по самым разным мотивам. Китай блокирует не только сайты инакомыслящих, но и электронные письма, содержащие запрещенные слова. Некоторые страны включают цензуру во время выборов или после кризисов (как это было в Бирме). В США ведутся дебаты о том, должны ли интернет-провайдеры, которые также являются телефонными компаниями, блокировать VOIP, и должны ли провайдеры, управляющие кабельными каналами, блокировать P2P-трафик (это вопрос принципа сетевого нейтралитета). В Европе проблема заключается в том, что разные страны

запрещают разный контент: Франция и Германия запрещают продажу нацистской символики. Многие страны пытались ввести контроль над детской порнографией — это стало стандартным оправданием для политиков, которые хотят «что-то сделать» с Интернетом. Также существует европейская инициатива по блокировке радикальных исламистских сайтов. Наконец, цензура иногда налагается судами в контексте гражданских споров, например, запрет на публикацию кода DeCSS.
Формы цензуры также разнообразны: от блокировки определенных типов трафика и фильтрации по IP-адресам до отравления DNS, инспекции контента и внеполосных механизмов (например, наказание людей, скачавших нежелательный материал).

Цензура авторитарными режимами

Китай. В конце 2006 года в Китае насчитывалось 137 миллионов пользователей Интернета. Правительство инвестировало огромные средства в технологии фильтрации. «Великий китайский файрвол» — это сложная социотехническая система, обеспечивающая эшелонированную защиту от различных материалов: от порнографии до религиозных материалов и политического инакомыслия.

- **Периметровая защита:** Маршрутизаторы в Шэньчжэне фильтруют по IP-адресам известные «плохие» сайты (Голос Америки, Би-би-си) и используют отравление DNS-кэша. Глубокая инспекция пакетов на уровне TCP используется для выявления писем и веб-страниц с запрещенными словами (например, «Фалуньгун»): пакеты TCP reset отправляются обоим концам соединения для его разрыва. Фильтрация по ключевым словам (около 1000 запрещенных слов) применяется в китайских поисковиках и блогах.
- **Защита на уровне приложений:** Некоторые сервисы блокируются, другие нет, в зависимости от того, насколько провайдер услуг играет по правилам режима. Были большие споры, когда Google согласился цензурировать свои результаты поиска в Китае (на самом деле они заполняют свой китайский индекс с помощью пауков, которые ищут изнутри Китая, и поэтому видят только тот материал, который и так доступен там). Стимулы, создаваемые быстро растущими рынками Китая, позволяют его правительству заставлять крупные международные фирмы подчиняться.
- **Социальная защита:** От 30 000 интернет-полицейских до судебных процессов над кибер-диссидентами и законов, требующих от интернет-кафе идентифицировать клиентов, до пары мультяшных маскотов

интернет-полиции (Цзинцзин и Чаоча), которые появляются везде в сети, чтобы напомнить пользователям, что они находятся в социальном пространстве, а не в частном.

Однако контроль отстает. В Китае более 20 миллионов блогов, и хотя интернет-полиция энергично удаляет откровенно подстрекательский материал, онлайн-обсуждение местных новостных событий привело к появлению надлежащего «общественного мнения», которое впервые не находится в рабстве у медиа-менеджеров. Это связано не только с электронной почтой и блогами, но и с быстрым ростом использования мобильных телефонов. Местные события, такие как захваты земель коррумпированными чиновниками, теперь могут быстро подняться в повестке дня, подвергая правительство давлению, от которого оно раньше было изолировано.

Бирма. Внезапный рост цен на топливо в августе 2007 года привел к массовым протестам и жестокому подавлению армией с 26 сентября, в результате которого, возможно, погибли несколько сотен человек. Во время протестов бирманские граждане использовали Интернет и мобильную связь для отправки фотографий и видео во внешний мир, в результате чего их восстание попало на первые полосы мировых газет, а подавление вызвало широкое осуждение хунты. Это произошло несмотря на то, что Бирма — одна из всего 30 стран в мире, где менее 1% населения пользуется Интернетом.
Мировые заголовки явно причинили боль, и 29 сентября началось полное отключение Интернета. Это был первый случай, когда массовая блокировка Интернета использовалась для предотвращения распространения новостей. С 4 по 12 октября действовал комендантский час, когда связь была доступна только с 22:00 до 4:00 утра, на третьем этапе некоторым интернет-кафе было разрешено вновь открыться, но скорость была ограничена до 256 Кбит/с, а другие были закрыты, а оборудование конфисковано. Большинство бирманцев использовали инструменты обхода цензуры, такие как прокси. Фактически восстание называли «революцией g-lite» в честь популярного прокси Gmail. Если урок из этого печального инцидента заключается в том, что даже 1% использования Интернета может дестабилизировать диктатуру, и что даже диктатуры с трудом обходятся без Интернета, то это скорее обнадёживает.

Сетевой нейтралитет

Ряд менее развитых стран блокируют услуги VOIP, чтобы облегчить прослушку телефонных разговоров и сохранить прибыльность государственных телефонных компаний. Телефонные компании в развивающихся странах часто

получают большую часть своих доходов от своей доли в платежах, которые иностранцы платят за звонки в эту страну, а VOIP позволяет эмигрантам избежать этих платежей.
Однако большинство проблем с VOIP возникает в развитых странах, особенно в Америке. Ряд ISP также являются телефонными компаниями и используют технические механизмы для нарушения работы сервисов VOIP — например, внося джиттер или короткие паузы в поток пакетов. В результате в Вашингтоне разгорелись ожесточенные дебаты о сетевом нейтралитете. С одной стороны, индустрия VOIP выступает за закон, который обязал бы ISP относиться ко всему трафику одинаково; с другой стороны, телефонные компании возражают: «Не регулируйте Интернет».
Вопрос шире, чем просто VOIP. Телефонные компании всегда взимали совершенно разные тарифы за разные типы трафика: учитывая, что у них высокие постоянные издержки и низкие предельные издержки, у них есть все стимулы для ценовой дискриминации. Эд Уитэйкер, председатель AT&T, начал эти дебаты в 2005 году, когда он заявил, что таким компаниям, как Google, Yahoo или Vonage, использовать «его» широкополосные каналы бесплатно, чтобы зарабатывать деньги для себя, — это «безумие». Это разделило Конгресс в основном по партийным линиям: демократы выступают за сетевой нейтралитет, а республиканцы — за телефонные компании.
В Европе сетевой нейтралитет является меньшей проблемой, так как там больше конкуренции на рынке ISP. Регуляторы склонны считать, что если одни ISP занимаются формированием трафика, то это не так важно, пока клиенты могут переключиться на других ISP, которые этого не делают.

Peer-to-peer, разжигание ненависти и детская порнография

Три «всадника», которых продвигают сторонники интернет-цензуры в развитых странах, — это обмен файлами, разжигание ненависти и детская порнография.

Обмен файлами. Системы обмена файлами поднимают некоторые вопросы сетевого нейтралитета, например, Comcast нарушала работу BitTorrent, используя те же методы подделки пакетов TCP reset, что и в «Великом китайском файрволе». Comcast, будучи кабельным оператором, хочет, чтобы их клиенты смотрели телевизор по их кабельному каналу, а не скачивали его, чтобы максимизировать свои доходы от рекламы. Главными игроками, выступающими за фильтрацию однорангового трафика, являются музыкальные компании. Многие университеты были запуганы угрозой судебных исков и ограничили такой трафик в студенческих локальных сетях. Поэтому будет интересно посмотреть, введут ли страны обязательную фильтрацию в

«моральных» целях, которую музыкальная индустрия затем сможет использовать и для своих целей.

Разжигание ненависти. В Европе была недавняя попытка ввести обязанность для ISP фильтровать разжигание ненависти, и в частности, джихадистские веб-сайты. Франция и Германия запрещают продажу нацистской символики. Эксперты скептически относятся к тому, сделает ли такой закон Европу безопаснее, запрет писаний радикальной мусульманской секты Деобанди, к которой принадлежит, возможно, треть мусульман Британии, скорее всего, усугубит напряженность в обществе. Более того, исследования показывают, что большая часть литературы о ненависти, распространяемой внутри и за пределами британских мечетей, производится или финансируется религиозными учреждениями из Саудовской Аравии. Реакция правительства — не противостоять королю Абдалле, а пригласить его на государственный визит. Интернет-цензура здесь является отвлекающим маневром, это позволяет правительству заявить, что оно что-то делает. Лучше оставить этот материал в открытом доступе, как это делает Америка, и позволить полиции отслеживать трафик на худшие из сайтов, а не заставлять мусульманскую молодежь приобретать навыки китайцев и бирманцев по использованию прокси.

Детская порнография. В 1990-х годах, когда правительства искали какой-то рычаг воздействия на Интернет, сложилось мнение, что явные изображения сексуального насилия над детьми — это примерно единственная вещь, с которой все государства могут согласиться, что ее следует запретить. Когда выступали в пользу репрессивной меры — такой как депонирование ключей — они приводили людей из детских благотворительных организаций, которые страстно утверждали, что сталинизм du jour жизненно необходим для спасения детей от вреда. Излишне говорить, что те из нас, кто был на либеральной стороне аргумента, предпочли бы, чтобы благотворительные организации тратили свои деньги на кампании по более серьезным проблемам защиты детей, таким как насилие над детьми в детских домах и детская проституция; а когда возникла действительно серьезная проблема на границе между ИТ-политикой и защитой детей — предложение о создании национальной базы данных о благосостоянии детей, которая откроет личную информацию миллионов детей сотням тысяч работников государственного сектора — эти достойные защитники детей молчали.

Дебаты о детской порнографии затихли в большинстве стран (Россия — заметное исключение, Путин использует детскую порнографию как главный предлог для цензуры, направленной на политических оппонентов), поскольку терроризм занял место детской порнографии в качестве туза в рукаве исполнительной власти. Но истерика действительно имела злые последствия.

Они были суровыми в Великобритании, где она использовалась для оправдания не только более повсеместного онлайн-наблюдения, но и создания Национального подразделения по высокотехнологичной преступности. Это подразделение провело операцию «ОО» (Operation Ore), в ходе которой около восьми тысяч британских граждан подверглись рейдам полиции по подозрению в покупке детской порнографии. Оказалось, что большинство из них, вероятно, стали жертвами мошенничества с кредитными картами. Отряд по борьбе с порнографией не понимал мошенничества с кредитными картами и не хотел этого знать, они были зациклены на получении обвинительных приговоров по порнографии. В результате несколько тысяч мужчин пострадали на месяцы или даже годы из-за ложного ареста по крайне стигматизирующим обвинениям, в которых они были невиновны. Для некоторых откровение о том, что полиция облажалась, пришло слишком поздно, более тридцати мужчин, столкнувшись с перспективой публичного судебного преследования, которое, вероятно, разрушит их семьи, покончили с собой. Причина всего этого заключалась в том, что операторы незаконных порно-сайтов скупали списки номеров кредитных карт, а затем проводили их через порталы для сбора платежей — вероятно, полагая, что многие люди не посмеют сообщить о дебетовых операциях за такие услуги в полицию. И хотя полиция оправдывала свои операции, утверждая, что они уменьшат вред детям, поставщики детской порнографии в деле «ОО» избежали судебного преследования.
Америка на самом деле справилась с этим случаем гораздо лучше, чем Британия. Около 300 000 номеров кредитных карт США были найдены на серверах оператора главного портала Томаса Риди, полиция использовала имена для разведки, а не в качестве доказательств, сопоставляя имена со своими базами данных, выявляя представляющих интерес подозреваемых — таких как люди, работающие с детьми — и тихо расследуя их. Было вынесено более сотни обвинительных приговоров за фактическое насилие над детьми, и ни одного ложного осуждения. Прагматичный акцент на старомодной полицейской работе гораздо предпочтительнее разжигания страха и грандиозных политических жестов.

Судебная экспертиза и правила допустимости доказательств

Это подводит нас естественным образом к последней главной теме в пространстве правосудия, а именно к тому, как информация может быть извлечена из компьютеров, мобильных телефонов и других электронных устройств для использования в качестве доказательств. Три больших изменения

в последние годы: во-первых, sheer volume (огромные объемы) данных, во-вторых, рост поисковых систем и других инструментов для поиска релевантного материала, и в-третьих, то, что суды постепенно становятся более расслабленными и компетентными.

Судебная экспертиза (Forensics)

Когда полиция проводит рейд даже против мелкого наркоторговца в наши дни, они могут получить хорошо более терабайта данных: несколько ноутбуков, полдюжины мобильных телефонов, пару iPod и, возможно, коробку флешек. Подозреваемый также может иметь десятки учетных записей онлайн для сервисов веб-почты, сайтов социальных сетей и других услуг. У него могут быть интересные гаджеты — например, навигаторы, которые хранят историю его местоположения (большая часть которой также доступна через записи его мобильного телефона). Исследователи безопасности нашли множество хитрых способов извлечения информации из данных — например, можно определить, какая камера сделала снимок, по паттерну шума массива CCD, и количество таких трюков может только увеличиваться.

Использование всего этого материала в качестве доказательств зависит, в большинстве стран, от соблюдения определенных процедур. Материал должен быть собран законно (с ордером на обыск или эквивалентными полномочиями) и судебный эксперт должен поддерживать цепочку custody (непрерывность хранения), что означает возможность удовлетворить суд в том, что доказательства не были подделаны после этого. Основная процедура заключается в использовании инструментов, которые были должным образом протестированы и оценены для создания надежных копий данных (например, вычисление одностороннего хэша данных для установления их подлинности) документирование всего, что делается и наличие средств для надлежащего обращения с любым частным материалом (например, привилегированные электронные письма между адвокатом и клиентом).

Компьютерная судебная экспертиза ставит все более сложные инженерные проблемы. Недавний пример заключается в том, что многие полицейские силы приняли жесткую процедуру всегда выключать ПК, чтобы жесткие диски можно было зеркалировать. Банда Rockphish использовала это, сделав свое фишинговое программное обеспечение резидентным в памяти. Полиция прибыла бы в дом, содержащий фишинговый сервер, выключила бы машину — и потеряла бы всю информацию, которая позволила бы им отследить реальный сервер, для которого захваченная машина действовала как прокси.

Связанная проблема заключается в том, что Windows Vista поставляется с Bitlocker, утилитой шифрования дисков, которая хранит ключи в чипе TPM на

материнской плате, и поэтому делает файлы неиспользуемыми после выключения машины, если вы не знаете пароль. Хотя в Великобритании теперь есть закон, позволяющий судам сажать людей в тюрьму за отказ предоставить пароль, в большинстве стран его нет.
Еще одна проблема заключается в том, что может быть важно минимизировать сбои, вызванные судебно-медицинским копированием. Даже если машина конфискована у подозреваемого, это может быть проблематично, если вы тратите слишком много времени на ее изучение. В случаях операции «ОО» у многих людей, которые позже оказались невиновными, забрали их ПК и хранили их месяцами или даже годами, потому что у полиции не было судебных возможностей справиться с этим. В результате они оставались под облаком подозрений гораздо дольше, чем это было разумно, это оказало неблагоприятное влияние на людей в регулируемых профессиях, что привело к судебным искам против полиции. Существует также проблема потери доступа к данным, что для отдельного человека или малого бизнеса может быть катастрофичным. В наши дни prudent practice (разумная практика) для студента — иметь резервную копию, защищенную от изъятия, например, завести учетную запись Gmail и регулярно отправлять туда копии своей диссертации.
Еще одна ловушка судебной экспертизы — полагаться на доказательства, извлеченные из систем одной из сторон в споре, не применяя достаточного скептицизма. Вспомните дело Munden, которое было описано в ранних частях Security Engineering. Человека ложно обвинили и ложно осудили за попытку мошенничества после того, как он пожаловался на несанкционированные списания средств со своего банковского счета. При апелляционном рассмотрении его команда защиты получила постановление суда о том, чтобы банк открыл свои системы для эксперта защиты. Банк отказался, банковские выписки были признаны недопустимыми, и дело развалилось. Поэтому, полагаясь на судебно-медицинские доказательства, предоставленные участником спора, стоит заранее подумать о том, выдержат ли они экспертизу враждебными экспертами.

Допустимость доказательств (Admissibility of Evidence)

Когда суды впервые столкнулись с компьютерными доказательствами в 1960-х годах, было много опасений по поводу их надежности. Была не только инженерная проблема, были ли данные точными, но и юридическая проблема, были ли компьютерные данные недопустимыми на том основании, что они являются hearsay (слухами). Различные законодательные органы решали это по-разному. В США большая часть закона содержится в Federal Rules of Evidence, где компьютерные записи обычно вводятся как business records (деловые записи). В

Великобритании ситуация похожа: Civil Evidence Act 1995 охватывает гражданские судебные разбирательства, а Police and Criminal Evidence Act 1984 касается уголовных дел. Требование о том, чтобы машина работала в обычном ходе бизнес-операций, может вызывать проблемы, когда машины должны эксплуатироваться ненормальными способами для извлечения информации. Существуют некоторые специальные юридические положения для определенных технологий, многие из них были приняты во время или вскоре после бума доткомов, поскольку законодатели стремились проложить путь для электронной коммерции, не понимая проблем. Многие отраслевые лоббисты утверждали, что электронной коммерции мешает неопределенность в отношении того, будут ли электронные документы приниматься как «письменная форма» для тех законов, которые требуют, чтобы определенные транзакции были письменными. Поэтому законодательные органы, начиная с Юты, приняли законы, предоставляющие особый статус цифровым подписям. В большинстве случаев это не имело никакого эффекта, так как суды приняли разумное мнение, что электронное письмо является письменной формой так же, как и бумажное письмо: суть подписи — это намерение подписавшего, и суды давно принимали решения таким образом. Например, сельскохозяйственный рабочий, который был раздавлен насмерть трактором и сумел нацарапать «все маме» на шине, был признан составившим юридическое завещание.
Однако есть один случай, когда нетерпеливые законодатели полностью ошиблись, и это Европа. Директива об электронных подписях, вступившая в силу в 2000 году, обязывает все государства-члены придать особую силу расширенной электронной подписи, что в основном означает цифровую подпись, сгенерированную с помощью смарт-карты. Индустрия смарт-карт Европы думала, что это принесет им много денег. Однако это имело обратный эффект. В настоящее время риск того, что бумажный чек будет подделан, несет сторона, полагающаяся на него: если кто-то подделывает чек на моем счете, то это не моя подпись, и я не дал банку свой мандат на дебетование моего счета, поэтому, если они по небрежности полагаются на поддельную подпись и делают это, это их проблема. Однако, если бы я был достаточно глуп, чтобы когда-либо принять устройство расширенной электронной подписи, тогда возникла бы презумпция действительности любой подписи, которая, похоже, была сделана с его помощью. Внезапно риск смещается с банка на меня. Я становлюсь ответственным перед кем угодно в мире за любую подпись, которая, похоже, была сделана моей смарт-картой, независимо от того, действительно ли я ее сделал! Это, наряду с фактами, что смарт-карты не имеют надежного пользовательского интерфейса, а ПК, которые большинство людей использовали бы для обеспечения этого интерфейса, легко и часто подвергаются взлому,

сделало электронные подписи мгновенно непривлекательными.
Наконец, слово о click-wrap. В 2000 году Конгресс США принял Закон об электронных подписях в глобальной и национальной коммерции (ESIGN), который придает юридическую силу любому «звуку, символу или процессу», посредством которого потребитель соглашается с чем-либо. Таким образом, нажатие клавиши на телефоне, щелчок гиперссылки для входа на веб-сайт или щелчок «продолжить» в установщике программного обеспечения, потребитель соглашается быть связанным контрактом. Это заставляет лицензии click-wrap работать в Америке. Общее мнение юристов в Европе заключается в том, что они, вероятно, не работают здесь, но никто не спешит возбуждать первое дело.

Конфиденциальность и защита данных

Защита данных — это термин, используемый в Европе для обозначения защиты личной информации от ненадлежащего использования. Личная информация обычно означает любые данные, хранящиеся об идентифицируемом человеке или субъекте данных, такие как детали банковского счета и модели покупок по кредитной карте. Это примерно соответствует американскому термину computer privacy (компьютерная конфиденциальность). Различие в терминологии сопровождается огромной разницей в законах и отношениях.
Европейское законодательство дает субъектам данных право проверять личные данные, хранящиеся о них, изменять их, если они неточны, понимать, как они обрабатываются, и во многих случаях предотвращать их передачу другим организациям без их согласия. Существуют исключения для национальной безопасности, но они не так полны, как хотелось бы спецслужбам: был большой скандал, когда выяснилось, что данные из SWIFT, которая обрабатывает межбанковские платежи, копировались в Department of Homeland Security без ведома субъектов данных. Европейские органы по защите данных постановили, что SWIFT нарушила европейское, бельгийское и швейцарское законодательство о защите данных, и она согласилась прекратить обработку европейских данных в США к концу 2009 года.
Охватываются почти все коммерческие данные, и существуют особенно строгие правила контроля над данными, касающимися интимных вопросов, таких как здоровье, религия, раса, сексуальная жизнь и политические убеждения.
Наконец, недавний закон предписывает, что личные данные не могут быть отправлены организациям в странах, законы которых не обеспечивают сопоставимую защиту. На практике это означает Америку и Индию, где правовая защита конфиденциальности фрагментарна. Решением до сих пор было соглашение safe harbor, согласно которому обработчик данных в Америке или

Индии обещает своему европейскому клиенту соблюдать европейское законодательство. Многие фирмы делают это, пионером была Citibank, которая создала такую договоренность для обработки данных держателей немецких карт в Южной Дакоте. Но это создает практические проблемы обеспечения соблюдения для граждан ЕС, которые считают, что их права были нарушены, они не являются стороной контракта и могут с трудом убедить Министерство торговли США принять меры против фирмы из США. Поэтому положения safe harbor могут провалиться при проверке в суде.

Европейская защита данных

Технофобия — это не изобретение конца двадцатого века. Еще в 1890 году судьи Уоррен и Брандейс предупредили об угрозе конфиденциальности со стороны «недавних изобретений и бизнес-методов» — в частности, фотографии и журналистских расследований. Годы спустя, после того как крупные розничные компании начали использовать компьютеры в 1950-х годах, а банки последовали за ними в начале 1960-х, люди начали беспокоиться о социальных последствиях, если все транзакции гражданина могут быть собраны, консолидированы и проанализированы. В Европе крупный бизнес избежал осуждения, выдвинув аргумент, что только правительство может позволить себе достаточно компьютеров, чтобы представлять серьезную угрозу конфиденциальности. Как только люди осознали, что для правительства экономически и рационально расширить свою власть, используя личные данные всех граждан в качестве основы для прогноза, это стало вопросом прав человека — учитывая недавнюю память о гестапо в большинстве европейских стран. Лоскутное одеяло законов о защите данных начало появляться, начиная с немецкой земли Гессен в 1969 году. Из-за скорости, с которой меняются технологии, успешные законы были технологически нейтральными. Их общей темой был регулятор (на национальном или государственном уровне), которому пользователи личных данных должны были отчитываться и который мог предписать им прекратить и воздержаться от ненадлежащей обработки.
Со временем обработка данных транснациональными компаниями также стала проблемой, и люди осознали, что чисто местные или национальные инициативы, вероятно, будут неэффективны против них. После добровольного кодекса поведения, принятого ОЭСР в 1980 году, защита данных была закреплена конвенцией Совета Европы в январе 1981 года, которая вступила в силу в октябре 1985 года. Хотя строго говоря, эта конвенция была добровольной, многие государства подписались на нее из страха потерять доступ к рынкам обработки данных. Она требовала от государств-подписантов принять внутреннее законодательство для реализации по крайней мере некоторых

минимальных гарантий. Данные должны были быть получены законно и обрабатываться справедливо, и государства должны были гарантировать, что правовые средства защиты были доступны при возникновении нарушений. Качество реализации сильно варьировалось. В Великобритании, например, Маргарет Тэтчер бесстыдно сделала минимум возможного для соблюдения европейского законодательства, был создан орган по защите данных, но он был лишен финансирования и технической экспертизы, и было предоставлено много исключений для избранных групп избирателей. В жестких странах по защите конфиденциальности, таких как Германия, органы по защите данных стали серьезными правоохранительными агентствами.
К началу 1990-х годов стало ясно, что разница между национальными законами создает барьеры для торговли. Многие компании вообще избегали контроля, перемещая свою обработку данных в США. Поэтому защита данных была окончательно возведена в ранг полноценного европейского законодательства в 1995 году с Директивой о защите данных. Она устанавливает более высокие минимальные стандарты, чем требовало большинство стран до этого, с особенно строгим контролем над высокочувствительными данными, такими как здоровье, религия, раса и политическая принадлежность. Она также предотвращает отправку личной информации в «убежища данных», такие как США, если только там не действуют сопоставимые меры контроля, обеспечиваемые контрактом.

Различия между Европой и США

История в США подробно описана в моих статьях об безопасности, в основном бизнесу удалось убедить правительство оставить конфиденциальность в значительной степени на «саморегулирование». Хотя существует лоскутное одеяло государственных и федеральных законов, они являются специфичными для приложений и сильно фрагментированными. В целом, конфиденциальность в федеральных правительственных записях и в коммуникациях довольно строго регулируется, в то время как бизнес-данные в значительной степени не контролируются. Есть несколько островов регулирования, таких как Fair Credit Reporting Act 1970 года, который регулирует раскрытие кредитной информации и в целом похож на европейские правила; Video Privacy Protection Act или «Bork Bill», принятый после того, как вашингтонская газета опубликовала историю аренды видео судьи Роберта Борка после его номинации в Верховный суд США; Drivers' Privacy Protection Act, принятый для защиты конфиденциальности записей DMV после того, как актриса Ребекка Шаффер была убита одержимым фанатом, который нанял частного детектива, чтобы найти ее адрес и Health Insurance Portability and Accountability Act, который защищает медицинские записи. Однако законодательство США о конфиденциальности также включает

несколько деликтов, которые обеспечивают основу для гражданского иска, и они охватывают удивительное количество обстоятельств. Был также знаменательный случай в 2006 году, когда Choicepoint заплатила 10 миллионов долларов за урегулирование иска, возбужденного FTC после того, как она не проверила подписчиков должным образом и позволила мошенникам купить личную информацию более 160 000 американцев, что привело по крайней мере к 800 случаям «кражи личности».

Отношения также различаются. Некоторые исследователи сообщают о растущем чувстве в США, что люди потеряли контроль над использованием их личной информации, в то время как в некоторых европейских странах конфиденциальность рассматривается как фундаментальное право человека, требующее энергичной законодательной поддержки, в Германии она закреплена в конституции. Но нужно сказать, что здесь есть постоянная проблема. Люди говорят, что они ценят конфиденциальность, но действуют иначе. Подавляющее большинство людей, будь то в США или Европе, обменяют свою конфиденциальность на очень небольшие преимущества. Технологии улучшения конфиденциальности предлагались на продажу, но большинство из них провалились на рынке.

Тем не менее, в других странах суды стали более защищающими права граждан после 11 сентября. В Германии, которая обычно занимает самую жесткую позицию, конфиденциальность превосходит даже «войну с террором»: высший суд признал неконституционным действие полиции 2001 года по созданию досье на более чем 30 000 студентов или бывших студентов мужского пола в возрасте от 18 до 40 лет из мусульманских стран — даже несмотря на то, что в результате никто не был арестован. Он постановил, что такие упражнения могут проводиться только в ответ на конкретные угрозы, а не в качестве превентивной меры.

Обратная сторона медали закона о конфиденциальности — это закон о свободе информации. Радикальную версию этого предлагает Дэвид Брин. Он рассуждает, что падающая стоимость приобретения, передачи и хранения данных сделает повсеместные технологии наблюдения доступными для властей, поэтому единственный реальный вопрос заключается в том, доступны ли они и для остальных из нас. Он рисует выбор между двумя будущими — одним, в котором граждане живут в страхе перед полицейским государством в стиле Восточной Германии, и одним, в котором чиновники несут ответственность перед общественным контролем. Камеры будут существовать: будут ли это камеры наблюдения или веб-камеры? Он утверждает, что по существу вся информация должна быть открытой — включая, например, все наши банковские счета. Более слабые версии этого были опробованы: налоговые декларации

публикуются в Исландии и в некоторых швейцарских кантонах, и эта практика сокращает уклонение, так как богатые люди боятся потери социального статуса, которую принесет искусственно заниженный заявленный доход.
Есть некоторые интересные инженерные вопросы. Например, в то время как осуждения за тяжкие преступления в США остаются в записях навсегда, во многих европейских странах есть законы о реабилитации правонарушителей, согласно которым большинство осуждений исчезают через период времени, который зависит от тяжести преступления. Но как можно обеспечить соблюдение таких законов сейчас, когда существуют поисковые системы в Интернете? Немецкая реакция заключается в том, что если вы хотите цитировать уголовное дело, вы должны получить официально обезличенную стенограмму из суда. В Италии осужденный бизнесмен добился решения суда об удалении из правительственного веб-сайта записи о его осуждении, после того как срок осуждения истек. Но если электронные архивы газет доступны для поиска в Интернете, какую от этого пользу — если только имена всех правонарушителей не будут заблокированы от электронных отчетов? Недавно было много дебатов по поводу мониторинга бывших сексуальных преступников, совершивших преступления против детей, с законами в некоторых штатах, требующими, чтобы реестры преступников были общедоступными, и бунтами в Великобритании после того, как воскресная газета назвала имена некоторых бывших преступников. Как можно реабилитировать преступников в мире с Google? Например, помечаете ли вы имена преступников в газетных отчетах о судебных процессах датой истечения срока и принимаете законы, обязывающие поисковые и архивные службы соблюдать их?
Суть в том, что даже если данные являются общедоступными, их использование все равно может вызывать правонарушения по европейскому законодательству о защите данных. Это вызывает своеобразные трудности в США, где суды последовательно толковали Первую поправку как означающую, что вы не можете остановить повторение истинных заявлений в мирное время, за исключением небольшого числа случаев.
Поэтому неудивительно, что текущая точка конфликта между Европой и Америкой по вопросам конфиденциальности касается Google. Непосредственный casus belli заключается в том, что законодательство ЕС требует удаления личных данных, как только они больше не нужны, в то время как Google создал свои системы для хранения таких данных, как потоки кликов, неопределенно долго. В течение 2007 года европейские органы по защите данных довели это до сведения Google, поисковая система предложила обезличивать потоки кликов через 18 месяцев. Учитывая сложность правильного осуществления контроля над выводами — заявление, безусловно, будет внимательно изучено

европейскими властями. Нет сомнений, что эта сага будет продолжаться. Даже в Америке был призыв от CDT и EFF к списку «Do Not Track», аналогичному списку «Do Not Call», чтобы люди могли отказаться, другие активисты не согласны, говоря, что это подорвет модель полезных веб-сервисов, оплачиваемых рекламой. В любом случае, менее одного процента людей используют программное обеспечение для блокировки рекламы. Нам придется подождать и посмотреть.

Итоги

Правительства и государственная политика все больше переплетаются с работой инженера по безопасности. «Крипто-войны» были предвестником этого, как и борьба за авторское право, DRM и Trusted Computing. Текущие проблемы также включают наблюдение, конфиденциальность, DRM, защиту потребителей и даже электронное голосование, приобретающие сопоставимую важность. Самый большой технический вызов, вероятно, будет связан с интеграцией систем и обеспечением (assurance). Десять лет назад обитатели разных островов в архипелаге безопасности все имели огромную уверенность в своих продуктах. Криптографы верили, что определенные шифры не могут быть взломаны, поставщики смарт-карт утверждали, что извлечение криптографических ключей, хранящихся в их чипах, абсолютно физически невозможно, а люди по безопасности печати говорили, что голограммы не могут быть подделаны без PhD по физике и оборудования на 20 миллионов долларов. На системном уровне тоже было много misplaced confidence (неуместной уверенности). Банки утверждали, что их банкоматы не могут даже теоретически сделать ошибочное дебетование, толпа по многоступенчатой безопасности продавала свой подход как решение для всех проблем защиты систем и люди предполагали, что оценка безопасности, проведенная лабораторией, лицензированной правительством развитой страны, будет как честной, так и компетентной. Все эти удобные старые уверенности испарились. Вместо этого безопасность стала частью более широкой проблемы надежности. Мы строим все лучшие и лучшие инструменты, и они помогают строителям систем подняться немного дальше на гору сложности, но в конце концов они падают. Пропорция крупных сложных системных проектов терпит неудачу, прямо как в 1970-х годах; но сейчас мы строим гораздо большие катастрофы.

Сложность — реальный враг безопасности. Различие между посторонними и инсайдерами раньше упрощало бизнес, но по мере того, как все связывается, оно быстро исчезает. Защита раньше основывалась на нескольких больших идеях и на предложениях, которые можно было сформулировать точно, в то

время как теперь предмет гораздо более разнообразен и включает много неточных и эвристических знаний. Жизненный цикл системы также меняется: в старые дни закрытая система разрабатывалась в конечном проекте, в то время как теперь системы эволюционируют и накапливают функции без ограничений. Изменения в характере работы значительны: в то время как раньше главный внутренний аудитор банка помнил бы все мошенничества за последние тридцать лет и не позволил бы отделу обработки данных повторять ошибки, которые их вызвали, новая корпоративная культура временной занятости и «perpetual revolution» (перманентной революции, как описал это Мао) уничтожила корпоративную память. Экономика будет продолжать обеспечивать построение небезопасных систем — и ответственность будет сбрасываться на других, когда это возможно. Правительства будут пытаться не отставать, но они слишком медленные, и их часто можно на время подкупить. Поэтому будет много регуляторных провалов тоже.

Чистый эффект всех этих изменений заключается в том, что защита информации в компьютерных системах больше не является научной дисциплиной, а инженерной. Инженер по безопасности двадцать первого века будет отвечать за системы, которые постоянно эволюционируют и сталкиваются с меняющимся спектром угроз. У него будет большой и постоянно растущий набор инструментов. Значительная часть его работы будет заключаться в том, чтобы не отставать технически: понимать последние атаки, учиться использовать новые инструменты и быть в курсе юридических и политических фронтов. Как и любой инженер, ему понадобится прочная интеллектуальная основа, он должен будет понимать основные дисциплины, такие как криптология, контроль доступа, информационный поток, сети и обнаружение сигналов. Ему также нужно будет понимать основы управления: как работают счета, принципы финансов и бизнес-процессы его клиента. Но самое главное будет способность управлять технологиями и играть эффективную роль в процессе эволюции системы для удовлетворения меняющихся бизнес-потребностей. Способность общаться с бизнес-людьми, а не только с другими инженерами, будет жизненно важна и опыт будет иметь огромное значение. Я не думаю, что кто-то с этой комбинацией навыков рискует остаться без работы — или заскучать — в ближайшее время.

Наконец, безудержный рост военно-промышленного комплекса безопасности после 11 сентября и вопиющее разжигание страха многими правительствами — это шрам на мире и на нашей профессии. У нас есть обязанность помочь ему зажить, и мы можем сделать это многими разными способами. В мире идет развитие дисциплин инженерии безопасности и экономики безопасности, чтобы мы могли сказать не только то, что работает в лаборатории, но и то, что может

быть сделано для работы в мире. Распространение знаний также важно — то что я делаю статьи по этой теме. Экономический рост также помогает, и образование: именно бедные и необразованные больше всего поддаются разжиганию страха (будь то от западных лидеров или от бен Ладена). По крайней мере, в странах с образованным населением, избиратели начали признавать излишества «Войны с террором» и справляться с ними. Точно так же, как отдельные люди учатся на опыте компенсировать наши психологические предубеждения и более рационально справляться с риском, так и наши общества учатся и адаптируются тоже. Демократия — это ключевой механизм для этого. Поэтому последний способ, которым инженеры по безопасности могут внести свой вклад, — это участие в политических дебатах. Чем больше мы можем вовлечь людей, которые ведут дискуссии о возникающих угрозах, тем быстрее наши общества адаптируются, чтобы справиться с ними.