Бёрд Киви

Гигабайты власти

Остальные, правда, предпочитали молчать, а коринфянин Сокл сказал вот что: "Поистине, скорее небо провалится под землю, а земля поднимется высоко на воздух над небом, скорее люди будут сжить в море, а рыбы – там, где раньше жили люди, чем вы, лакедемоняне, решитесь уничтожить свободу, восстановив господство тиранов в городах. Нет ведь на свете никакой другой более несправедливой власти и более запятнанной кровавыми преступлениями, чем тирания."

Геродот. История

Все имена и события, упомянутые в книге, являются подлинными. Любое совпадение с вымышленными персонажами и сюжетами, надо полагать, неслучайно.

Глава 0. Вчера-сегодня-завтра

Страницы жизни героя, 1895.
Самая знаменитая сточная яма США

Воскресным днем 1 января 1895 года в половине восьмого утра, в нескольких кварталах от вашингтонского Капитолия, в доме своих родителей на свет появился Джон Эдгар Гувер. Во всяком случае, так принято считать со слов самого Гувера, а он хорошо известен тем, что постоянно врал всю свою долгую жизнь.

Но, конечно же, это не самая главная особенность человека, вошедшего в мировую историю как самый знаменитый полицейский Соединенных Штатов Америки. Дж. Эдгар Гувер возглавил ФБР в возрасте 29 лет и умудрился сохранить свой пост на всю остальную жизнь. Его цепкие лапки, ухватившие кормило столь влиятельного в государстве органа, разжались лишь в результате естественной смерти, наступившей в возрасте 77 с лишним лет в мае 1972 года.

Несмотря на все демократические порядки «самой свободной страны мира», издавна практикующей профилактическую ротацию руководящих кадров, Гувер за почти полвека своего директорства в ФБР пересидел 8 президентов и 18 генеральных прокуроров. Достигнут же столь выдающийся результат был старым как мир способом – тщательным сбором и умелым использованием компромата на всех потенциальных противников, начиная с самых высших лиц государства и кончая любым мало-мальски известным журналистом.

Когда в 1960-е годы президента Линдона Джонсона в очередной раз спросили, доколе страна будет все это терпеть, тогдашний хозяин Белого дома произнес бессмертную фразу: «Таких людей, как Гувер, предпочтительнее держать внутри палатки, чтобы он мочился наружу, а не снаружи, чтобы он писал внутрь»…

Тема испражнений, судя по всему, возникала в связи со специфической личностью Гувера регулярно и как бы сама собой. Так, уже

после кончины непотопляемого директора ФБР, когда в 1974 году были обнаружены некоторые из его «секретных файлов» с компроматом, судья Лоуренс Зильберман, исполнявший в ту пору обязанности министра юстиции, высказался следующим образом: «Джон Эдгар Гувер был словно сточная яма, накапливающая грязь. Сейчас я полагаю, что он был самым худшим государственным деятелем за всю нашу историю».

Обман и Отрицание

В процессе пропагандистской подготовки военного вторжения США в Ирак, 8 октября 2002 года в американском Министерстве обороны было проведено на редкость интересное мероприятие. В этот день Пентагон устроил для прессы специальную презентацию, целиком посвященную методам «отрицания и обмана», практикуемым Ираком для сокрытия своего оружия массового поражения и баллистических ракет, как средств его доставки. Доклад-презентацию провел один из ответственных чинов РУМО, Разведывательного управления Министерства обороны США, доктор Джон Юречко. Личность докладчика здесь весьма показательна, поскольку Джон Юречко не является специалистом ни по баллистическим ракетам, ни по оружию массового уничтожения. Этот представитель разведслужбы, уже не в первый раз выступающий перед журналистами, является начальником отдела по методам ведения информационной войны или, говоря попросту, специалистом по дезинформации [KR02].

Имеет смысл пояснить, что конкретно принято понимать под «ОиО», т.е. «отрицанием и обманом» (по-английски «DD», или Deception and Denial). В сущности, ничего особого хитрого за данным термином не скрывается и, как заметил тот же Юречко, эти методы так же стары, как и вся зафиксированная история человечества. Вкратце, под «отрицанием» понимаются такие методы, которые используются страной для утаивания своих государственных и военных секретов, в частности, от устремлений зарубежных разведок. «Обман», в свою очередь, это манипуляция информацией и восприятием для того, чтобы вынудить обманываемые государства к определенным действиям или, наоборот, к бездействию, в зависимости от намерений манипулятора.

Джон Юречко

Понятно, что обман и отрицание взаимосвязаны. Отрицание – это

базис для успешных операций по обману. Невозможно манипулировать истиной и ложью до тех пор, пока истина предварительно как следует не замаскирована. Понятно и то, что спецслужбы США являются чрезвычайно искушенными в «ОиО», умудряясь в течение многих лет весьма успешно скрывать многомиллиардные разработки нового оружия или масштабные тайные операции в разных регионах планеты. Но доклад Джона Юречко, ясное дело, был посвящен не этой стороне его работы, а методам «ОиО», успешно применявшимся Ираком для обмана зарубежных разведслужб и инспекторов ООН.

Хотя, по оценкам этого искушенного эксперта, действия Ирака в области «ОиО» зачастую выглядели довольно топорно, тем не менее Юречко вынужден признать, что они успешно помешали как международным инспекторам, так и западной разведке представить хоть сколько-нибудь серьезные свидетельства или фотографии, способные убедить скептиков в нарушении Саддамом Хусейном резолюций ООН, запретивших создание оружия массового поражения. По сути дела, с тех пор как предыдущая смена инспекторов ООН покинула Ирак в 1998 году, в этой стране так и не удалось выявить ничего по-настоящему компрометирующего. Тем не менее, специальный отчет ЦРУ, представленный политическому руководству США непосредственно накануне презентации Юречко, утверждал, что Багдад по-прежнему утаивает крупные программы по созданию ОМП.

В докладе Юречко эти выводы разведки были обоснованы весьма специфическим образом – длинным перечислением прошлых грехов режима Саддама Хуссейна, которых действительно было в достатке. После чего сделан элегантный переход к нынешним, как следует понимать, методам обмана, что надо процитировать дословно: «Вот один из типичных и относительно нехитрых методов „ОиО“, а именно маскировка. На этом слайде – пример предполагаемого иракского объекта, где создается биологическое оружие. Посмотрите внимательно на это фото. Одна из интересных особенностей объекта – его местоположение. Он замаскирован посреди жилого района. Здания ничем не выдают себя по внешнему виду. В объекте вообще нет ничего примечательного»…

На этом месте, казалось бы, Юречко должен был поведать о том, как доблестная разведка все же сумела выявить опаснейшую фабрику смертоносных вирусов в жилом квартале ни о чем не подозревающих мирных людей. Но вместо этого лектор многозначительно цитирует знаменитый афоризм покойного Амерона Кэппса, эксперта по контролю за вооружениями, который однажды изрек: «Мы никогда не находили ничего из того, что наши противники успешно скрывали». Из чего внимательный слушатель легко сделает вывод, что никакого биологического оружия разведка в действительности не выявила. Ни в этом жилом квартале, ни где-либо еще.

Но сам Юречко, конечно, ничего подобного не произносит, зато тут же приводит другую цитату, на этот раз из высказываний Тима Тревэна, бывшего инспектора ООН, который как-то изрек, что если в стране существуют недекларированные и невыявленные объекты оружия массового уничтожения, то их по определению невозможно инспектировать или отслеживать. А значит, делает вывод докладчик, практика инспекций

не может дать никаких гарантий того, что страна не занимается запрещенной деятельностью.

Короче говоря, весь большой доклад доктора Юречко с убедительной демонстрацией спутниковых снимков, не доказывающих, по сути, абсолютно ничего, сам по себе стал классическим примером дезинформационной операции государства по обману и отрицанию. Обману собственного народа об истинных целях уже подготовленной иракской войны и отрицанию вполне очевидного факта – что у американских спецслужб нет ни одного убедительного доказательства нарушений Саддамом Хусейном резолюций ООН. А у США, соответственно, ни единой достойной причины для развязывания войны и убийства тысяч ни в чем не повинных людей.

Да и могут ли вообще существовать для этого достойные причины?

Одной ногой в будущем

Действие недавнего фильма Стивена Спилберга «Особое мнение» (Minority Report) происходит в 2054 году. Если кто почему-либо не в курсе, то это – фильм-предупреждение, фильм об обществе, тотально контролируемом органами безопасности. Об обществе, граждане которого практически полностью утратили тайну личной жизни. Режиссер вынашивал замысел этой картины не один год и, стремясь как можно более убедительно изобразить даже мелкие бытовые реалии сравнительно недалекого будущего, специально созывал в 1999 году на трехдневный коллоквиум две дюжины известных футурологов. В ходе того своеобразного «мозгового штурма» была сделана попытка набросать наиболее вероятные черты технологий грядущего.

Стивен Спилберг

Споры, как вспоминает Спилберг, были самые яростные, и все же в некоторых своих прогнозах футурологи оказались на редкость единодушны. Например, в том, что техника будущего непременно будет настраиваться индивидуально на каждого конкретного человека. Естественно, эта идея не могла не найти яркого отражения в кинокартине. А чтобы стало ясно, насколько быстро прогнозы визионеров воплощаются в жизнь, достаточно лишь взглянуть на небольшой тест, предложенный в 2002 году читателям одного из популярных изданий в связи с выходом на

экраны фильма Minority Report. Спрашивается, какие технологии уже реализованы, а какие появятся в обозримом будущем:

- банкомат, предоставляющий клиенту банка доступ к его счетам путем сканирования радужки глаза;
- кассовый аппарат в супермаркете, позволяющий оплатить покупку бакалейных товаров простым прикосновением пальца к биометрическому сенсору;
- электронные журналы, мгновенно доставляющие читателям интересующие их новости по беспроводным сетям;
- топографические рекламные щиты, обращающиеся по имени к оказавшемуся поблизости прохожему.

Две первые технологии уже реализованы сегодня, две следующие показаны в MR, причем третья – уже на подходе, и лишь четвертая ожидает нас, вероятно, в грядущем. Тенденция все более глубокой «персонализации обслуживания» вполне отчетливо обозначена в нынешних высокотехнологичных продуктах. Например, персональные видеорекордеры (PVR) вроде тех, что изготовляют компании TiVo и SonicBlue, умеют по-тихому собирать данные об индивидуальных предпочтениях своих владельцев, предоставляя возможность рекламодателям более конкретно и целенаправленно адресовать свои обращения к зрителям. А следующее поколение сотовых телефонов оснащается функциями точного географического позиционирования, давая магазинам потенциальную возможность зазывать находящихся поблизости прохожих, суля им заманчивые, но краткосрочно действующие бонусы и скидки в течение ближайшего получаса. Текущие социологические исследования показывают, что ради какой-нибудь постоянной 10-15-процентной скидки большинство рядовых потребителей готово с радостью отказаться чуть ли не от всех своих прав на тайну личной жизни, предоставив торговцам любую интересующую их информацию – о вкусовых предпочтениях, ближайших планах, распорядке дня, кредитоспособности и так далее [FS02].

Всякому, кто внимательно наблюдает за происходящим, достаточно очевидно, что благодаря технологиям тайна личной жизни размывается и исчезает не только для настырной коммерции. Жизнь людей становится все прозрачнее и для не менее (скорее, более) любопытных правоохранительных органов, понемногу обретающих возможность проконтролировать каждого человека практически в любом месте и в любой момент времени. Только в этом случае роль «морковки», обеспечивающей добровольный отказ от прав на свободу, играют уже не скидки-бонусы, а некая гипотетическая «всеобщая безопасность», гарантируемая пастырями от власти своему безразлично-согласному стаду.

У многих есть ощущение, что все мы одной ногой уже вступаем примерно в то будущее, которое изобразил Спилберг в MR. Сам режиссер не скрывает, что всерьез озабочен ходом реальных событий, и честно признается, что побаивается реальности нарисованных картин будущего: «Предсказания Джорджа Оруэлла сбываются, но не в XX, а в XXI веке. Большой Брат уже следит за нами, и та небольшая приватность, которая есть у нас сейчас, полностью испарится лет через 20-30, потому что технология позволит смотреть сквозь стены и крыши, заглядывать в самые

сокровенные тайны нашей личной жизни, в святая святых семьи» [BW02].

Никто, наверное, не станет сегодня утверждать, что страхи Спилберга абсолютно безосновательны. И картины-предупреждения, подобные Minority Report, время от времени создавать необходимо уже затем, чтобы люди наглядно видели, куда способен увести общество неудержимый прогресс технологий.

Однако, имеет смысл всегда помнить, что никакой консенсус даже самых авторитетных футурологов планеты не в силах предсказать реальное будущее человечества. Ведь самая главная особенность нашей истории – это ее полнейшая непредсказуемость. Достаточно вспомнить события бурного XX века. Столь радужные надежды на торжество прогресса, науки и просвещения в самом начале столетия, а вместо этого – чудовищная по масштабам жертв и разрухи мировая война. Через пару десятков лет – еще одна, даже более страшная глобальная бойня. В середине века – мир, расколовшийся на два непримиримых враждующих лагеря и подготовка к третьей, теперь уже ядерной мировой войне. А вместо этого – еще через полстолетия – фактически полный, никем не предсказанный коллапс коммунистической системы, глобализация экономики и единое информационное пространство планеты.

В данной книге не дается никаких предсказаний на будущее. Но здесь достаточно тщательно собраны факты о реальных возможностях, недостатках и перспективах современных информационных технологий, столь серьезно влияющих ныне на развитие человеческого общества. И среди этих фактов время от времени непременно мелькают и такие, что окажут очень серьезное воздействие на мир, каким он станет еще через 50 лет.

Глава 1. Матрица, ее мутанты и хакеры

Страницы жизни героя, 1917. Лучше бы он остался библиотекарем

В июле 1917 года Эдгар Гувер закончил юридический факультет Университета Джорджа Вашингтона и в том же месяце по протекции дяди-судьи начал работу в Министерстве юстиции США. Все четыре года в университете Гувер учился по вечерам, а днем должен был работать – курьером в Библиотеке Конгресса, – поскольку семья постоянно испытывала серьезные денежные затруднения из-за плохого здоровья отца, Дикерсона Гувера.

Карьера Гувера в министерстве развивалась стремительно. Всего через два года тогдашний генеральный прокурор Александр Палмер сделал смышленого молодого человека своим помощником по особым поручениям. В этой должности Гувер стал отвечать за новое подразделение, Отделение общей разведки, сформированное для сбора информации на «революционные и ультрареволюционные группы». Эта работа, по сути дела, идеально подошла Гуверу, поскольку тот всегда получал огромное удовольствие от составления картотеки на книги личной библиотеки и от работы с каталогами огромного книгохранилища Библиотеки Конгресса. Теперь он получил возможность использовать свой большой опыт для

составления огромной картотеки на коммунистов, анархистов и прочих левацких «подрывных элементов».

В течение нескольких лет под руководством Гувера была составлена гигантская проиндексированная картотека почти на полмиллиона (450 тысяч) имен людей предположительно левых убеждений. Примерно на 60 000 из них, расцененных Гувером в качестве наиболее опасных, были собраны подробные биографические данные. С юных лет напуганный красной угрозой, Гувер убедил Палмера, что всех подобных людей необходимо хватать и высылать из США. В день второй годовщины русской Октябрьской революции, 7 ноября 1919 года, полиция одновременно арестовала в 23 городах свыше 10 000 человек, подозревавшихся в большевистских, анархистских и прочих леворадикальных взглядах. Аресты сопровождались побоями и чрезвычайно жестоким обращением, войдя в историю как один из наиболее, вероятно, чудовищных прецедентов нарушения гражданских прав в США в XX веке. Подавляющее большинство арестованных были американскими гражданами, выслать их из страны не было никаких оснований, так что в конечном итоге власти были вынуждены их отпустить. Но Эдгар Гувер в результате получил в свое распоряжение имена сотен адвокатов, вызвавшихся представлять интересы арестованных в суде. Всех этих адвокатов, так же как и журналистов, и всех прочих, подавших голос сочувствия в адрес репрессированных, также занесли в постоянно растущую базу данных.

Когда в 1921 году Отделение общей разведки вошло в состав Бюро расследований Министерства юстиции, Гувера произвели в заместители директора Бюро. В 1924 году он уже сам стал директором, постоянно озабоченным улучшением информационного обеспечения расследований. В 1926 году Эдгар Гувер создал в Бюро базу отпечатков пальцев, которая со временем стала самым большим в мире хранилищем подобного рода.

В 1975 году, три года спустя после смерти Гувера, американский Конгресс отдал распоряжение произвести тщательную проверку всех досье по тематике «внутренняя безопасность», хранящихся в десяти основных управлениях ФБР. В результате этой проверки выяснилось, что свыше двадцати процентов всех усилий Бюро было направлено на охоту за предположительно «подрывными элементами». Причем реальный криминал был обнаружен лишь в четырех из девятнадцати тысяч семисот расследований, да и выявленные четыре случая не имели ничего общего с национальной безопасностью, шпионажем или терроризмом.

Похоже, для США было бы гораздо лучше, если бы Эдгар Гувер так и остался библиотекарем.

Матрица – перезагрузка TIA

Явление TIA

В ноябре 2002 года мир узнал о новой, чрезвычайно амбициозной инфотехнологической программе Пентагона, получившей название «Тотальная информационная осведомленность» или кратко TIA, от Total Information Awareness. Целью этой программы, запущенной в Агентстве

передовых военных исследований (DARPA), виделось создание гигантской компьютерной системы для наблюдения за многими миллионами граждан США и других стран мира – для предотвращения, как объявлено, будущих террористических актов на этапе их подготовки. Под «наблюдением» здесь понимаются постоянные анализ и оценка данных из множества сведенных воедино информационных баз, правительственных и коммерческих, содержащих самые разные сведения о личной жизни граждан по всему миру.

Для общего руководства проектом в DARPA было создано специальное Управление информационной осведомленности, возглавил которое адмирал Джон Пойндекстер, в свое время получивший очень громкую скандальную известность в качестве советника по национальной безопасности президента Рейгана. По словам Пойндекстера, его задача – создать новую технологию для эффективного просеивания информации, накапливаемой в «сверхбольших» хранилищах данных и в объединенных сетью компьютерах. Такая технология позволит отыскивать характерные следы назревающих угроз среди множества ежедневных транзакций – покупок литературы или химикатов, бронирования билетов или мест в гостинице, обращения к врачам или консультантам. Власти уже достаточно давно имеют доступ к массе всевозможной информации о деятельности конкретных установленных террористов, но для этого, говорит Пойндекстер, каждый раз приходится либо получать ордер в суде (на территории США), либо предпринимать достаточно утомительные усилия по дипломатическим или разведывательным каналам (за рубежом). Новая же система TIA, как виделось ее создателям, позволила бы достигать нужных целей намного более эффективным способом [RO02].

Суть новой технологии не столько в отслеживании уже известных людей, догадывающихся, возможно, что за ними следят, сколько в выявлении «подозрительных» структур в поведении всех людей вообще. Иначе говоря, всякий заказ по кредитной карте, всякая подписка на журнал или газету, всякий выписанный рецепт на медикаменты, всякий вебсайт, посещаемый в Интернете, всякая электронная почта, входящая или исходящая, всякий взнос в банк или съем денег, всякая запланированная поездка – все эти данные, фиксируемые в каких-то базах данных, становятся предметом пристального интереса спецслужб и объектом обработки для их специального аналитического инструментария.

Вдохновленные грандиозностью задачи, создатели TIA украсили, как смогли, свой веб-сайт богатой и многозначительной символикой. В качестве эмблемы проекта был выбран древний масонский знак «всевидящего ока» – глаз в вершине пирамиды, пристальным взором осматривающий земной шар. Девиз тоже подобрали подходящий – латинское изречение Scientia Est Potentia (Знание – сила), обычно приписываемое Фрэнсису Бэкону.

Чего же не удалось предусмотреть искателям «тотального знания-силы», так это в высшей степени негативной реакции общественности на программу TIA. Мало того, что создается технология для грандиозного вторжения государства в частную жизнь граждан, так еще во главе проекта поставили отъявленного прохиндея и лжеца Пойндекстера. Тут же всплыли все известные нелицеприятные факты из

биографии отставного адмирала. Как бывший глава совета национальной безопасности в Рейгановской администрации, Джон Пойндекстер в 1990 году был осужден федеральным судом по пяти уголовным преступлениям, включая ложь в показаниях Конгрессу, уничтожение компрометирующих официальных документов и препятствование парламентскому расследованию в деле «Иран-Контрас». Пойндекстер был одной из центральных фигур в этом самом громком политическом скандале США 1980-х годов, включавшем тайную продажу оружия Ирану с переводом полученных денег на помощь контрреволюционному движению в Никарагуа, активное участие ЦРУ в подпольном наркобизнесе и другие нелегальные формы деятельности спецслужб для тайного финансирования своих операций. Покидая Белый дом, президент Джордж Буш-папа, сам в прошлом директор ЦРУ, амнистировал всех, кто был осужден по этому громкому делу, а многие шокирующие подробности этой истории так и не стали достоянием широкой общественности.

INFORMATION AWARENESS OFFICE
Scientia Est Potentia.

Исходный вид оформления веб-сайта TIA

В TIA достаточно быстро поняли, что затеянная работа была подана неудачно – и уже в декабре интернет-публика стала отмечать заметные косметические коррективы в оформлении веб-сайта проекта. Сначала исчезли биографии главных создателей программы, затем существенно сократился перечень конкретных типов данных, просеиваемых фильтрами TIA. Наконец, к концу декабря, вместе с другими содержательными деталями исчезла и «тайно-масонская» эмблема с пирамидой и земным шаром. Сам же проект, тем не менее, продолжал развиваться своим ходом, но теперь в менее доступной взору общественности форме [DM02].

Подозреваются все

В апреле 2003 года стали известны некоторые подробности о том, как происходит наполнение централизованной базы данных файлами со списками потенциально «неблагонадежных» граждан. В Нью-Йорке забили тревогу правозащитники, установившие, что полиция, в массовых количествах арестовывавшая участников демонстраций против войны в Ираке, задерживала людей в участке, если те отказывались помимо обычных имени и адреса сообщать о себе массу дополнительных сведений: где они учились, членами каких организаций состоят, участвовали в акциях протеста прежде и так далее. Здесь уместно вспомнить, что согласно официальным статистическим данным в 2002 году в тюрьмах США содержалось свыше 2 миллионов граждан страны, что при населении 286 миллионов составляет около 0,7% от общего числа. Для сравнения в Китае, который многими расценивается как авторитарное полицейское государство, насчитывается 1,4 миллиона заключенных при населении 1,3 миллиарда, т.е. около 0,1% [NY03], [PS02].

Для повышения эффективности «поиска врагов» в марте 2003 г. Министерство юстиции США существенно понизило планку достоверности информации, вносимой в национальную базу данных о преступности NCIC (National Crime Information Center). До введения новых правил там содержалось 39 миллионов записей о зарегистрированных преступлениях и преступниках, теперь же туда вносится не только абсолютно достоверная информация, но и непроверенные сигналы, расценивающиеся как серьезные. Помимо этого, в ФБР составлен совершенно необозримый список «подозреваемых в терроризме», состоящий из 13 миллионов человек, т.е. почти 5% от всего населения США. Сведущие люди, умеющие считать, тут же несложными арифметическими калькуляциями наглядно продемонстрировали, сколь нелепы попытки пристально следить за 1/20 долей страны и к сколь чудовищным ошибкам это будет постоянно приводить [BS03], [JM03].

Подобные расчеты, однако, убеждают кого угодно, но только не тех, кто формирует тотальную супербазу. Весной 2003 года стало известно, что едва ли не за год до объявления инициативы TIA по заказу правительства американские частные компании интенсивно, тайно и в массовых объемах начали скупку информации о гражданах иностранных государств. В частности, фирма из Атланты ChoicePoint продала «заинтересованным правительственным ведомствам» США свыше сотни миллионов собранных ею записей о гражданах Бразилии, Мексики, Колумбии, Венесуэлы, Коста-Рики, Гватемалы, Гондураса, Сальвадора, Никарагуа. Понятно, что ChoicePoint специализируется на государствах Латинской Америки, но наверняка есть и другие фирмы, специализирующиеся на прочих регионах планеты. Ведь теперь фактически вся заграница – это потенциальная угроза Америке.

Больной скорее жив, чем умер

Трудно сказать, чем именно система TIA не понравилась американским конгрессменам, но летом 2003 года стало понятно, что будущее программы далеко не столь радужно, как виделось ее идеологам. Пытаясь спасти ситуацию, они и название сменили на менее вызывающее – теперь уже не

тотальная, а «Информационная осведомленность о терроризме» (Terrorism Information Awareness). И начальника программы сменили, вновь убрав в тень одиозную фигуру адмирала Пойндекстера. Ничего не помогло – система TIA так и не смогла стяжать ничего, кроме чрезвычайно негативной прессы и критических отзывов конгрессменов, усмотревших в гипер-базе данных чистую оруэлловщину и отчетливые контуры тоталитарного Большого Брата.

Официальная смерть TIA наступила 24 сентября 2003 года. В этот день на совместном заседании обеих палат американского Конгресса большинством голосов было принято решение о полном лишении финансирования в 2004 году как программы TIA, так и ее организующей структуры – Управления информационной осведомленности. Правда, в действительности столь эффектное решение вовсе не означало прекращение разработки комплекса исследовательских проектов, входивших в состав TIA. Просто их раскидали по другим управлениям и агентствам. В результате ситуация стала скорее даже хуже, чем была, поскольку работы государства, сосредоточенные на копании в личной жизни граждан и попавшие под огонь критики, теперь стали практически невидимыми для публики. А значит, и намного меньше доступными для контроля со стороны общества.

Отныне известно лишь то, что восемь самостоятельных программ, входивших в состав TIA, будут продолжены в других подразделениях DARPA, т.е. их финансирование просто будет осуществляться по другим каналам. Кроме того, родственные исследования будут осуществляться в рамках значительно более скрытной программы спецслужб, известной под названием NFIP или National Foreign Intelligence Program. Эту программу совместно ведет целая группа таких агентств, как Центральное разведывательное управление, Федеральное бюро расследований и Агентство национальной безопасности. Бюджет программы полностью засекречен, также как и подробное раскрытие целей совместной работы, скрываемой за набором примерно таких слов – «инструментарий для обработки, анализа и совместных действий в контртеррористической внешней разведке». В соответствии с новыми законами США, следует напомнить, теперь ничто не мешает использовать любые инструменты NFIP и внутри страны [SC03].

MATRIX сегодня – это TIA вчера

Случайно или нет, но ровно через год после явления народу TIA, в ноябре 2003 стало известно о новой реинкарнации той же самой, в сущности, идеи, но теперь уже под видом не государственной, а коммерческой программы. Программа носит на редкость подходящее название MATRIX, как акроним полного названия – Multistate Anti-Terrorist Information Exchange, т.е. «Антитеррористический информационный обмен множества штатов». Согласно ее создателю, флоридской компании Seisint, MATRIX представляет собой крупнейшую на этой планете базу данных, содержащую на тот момент свыше 20 миллиардов записей. Работая совместно с Департаментом правоохранительных органов Флориды (FDLE) и получив 12 миллионов долларов из федерального бюджета, фирма

Seisint разрабатывала MATRIX так, чтобы система могла накапливать досье на каждого отдельно взятого гражданина страны. Естественно, вся работа затеяна лишь для того, чтобы помочь стране в борьбе с терроризмом. Ну а попутно, как приятный бонус, эта же система поможет эффективно выявлять бандитов, рэкетиров, мошенников и прочих педофилов.

Небезынтересно отметить, что MATRIX имеет большое сходство с TIA не только в функциональной части, но и в крайне сомнительном моральном облике главного инициатора проекта. Человек, стоящий за MATRIX – это весьма состоятельный флоридский предприниматель Хэнк Эшер, щедрый спонсор нынешнего политического руководства штата (губернатор Флориды Джеб Буш – брат 43-го и сын 41-го президентов США) и большой друг недавно ушедшего на пенсию главы FDLE. А кроме того, как недавно выяснилось, в начале 1980-х годов – активный наркодилер, лично доставивший в США из Колумбии несколько самолетов, загруженных кокаином (этим бизнесом, напомним, активно занималось в ту пору ЦРУ).

Общенациональное расширение флоридской компьютерной базы Seisint, поначалу созданной для FDLE, происходило примерно по следующей схеме. Администрациям других штатов предлагалось за свой счет прислать имеющиеся у них файлы с данными обо всех выданных водительских лицензиях, обо всех зарегистрированных машинах, а также имеющие архивы о криминальной деятельности. В Seisint смешивают их с аналогичными данными других штатов и со всеми «коммерческими» базами данных, которые компания уже успела приобрести и скомпилировать. После чего вновь подключившийся штат получает доступ ко всему хранилищу, но не бесплатно, а, скажем, за полтора миллиона долларов в год.

В результате, как обещают в Seisint и FDLE, пользователь MATRIX элементарным нажатием кнопки получает доступ к самой разнообразной информации на интересующих людей: номера социального страхования, фотографии, даты рождения, нынешние адреса и старые адреса за последние 30 лет, телефонные номера и имена других людей, живущих по тому же адресу и по соседству. А также: заявления на получение кредита и отчеты по выплатам, описание принадлежащей собственности, когда и где она куплена, сколько и кому уплачено вместе с суммами выплаченных налогов, история нарушения правил при вождении транспортных средств с полной информацией о правах и зарегистрированных на это имя машинах. Ну, и так далее, включая всю перечисленную информацию о родственниках, близких и соседях.

MATRIX MultistateAnti-TeRrorism Information EXchange

География « Матрицы »

Трудно сказать, как далеко в другие штаты успела бы распространить свои сети система MATRIX, если бы информация о ней не начала появляться в прессе, породив журналистские расследования. Именно одна из флоридских газет раскопала материал о криминальном прошлом Хэнка Эшера, после чего тот резко разорвал все связи с компанией Seisint. Но волна уже пошла, и местные власти ряда штатов начали забирать обратное данное поначалу согласие. Так, после поднятого журналистами шума генеральный прокурор Джорджии постановил, что передача на сторону информации о водительских лицензиях и зарегистрированных машинах нарушает законы штата. Дальше – больше. Из 14 штатов, успевших присоединиться к МАТРИЦЕ, за несколько месяцев отвалились Орегон, Алабама, Южная Каролина, Кентукки и Луизиана, найдя для этого в каждом случае свои причины. [СМОЗ]

Эта история чрезвычайно наглядно продемонстрировала, насколько охотно власти идут на нарушение собственных законов и вторжение в частную жизнь граждан, но только при единственном важном условии – чтобы об этом ни в коем случае не узнали ни пресса, ни публика, приходящая на избирательные участки.

Радиочастотное число зверя

RFID многоликая

В ноябре 2003 года почти одновременно в разных точках планеты прошли два независимых друг от друга мероприятия, тесно связанных, тем не менее, единым предметом обсуждения. Сначала, 15 ноября в Массачусетсом технологическом институте, Кембридж, прошел семинар «RFID и приватность» (от RadioFrequency IDentification – технология радиочастотной идентификации), в дискуссиях которого приняли участие ученые-разработчики, представители продвигающих технологию компаний, правозащитники и журналисты. Подобный научно-практический семинар организован впервые, однако актуальность его очевидна практически для всех, кто понимает, сколь серьезную угрозу тайне личной жизни представляют новейшие технологии бесконтактной идентификации

и базы данных на этой основе.

Всего несколькими днями позже, 20-21 ноября, по другую сторону Атлантики, в парижском отеле «Шарль де Голль» состоялся большой международный конгресс ID World 2003. Под общим девизом «Революция идентификации в реальном и цифровом мирах» участники форума обсуждали достижения и перспективы бурно развивающихся ныне технологий RFID, биометрии, смарт-карт, а также в целом сбор информации на основе этих технологий.

Поскольку оба форума прошли практически в одно время, прежде всего бросилось в глаза то, сколь по-разному оценивают технологию бизнес-круги, в зависимости от места, где она обсуждается. На семинаре в МТИ много выступали правозащитники, рассказывавшие о лицемерии, двуличности и лжи, сопровождающих внедрение новых технологий идентификации. А представители бизнеса, в свою очередь, напирали на то, сколь сильно преувеличивают неспециалисты опасности чипов идентификации, сколь слабым и подверженным помехам является излучение RFID, как много способов сделать чип бездействующим и сколь легко его блокируют всякие материалы – от жидкостей и человеческого тела до пластмасс и фольги [MAO3].

Зато на парижском конгрессе ID World доклады рисовали захватывающую картину победного шествия новаций едва ли не во всех мыслимых сферах – от торговли и учета производства до охраны объектов. Вообще говоря, впервые технологию радиочастотной идентификации в задачах отслеживания перемещений и контроля доступа начали применять еще в 1980-е годы. Основу систем RFID составляют устройства-считыватели (ридеры) и «умные метки», т.е. микрочипы с подсоединенной антенной. Когда такая метка приближается к ридеру, она активизируется и радиоволнами выдает считывателю информацию, хранящуюся в памяти чипа. К концу 1990-х годов технология RFID достигла такой степени миниатюризации, что чипами-ярлыками в принципе можно помечать уже что угодно – от людей и одежды до денежных знаков и насекомых [SI03].

Например, Европейский центральный банк (ECB) активно сотрудничает с ведущими европейскими изготовителями микросхем, создающими RFID, намереваясь в ближайшем будущем с помощью этой технологии защитить от подделки единую европейскую валюту, запрессовывая чипы непосредственно в банкноты евро. Все работы по принципиально новой защите бумажных денег ведутся в обстановке повышенной секретности, поэтому представители ECB крайне неохотно соглашаются на комментарии, дают уклончивые ответы и предпочитают говорить сразу о множестве современных мер защиты банкнот, включая рельефную печать и топографические полосы. Что же касается микрочипов, то, согласно информации специализированных изданий по микроэлектронике, над этой задачей по заказу Европейского Центробанка работают германская фирма Infineon Technologies AG и голландская Philips Semiconductors NV. Что же касается конкретных сроков, то анонимные источники в ECB в качестве ориентировочной даты выпуска евроденег с встроенными чипами называют 2005 год [JY01].

Одна из самых многообещающих сфер приложения RFID – это

автоматизация материального учета. В 1999 году в результате совместной договоренности множества крупных компаний при Массачусетском технологическом институте была сформирована исследовательская группа Auto-ID Center. В качестве главных задач перед этим центром были поставлены разработка и полевые испытания новой разновидности компьютерных сетей, способных при помощи чипов и считывателей RFID отслеживать расположение и перемещение по складам или магазинам огромной массы штучных объектов, таких как бритвы, бутылки или ботинки. Главными спонсорами Auto-ID-центра стали такие фирмы и торговые сети, как Coca-Cola, Gillette, Target, Home Depot и Wal-Mart, которые вложили в проект свыше 20 миллионов долларов. В октябре 2003 разработанная в Auto-ID Center технология сочтена настолько зрелой, что ее решено перевести на следующую ступень развития. Все разработанные в МТИ стандарты и прочие обязанности по поддержке RFID переданы фирме EPCglobal, совместному предприятию организаций Uniform Code Council и EAN International, ведающих стандартами штрих-кодов [GI03].

Грандиозные перспективы для RFID видятся в самых разных областях индустрии. Так, в январе 2003 г. автошинный гигант Michelin объявил о начале испытаний чипов-идентификаторов, вулканизируемых непосредственно в резину покрышек. Радиочастотная микросхема-идентификатор изготовляется компаниями Fairchild Semiconductor International и Philips, имеет размер со спичечную головку и специально предназначена для отслеживания индивидуальной судьбы каждой из автопокрышек. Для этого в чипе хранится уникальный номер шины, который можно привязать к номеру автомобиля; данные о том, где и когда покрышка сделана; максимально допустимое давление; размеры и так далее. Всю эту информацию можно считывать и обновлять дистанционно с помощью ручного прибора. Кроме того, компании Philips и Texas Instruments разработали для шин специальные чипы RFID с датчиками температуры и давления, по радио связанные с бортовым компьютером автомобиля, чтобы водитель мог по приборной панели отслеживать состояние каждой из шин индивидуально. Правда, в мишленовскую резину такие датчики пока встраивать не планируется, поскольку для начала компания хочет убедиться, найдут ли спрос шины с простыми чипами-идентификаторами. Пока что упрочненные микросхемы RFID для шин – удовольствие довольно дорогое, добавляющее к стоимости покрышки несколько долларов. Точно еще неизвестно, захотят ли автомобильные компании платить дополнительные деньги за новые возможности, однако в Michelin уверены, что цена существенно упадет, если дело дойдет до массового производства (ежедневно здесь выпускается 800 000 шин) [RF03].

Периодически поступают известия и о весьма экзотических приложениях RFID. Вроде, к примеру, оригинальной системы iGlassware, наделяющей зачатками интеллекта самые обыкновенные стаканы и фужеры. Благодаря этому изобретению американца Пола Дитца из научно-исследовательского центра MERL, бармены и официанты в ресторанах смогут теперь мгновенно узнать, у кого из посетителей опустело в бокале, мгновенно подскочить, вновь наполнить посуду и продемонстрировать тем самым высочайший класс обслуживания клиентов

в заведении. В системе iGlassware микрочип с крошечной катушкой антенны крепятся к дну стакана в упаковке, защищающей электронику от посудомоечной машины. Специальное прозрачное покрытие стакана играет роль электродов конденсатора, а жидкость, заполняющая посуду, в данном случае выполняет функцию диэлектрика, перетекание которого в желудок клиента изменяет емкость конденсатора. Поскольку реагирующий на эти перемены микрочип каждого стакана имеет индивидуальный идентификатор, а в каждый стол встроен транслятор-радиопередатчик, то на пульте у бармена или метрдотеля ведется постоянный учет степени наполненности посуды клиентов. И как только емкость конденсатора в одном из стаканов уменьшается до критической, официант получает сигнал с координатами стола и места, требующего, возможно, налить «еще по одной». Электропитание чипов в стаканах осуществляется за счет радиочастотного сигнала, излучаемого передатчиком в столе. Эксперты по менеджменту ресторанов и отелей проявили к новинке самый горячий интерес, назвав ее «долгожданным и весьма многообещающим приложением» [YB02].

Ну и, конечно же, нельзя не сказать о масштабном распространении RFID за последние годы в торговле и системах оплаты. Так, компания ExxonMobil с большим успехом внедрила систему Speedpass на более чем 7500 своих автозаправочных станций. Благодаря этому водители мгновенно расплачиваются за бензин, просто проведя брелоком или карточкой с RFID-чипом вблизи считывателя – соответствующая сумма через компьютер автоматически снимается с банковского счета клиента. Эту же систему Speedpass недавно реализовали в более чем 400 закусочных McDonald's в Чикаго, где теперь клиентам предоставлена возможность моментально расплачиваться за свои гамбургеры и картошку-фри.

Весьма похожую систему под названием PayPass начала внедрять сеть MasterCard, встраивая RFID непосредственно в кредитную карточку. Благодаря чипу-идентификатору владелец освобождается от необходимости вводить код PIN, подписывать чек или как-либо еще взаимодействовать с персоналом – если в точке расчета, конечно, уже имеется соответствующий считыватель. Поскольку при таком подходе нужды в пластиковой карточке, как таковой, в общем-то уже нет, в MasterCard рассматривают и иные варианты реализации RFID, вроде встраивания микрочипов в авторучку (для солидных мужчин) или же, к примеру, в серьги (для дам). Все эти предметы, правда, несложно потерять, поэтому в конечном счете банковские институты очень устроил бы вариант с имплантацией RFID непосредственно в тело человека.

И вот тут в центре внимания оказывается американская фирма Applied Digital Solutions (ADS), на сегодняшний день единственная, кто уже занимается подкожными инъекциями RFID-микросхем не только животным, но и людям. Глава ADS Скот Силвермен тоже выступал на парижском конгрессе ID World, где сообщил, что его фирма уже готовится к запуску в обозримом будущем специального сервиса VeriPay, который позволит людям расплачиваться за товары и услуги с помощью чипа, имплантированного в руку [JU03].

Время двойных стандартов

Флоридская компания Applied Digital Solutions регулярно привлекает внимание прессы и общественности начиная с начала 2000-х годов, когда впервые стали появляться известия о ее технологии Digital Angel, позволяющей с помощью чипа-импланта дистанционно идентифицировать человека, следить за его географическим местоположением и физическим состоянием. Особый же резонанс инициативы ADS получили в феврале 2002, с появлением торговой марки «Чипсоны». Эту торговую марку – The Chipsons – компания Applied Digital зарегистрировала для своеобразного увековечения флоридской семьи Джекобсов – дантиста Джефри, его жены Лесли и их сына-подростка Дерека, – вызвавшихся быть первой семьей с имплантированными в руку устройствами VeriChip, капсулами размером 11x2 мм, содержащими внутри катушку антенны и RFID-микросхему, подпитывающимися от тепла человеческого организма [JU02a], [JM02].

Эта акция наглядно продемонстрировала, насколько быстро стала меняться ситуация в Америке после 11 сентября 2001. Когда в 2000 году только-только появились сообщения о технологии Digital Angel, то американская общественность буквально вскипела от негодования. Очень громко зазвучали голоса не только правозащитников, усмотревших в технологии посягательство на приватность граждан, но и христиан-ортодоксов, сразу вспомнивших знаменитое библейское пророчество об Антихристе из книги Апокалипсис апостола Иоанна: «И он сделал так, что всем – малым и великим, богатым и нищим, свободным и рабам – положено будет начертание на правую руку или на чело их; и что никому нельзя будет ни покупать, ни продавать, кроме того, кто имеет это начертание (число имени его) или знак зверя»… Интересно, что слова о «числе зверя» в данном случае подходили на редкость точно, поскольку патенты на свой чип-имплант Applied Digital Solutions приобрела вместе с покупкой фирмы Destron Fearing, специализировавшейся на чипах-метках для скота и других животных. Волна протестов в обществе оказалась тогда настолько мощной, что руководство ADS поспешило дать задний ход и заверить публику, что решила отказаться от технологии имплантации и переключиться на сенсоры, встраиваемые в браслеты или пейджеры [LD03].

VeriChip , подкожная капсула с микросхемой RFID

Но затем случились известные события 11 сентября 2001, и уже через пять дней на волне национальной истерии хирург из Нью-Джерси Ричард Силиг самостоятельно имплантировал себе сразу две капсулы с

устройством VeriChip – в правое предплечье и бедро, – дабы на собственном организме продемонстрировать полезность новой технологии в деле обеспечения личной безопасности. После этого пошли сообщения об интенсивных контактах Applied Digital Solutions с латиноамериканскими странами, где технологию якобы чрезвычайно активно востребовала общественность, озабоченная ростом количества похищений людей. А в феврале во флоридскую штаб-квартиру компании нанес личный визит бразильский сенатор Антонио де Кунха Лима, вызвавшийся стать «первым политиком с чипом-имплантом»… [JU02b].

Дело это, конечно, сугубо личное и каждый, как известно, сходит с ума по-своему. Но в свете чрезвычайной озабоченности американской госадминистрации проблемами тотального контроля, в стране стали рождаться опасения, как бы наиболее лояльная к власти часть общества не потребовала всеобщей поголовной имплантации. Подобные опасения не так-то просто назвать полностью безосновательными, поскольку в прессе и Интернете уже неоднократно выдвигались предположения, что у флоридской фирмы ADS явно имеются какие-то очень влиятельные покровители на самой вершине политической власти США. Уж слишком уверенно держится ADS на плаву и продолжает продвигать свои сомнительные инициативы, несмотря на очевидно негативное отношение к ее технологии со стороны подавляющего большинства общества. Событие, произошедшее в октябре 2002, весьма убедительно подтвердили, что дело тут действительно нечистое.

Тогда, ко всеобщему удивлению народа, национальное Управление по надзору за качеством пищевых продуктов и медикаментов (Food and Drug Administration, FDA), еще совсем недавно заявлявшее, что будет тщательно разбираться с продукцией ADS, вдруг издало официальный документ, вообще освобождающий VeriChip от исследований и сертификации в FDA, если устройство используется в целях «безопасности, финансовой и персональной идентификации». Для формального объяснения такого шага заявлено, что FDA занимается лишь имплантами медицинского назначения. Однако хорошо известно, что до этого в США ничего нельзя было вживлять человеку под кожу без достаточно длительной процедуры сертификации в FDA. Даже косметические имплан-ты, включая средства увеличения размеров бюста или пениса, хотя и не имеют никакого медицинского назначения, проходят тщательное исследование экспертов FDA на предмет побочного воздействия на человеческий организм. Известно и то, что ADS при рекламе VeriChip всегда напирает именно на медицинскую полезность своего устройства, потенциально обещающего спасать жизни попавшим в беду людям [JU02c].

Поскольку и управление санитарного надзора, и Applied Digital Solutions отказались передать в печать документы, сопровождающие выдачу разрешения на VeriChip, правозащитная организация EPIC запустила официальный запрос на получение этой документации на основании закона о праве граждан на доступ к информации (FOIA). У правозащитников нет сомнений, что всякий человек имеет право вживлять в собственный организм что угодно – хоть хвост или рога. Но нынешние совместные маневры бизнеса и власти легко могут привести к тому, что однажды частные работодатели или государственные учреждения в

качестве приема на работу начнут требовать у людей согласия на вживление под кожу чипа идентификации. Совершенно добровольного согласия, естественно… [EA02].

Учет и контроль

То, что технология RFID чрезвычайно нравится американской госадминистрации, особенно спецслужбам и военным, не подлежит никакому сомнению. Имеются сведения, что Министерство обороны США впервые начало применять радиочастотные метки еще в 1991 году, во время войны в Персидском заливе, для отслеживания перемещений крупных грузов и транспортных средств. К концу 2003 года высшее руководство Пентагона сочло технологию «умных ярлыков» настолько развитой, что решило радикально перестроить всю неповоротливую, «византийскую» систему закупок и инвентаризации в гигантском военном ведомстве. В конце октября 2003 Пентагон официально объявил о выработке «Политики радиочастотной идентификации», которая потребует от каждого поставщика Министерства обороны снабдить к январю 2005 года все свои товары пассивными (с питанием от антенны) чипами RFID. Исключение сделано только для таких «массовых товаров», как песок, гравий и вода [GL03].

Другая весьма привлекательная для военных область применения технологии RFID и близко ей родственных бесконтактных смарт-карт – это контроль доступа. Широкомасштабные эксперименты с «умными бейджами» начались в Пентагоне в 2000 году, вместе с постепенным вводом личных «карт общего доступа» для идентификации военного и гражданского персонала на основе смарт-карт [REOO].

Но, вообще говоря, к технологиям смарт-карт в Министерстве обороны США начали примеряться по крайней мере года с 1993. Тщательно знакомились с опытом правительственных органов стран поменьше, таких как Испания или Финляндия, где подобные вещи уже введены достаточно широко. Изучали и готовили технологический фундамент в национальной промышленности. Приблизительное представление о том, что представляет собой система автоматизированного контроля доступа в режимных ведомствах, можно получить на следующем примере. На рубеже 1998-99 гг. американская фирма 3-G International (3GI) объявила о выпуске «смарт-картной системы широкого применения Passage Government», предназначенной для решения задач по обеспечению безопасности в правительственных агентствах и организациях. В системе 3GI предусмотрено шесть базовых приложений, куча дополнительных, а также технология управления картами, позволяющая правительственным организациям выпускать «персонализированные» многоцелевые смарт-карты. Каковы же основные приложения Passage Government?

- Мониторинг физического доступа и определение местонахождения персонала – обеспечивает контроль и регистрацию прихода и ухода сотрудников с работы. Для идентификации сотрудников используются цифровые фотографии, и в реальном масштабе времени поддерживается база данных о персональном местонахождении людей. По запросу администрации генерируются соответствующие сообщения и отчеты.

• Учет посетителей – работает совместно с предыдущим приложением. Приложение поддерживает базы данных о посетителях, о временных картах-пропусках, о выдающих эти карты и о принимающих посетителей.

• Контроль за оборудованием – обеспечивает усовершенствованный учет и контроль за имуществом и оборудованием на объекте. Доступ к оборудованию контролируется соответствующей базой данных о владельцах смарт-карт.

• Учет посещаемости – использует возможности смарт-картной технологии для оперативного документирования посещений сотрудниками учебных занятий, встреч, конференций и прочих служебных сборов. Это клиентское приложение «снимает» персональную/административную информацию со смарт-карты посетителя мероприятия и формирует отчеты заседаний.

В 2001 году фирму 3GI поглотила более крупная RSA Security, включив Passage Government в более широкий пакет приложений RSA SecurID Passage [FA01].

Одно из главных «неудобств» традиционных смарт-карт – для считывания информации их надо непременно проводить через щель прибора считывателя. Другое дело – новые бесконтактные смарт-карты, обменивающиеся информацией с ридером или программатором дистанционно через радиочастотный интерфейс. Метка RFID, по сути своей, та же самая бесконтактная смарт-карта, но с меньшей функциональностью из-за крошечных размеров. С начала 2000-х годов именно RFID и бесконтактные смарт-карты выступают в качестве основы современных систем «умных бейджей», внедряемых повсеместно – в госучреждениях и корпорациях, учебных заведениях и тюрьмах [PEO3], [JS03].

По секрету всему свету

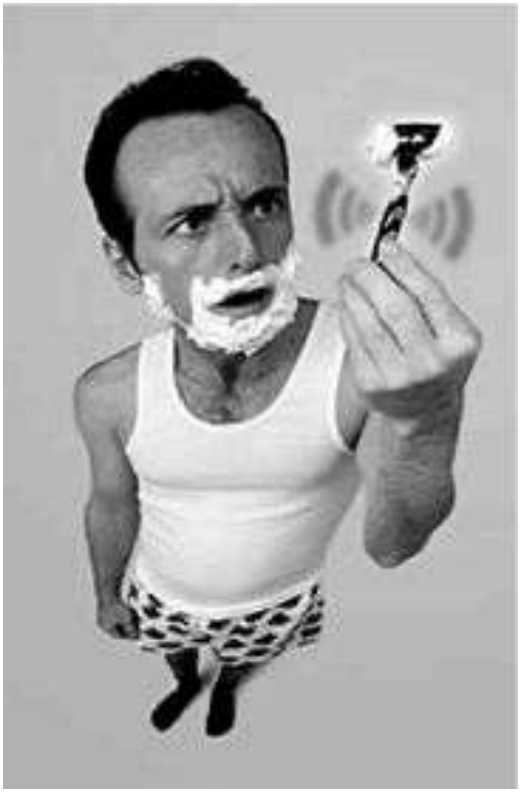
Мало кому (кроме государства и корпораций) нравится идея крупных баз данных, централизованно хранящих персональную информацию о гражданах. Во-первых, это сверхпривлекательный объект устремлений для злоумышленников, использующих реквизиты чужой личности в своих гнусных целях. Во-вторых, это мощная потенциальная угроза злоупотреблений со стороны владельцев базы и обслуживающего персонала. И в-третьих, коль скоро здесь так глубоко замешан человеческий фактор, надежно защитить подобные хранилища практически невозможно. В таких условиях можно гарантировать, что известия о компрометации очередной крупной базы как появлялись часто прежде, так и будут регулярно появляться впредь. Широкое же внедрение микрочипов радиоидентификации, которые индустрия в ближайшем будущем намерена встраивать чуть ли не во все потребительские товары, непременно увеличит и масштабы компрометации. Потому что RFID, облегчающие корпорациям и торговым сетям учет производства и сбыта, для покупателей означают ведение соответствующих гигантских баз данных о приобретенных ими товарах.

Эта тенденция очень не нравится той части общества, что обеспокоена вторжением корпораций и властей в личную жизнь граждан. Для

сопротивления бесконтрольному насаждению RFID создана специальная общественная организация CASPIAN или «Потребители против вторжения супермаркетов в частную жизнь» (Consumers Against Supermarket Privacy Invasion and Numbering). Летом 2003 г. активисты этой организации и решили проверить, как радетели RFID, заверяющие всех в надежной защите накапливаемой информации, в действительности способны хранить секреты. Для этого был проведен нехитрый тест на сайте Auto-ID Center (www.autoidcenter.org) – исследовательского центра консорциума, объединяющего около 100 компаний и 5 университетских лабораторий, разрабатывающих инфраструктуру для широкомасштабного внедрения чипов идентификации. Абсолютно без всяких хакерских ухищрений, просто введя в окошке поиска волшебное слово «confidential», правозащитники получили свободный доступ к целой библиотеке (около 70) конфиденциальных документов, не предназначенных для посторонних глаз [AMO3].

Среди этих материалов оказался, в частности, доклад о мерах по «умиротворению» противников RFID, в котором приводятся цифры внутреннего социологического исследования, показавшего, что около 78% опрошенных граждан «встревожены» посягательством чипов-меток на частную жизнь, а 61% обеспокоены влиянием повсеместно встроенных микросхем на здоровье. В другом документе вносятся предложения по смене отпугивающего названия RFID-чипов на более дружелюбное типа «зеленые ярлыки». О документах с подробным расписанием рабочих встреч и детальной контактной информацией функционеров консорциума и говорить не приходится.

Естественно, это дало повод активистам CASPIAN громко заявить о неспособности консорциума обеспечить надежное хранение чувствительной к разглашению информации. В Auto-ID Center, в свою очередь, воздержались от комментариев, однако усилия для более надежного закрытия документов все же приложили. Впрочем, птичка уже выпорхнула из клетки, и конфиденциальные документы можно найти в Сети на множестве сайтов-зеркал (см. cryptome.org/rfid-docs.htm).



Интересно также, что буквально на следующий день после скандала крупнейшая в мире сеть универмагов Wal-Mart (порядка 4700 магазинов по всему миру) неожиданно объявила о сворачивании торгового эксперимента с RFID-чипами в бритвах Gillette. Руководство Wal-Mart не пожелало комментировать прекращение этого проекта, получившего название «умные полки» и уже практически подготовленного к запуску в универмаге Броктона, одного из пригородов Бостона. Но можно предполагать, что скандал в Auto-ID Center был сочтен слишком неблагоприятным фоном для представления публике новой технологии [GS03].

Охота на ведьм XXI века

> *[В Древнем Египте] термином «хэка» обозначалась магия, то есть «слова власти» – магические слова, заклинания.*
>
> **Уоллис Бадж. Египетская магия**

> *Имеется некоторое сообщество, некая общая культура, состоящая из опытных программистов и сетевых чародеев, которая ведет свою историю от многолетней давности первых миникомпъютеров и от самых ранних экспериментов с сетью ARPAnet . Члены этой культуры и дали рождение термину " hacker " [хэка]. Хэкеры построили Интернет.*
>
> **Эрик Рэймонд. Как стать хэкером**

Во все времена власти с опаской относились к компетентным людям, хорошо знающим свое дело, а потому имеющим тенденцию к

самостоятельному мышлению и независимым суждениям. В древнейшие времена такой репутацией пользовались маги, с наступлением эры высоких технологий обостренное раздражение властей стали вызывать так называемые «хакеры». Сейчас уже никто, наверное, и не скажет, в какой момент к термину «хакер» прирос криминальный смысл. Обычно в этом принято винить поверхностных журналистов и киношников, не способных провести грань между пытливым исследователем-профессионалом и каким-нибудь безответственным или злонамеренным негодяем (кракером, т.е. криминальным хакером), использующим чужие результаты в собственных корыстных целях.

Откуда исходит угроза миру?

В последний день 1999 года на страницах популярного сайта Slashdot.org была опубликовано интервью с членами известной хакерской организации LOpht [В 2000 году на базе LOpht была создана консалтинговая компания @Stake, специализирующаяся на проблемах компьютерной безопасности], признанное читателями, как один из лучших материалов такого рода за всю историю Slashdot. Интервью было коллективным, то есть ответы давал как бы просто LOpht, без конкретизации отвечавших личностей. И один из самых первых вопросов звучал примерно так: «Чьи угрозы следует рассматривать более опасными для личных свобод, со стороны правительства или со стороны транснациональных корпораций?»

Вот что, в несколько вольном пересказе, ответили на это хакеры из Lopht: [BR99]

Хотя и правительства, и транснациональные корпорации в значительной степени несут угрозу личным свободам человека (в частности, в Интернете), но существует опасность, значительно превосходящая первые две. Имя ей – неинформированные граждане. И как это ни парадоксально звучит, эта опасность многократно реальнее именно в условиях демократических режимов, где правительства стараются следовать общественному мнению. Потому что уже абсолютно четко видно, как большинство граждан вполне согласны и готовы поступиться своими личными свободами в обмен на ощущение некой безопасности. Обычно это укладывается в формулу типа «ради безопасности наших детей».

Уже сейчас многие люди полагают, что анонимный доступ к Интернету – это признак криминального поведения. Тем, кто управляет рычагами власти, обычно очень хочется, чтобы стремление воспользоваться правом на личную тайну воспринимали как «антисоциальное» поведение. Ведь добропорядочному гражданину нечего скрывать, не так ли? Это только террористам, наркодельцам и педофилам нужно скрывать свои темные замыслы.

На правительство надавливают неинформированные граждане, либо те, кому уже промыли мозги до стадии панического ужаса от угроз современных технологий и от тех людей, которые бесконтрольно могут технологии использовать (хакеров, одним словом). В этом процессе лоббирования активно участвуют и транснациональные корпорации, финансируя деятельность «озабоченных» общественных групп или

принимая участие в деятельности ассоциаций, оказывающих консультативную помощь правительственным структурам в технических вопросах. И весьма часто эти рекомендации приводят к очередному урезанию священного права граждан на личные свободы.

Весьма проблематичным является и то, что мир деятельности транснациональных корпораций – это мир частной собственности. И когда какая-либо внешняя группа начинает заниматься тщательным анализом технологических продуктов или коммуникационных услуг корпораций, то возникают конфликты принципиального характера. Если эта группа обнаруживает существенный изъян, скажем, в безопасности и публикует информацию о дыре в защите, то корпорация в свою очередь нередко объявляет, что этим нанесен сильнейший ущерб ее деятельности и затевает судебное преследование в отношении опубликовавших компромат, а то и добивается изменений в законодательстве.

Одна из наиболее известных историй такого рода – судебная тяжба индустрии сотовой связи в США. Клонирование сотовых телефонов было острейшей занозой в наиболее нежных местах индустрии мобильной связи. В конце концов к решению проблемы привлекли американское правительство, дабы подобного рода мошенничество было запрещено специальным законом. В итоге же определенный участок спектра радиочастот стал в США запрещенным для прослушивания и сканирования. А обладание «оборудованием для клонирования» стало преступлением, хотя это просто компьютер, программатор перезаписываемых микросхем и сотовый телефон. Любому, кто понимает техническую суть проблемы, очевидно, что это явная глупость. Но имеющие большие деньги имеют и большое влияние на власть. И именно государственная власть принимает такого рода законы.

Правительство подталкивает людей, люди подталкивают правительство. Уже и не найдешь, кто первым высадил это семя… Те же, кто смыслят что-то в технологиях, страсть как все заняты разработкой какой-нибудь очередной крутой штуковины. Ну, а погруженный в эти технические чудеса мир тем временем все больше сползает к глобальной диктатуре, пока население понемногу привыкает к ней под видом «безопасности».

Конец цитаты, как говорится.

Когда законы готовит полиция

В ноябре 2003 года президент США Джордж Буш обратился с просьбой к американскому Сенату ратифицировать первый международный закон о компьютерных преступлениях или Конвенцию о киберпреступности (Convention on Cybercrime). В своем письме к Сенату Буш назвал этот весьма спорный в своем содержании договор, официально подготовленный Советом Европы, «эффективным инструментом в глобальных усилиях по противодействию преступлениям, связанным с компьютерами» и «единственным многосторонним договором, направленным на компьютерные преступления и электронный сбор улик».

Хотя США не являются членом Евросовета с правом голоса, достаточно хорошо известно, что именно американские правоохранительные органы

были главной силой, стоявшей за подготовкой международного договора о киберпреступности. В этом законе они видят путь к выработке интернациональных стандартов в оценке криминальной деятельности, имеющей отношение к посягательствам на авторские права, к онлайновому мошенничеству, детской порнографии и несанкционированным сетевым вторжениям. Как заявляют в Министерстве юстиции США, эта конвенция устранит «процедурные и юридические препятствия, которые могут задерживать или мешать международным расследованиям» [DE03].

Поскольку столь благородному, на первый взгляд, делу яростно и который уже год подряд сопротивляются правозащитники многих стран, имеет смысл рассмотреть историю рождения данной конвенции в некоторых содержательных подробностях.

Для компьютерных специалистов, уважающих термин «хакер», под «хакингом» обычно понимается процесс проникновения в суть той или иной вещи. Конечный результат – понимание того, «как это работает», зачастую сопровождаемое предложениями по улучшению работы. У властей же понимание «хакинга» сложилось совсем иное. Поскольку политическое руководство государств – народ занятой, то им некогда разбираться во всех этих терминологических тонкостях. Для этого есть эксперты и консультанты. Раз кругом говорят, что хакеры взламывают защиту компьютерных сетей, значит это дело экспертов из полиции и прочих правоохранительных органов. Логика же полиции свелась примерно к следующему умозаключению: раз хакерская публика мнит себя дюже умной и пишет всякие-разные программы, плодящие киберпреступность и лишающие корпорации доходов, то надо это дело запретить. Причем на корню.

Впервые о подготовке закона стало известно в октябре 2000 года, когда был рассекречен весьма важный и любопытный документ, подготовленный под эгидой Совета Европы и носивший название «22-я версия Проекта договора о киберпреступлениях» (Draft Convention on Cybercrime, № 22 rev). Этот документ, подготовленный в условиях необычной для европейского сообщества секретности, был представлен как «первый международный договор, посвященный уголовному праву и процедурным аспектам разного рода преступного поведения, направленного против компьютерных систем, сетей и данных».

В 22-й версии проекта обнаружилось много чего интересного: и намерение заставить всех интернет-провайдеров хранить подробные отчеты о деятельности своих клиентов (нечто подобное уже реализовал у себя Китай, поскольку это крайне полезный инструмент в борьбе с инакомыслием); и намерение привлекать к уголовной ответственности за посягательство на копирайт (для множества европейский стран это весьма спорный с правовой точки зрения вопрос); и запрет на хакерскую деятельность вкупе с хакерским инструментарием, и ряд положений, игнорирующих презумпцию невиновности, а также побуждающих граждан к «самообвинению». Достаточно подробный разбор весьма спорных юридических новшеств, предложенных в проекте и противоречащих европейской Конвенции о правах человека, был сделан в коллективном письме GILC (www.gUc.org), международной коалиции нескольких десятков правозащитных групп, на имя генерального секретаря Евросовета. По

оценкам, сделанным в заявлении GILC, этот проект «противоречит прочно утвердившимся нормам защиты личности, подрывает разработку эффективных технологий сетевой безопасности и снижает подотчетность правительств в их правоохранительной деятельности» [GIOO].

В контексте нашей истории наибольший интерес представляют те положения проекта Договора, что посвящены непосредственно хакерам и их инструментам. В компактном представлении выглядят эти положения проекта следующим образом.

Каждая сторона, подписывающая договор, должна принять такое законодательство и прочие меры, которые окажутся необходимы для преследования как уголовных преступлений следующих деяний: (1) доступ к компьютерной системе в целом или любой ее части без надлежащего на то права; (2) осуществляемый с помощью технических средств перехват компьютерных данных, идущих внутри компьютерной системы, от нее или к ней, а также перехват электромагнитных излучений системы, несущих такие компьютерные данные; (3) внесение, уничтожение, подмена, повреждение или удаление компьютерных данных без надлежащего на то права; (4) создание, продажа и прочее распространение устройств и компьютерных программ, разработанных или приспособленных для целей, перечисленных в предыдущих пунктах; (5) распространение информации, способствующей доступу к компьютерным системам без надлежащего на то права.

На проходившей в ту пору в Амстердаме конференции DEFCON, где собираются хакеры, занимающиеся вопросами компьютерной безопасности, новость о подготовке драконовского договора взбудоражила всех. Как прокомментировал ситуацию один из участников форума, «они просто боятся тех вещей, которых не понимают, того, что не могут контролировать… это действительно может превратиться в охоту на ведьм». По заключению американского эксперта по киберправу Дженифер Грэник, из положений документа следует, что вне закона оказываются и все публикации об уязвимостях и слабостях компьютерных систем. В частности, и столь популярные среди профессионалов рассылочные листы как BugTraq и NTBugTraq, имеющие десятки тысяч подписчиков и служащие ценным источником для поддержания компьютерных систем «в форме». А то, что под запретом окажутся такие программы, как сетевые сканеры, тестирующие уязвимость портов системы, очевидно и без заключения экспертов. Более того, логика документа может со временем наложить запрет и на самые обычные программы-отладчики (дебаггеры), поскольку и этот инструмент широко используется для «хакинга». Конечно, всем ясно, что это абсурд и глупость, поскольку для программиста дебаггер – что отвертка для слесаря. (Талантливый слесарь, как известно, и отверткой может открыть замок, но никому не приходит в голову запретить отвертки) [SUOO].

Весьма примечательно, как именно готовился этот законопроект – в обстановке строгой секретности «авторами из 41 страны в тесном сотрудничестве с Министерством юстиции США». Этот нюанс кое-что проясняет и косвенно указывает «откуда ноги растут». Весной 1999 года в результате утечки в прессу попали секретные документы Европейской Комиссии (Enfopol 19), свидетельствующие об обширных планах взятия под

контроль Интернета и всех будущих цифровых коммуникационных систем. Основу этих планов составляют предложения секретной международной организации, возглавляемой США и объединяющей органы безопасности и полиции. Эта организация именуется «Международным семинаром правоохранительных органов по телекоммуникациям» или ILETS (International Law Enforcement Telecommunications Seminar) и объединяет сотрудников полиции и госбезопасности из более чем 20 стран, включая Европу, Гонконг, Канаду, Австралию и Новую Зеландию, которые проводят регулярные встречи с начала 1990-х годов [DC99].

Организация ILETS была создана ФБР в 1993 году после нескольких неудачных попыток провести через Конгресс США новый закон, требующий от производителей оборудования и операторов связи за собственный счет встраивать в аппаратуру средства прослушивания. То, что не получилось сделать в лоб в США, стали проводить через международные структуры. К концу 1990-х годов ILETS удалось добиться одобрения своих планов в качестве политики Евросоюза и их включения в национальное законодательство нескольких стран. Впервые эта группа встретилась в исследовательском и учебном центре ФБР в Куантико, штат Вирджиния в 1993 году. На следующий год они встречались в Бонне и одобрили документ, получивший название «Международные требования по перехвату» или IUR 1.0. В течение следующих двух лет «требования» IUR незаметно стали секретной официальной политикой Евросоюза. ILETS и его эксперты снова встречались в Дублине, Риме, Вене и Мадриде в 1997 и 1998 годах, и разработали новые «требования» по перехвату Интернета. Результатом же стал документ Enfopol 19 [EP99].

В конце октября 2000 г. информированное американское издание Wall Street Journal опубликовало информацию о том, что Министерство юстиции США в приватном порядке сообщило компаниям американской индустрии инфотехнологий, что подготовленный вариант «Договора о киберпреступлениях» уже практически согласован и «слишком поздно что-либо существенное в нем переделывать». В действительности дела пошли несколько не так – под давлением общественности подписание договора было задержано еще на год, в течение которого в текст документа были внесены многочисленные «смягчающие» поправки [SL01].

Но, вообще говоря, если полиция сама начинает готовить под себя законы, вместо того, чтобы лишь обеспечивать их выполнение, то единственное, что может здесь получиться – это полицейское государство.

Глава 2. Тайные рычаги власти

Страницы жизни героя, 1920. Братья-масоны

Главным хранителем памяти о самом знаменитом директоре ФБР стал после его смерти Фонд Дж. Эдгара Гувера, организованный масонами Шотландского обряда. В вашингтонской штаб-картире Верховного совета масонов тридцать третьей степени, именуемой «Дом Храма», создан мемориальный музей, хранящий многочисленные личные вещи, документы

и фотографии из особняка и рабочего кабинета Гувера.

Все это, конечно, не случайно, ибо деятельность в тайном масонском обществе была одной из важных сторон жизни главного полицейского США на протяжении более полувека. Вот что пишет об этой стороне Картха Де Лоуч, многолетний помощник директора ФБР, а ныне председатель Гуверовского фонда в «Журнале Шотландского обряда» в мае 1997 года: «Прославленный Гувер был абсолютно предан своему масонскому братству. Он был принят в масоны Федеральной ложей № 1 в Вашингтоне, 9 ноября 1920 года, всего за два месяца до своего 26-го дня рождения. За 52 года в Ложе он был награжден бесчисленными медалями, наградами и знаками отличия. В 1955 году, к примеру, он был произведен в Генеральные инспекторы 33-й степени, а в 1965-м удостоен знака высочайшего признания в Шотландском обряде – Большого креста почета» [CD97].

В 1921 году в Белый дом вступил очередной, 29-й президент США, республиканец Уоррен Хардинг. Назначенный им новый генеральный прокурор Гарри Догерти был весьма приятно удивлен, когда Гувер предоставил в его распоряжение обширную картотеку на политических противников президента, а также на сотни тысяч радикально настроенных граждан. Эдгар Гувер всегда уделял тщательное внимание своей репутации нейтрального государственного чиновника, лишенного каких-либо склонностей к той или иной политической партии. Поэтому когда Догерти стал заменять в Министерстве юстиции всех демократов на республиканцев, Гувер от этого только выиграл, получив в августе 1921 года давно желанный пост – помощника начальника Бюро расследований.

Начальником его тогда был некто Уильям Бернс, человек, мягко говоря, без особого служебного рвения. Гувер же для него стал просто незаменим, поскольку взялся готовить ежегодные планы на бюджетные ассигнования и отчеты для Конгресса. Свободного времени при этом появилось заметно больше, поэтому Гувер увлекся гольфом, а также стал заметно активнее в масонской ложе. Естественно, не без личной пользы.

Вскоре политическая ситуация в Вашингтоне существенно изменилась. В 1923 г. Хардинг скоропостижно скончался от сердечного приступа, на следующий год очередной президент Калвин Кулидж привел в госадминистрацию своих людей, а новый министр юстиции Харлан Стоун, недовольный общей ситуацией в министерстве, решил непременно поменять, среди прочих руководителей, и главу Бюро расследований. Тут-то и вступили в ход невидимые масонские рычаги. Когда Стоун обронил среди коллег-министров, что подыскивает для Бюро нового шефа, то Лоуренс Ричи, заместитель министра торговли, не мешкая порекомендовал своего доброго друга и соратника по масонской ложе Дж. Эдгара Гувера. В поддержку этой же кандидатуры выступил и заместитель генпрокурора, поэтому вскоре Стоун вызвал в свой кабинет Гувера и сообщил, что намерен назначить его временно исполняющим обязанности директора Бюро, пока будет подыскиваться более подходящая фигура. Вскоре, однако, для Стоуна стало очевидно, что именно Гувер является наиболее подходящим человеком для полной реорганизации Бюро и перевода деятельности спецслужбы на высокопрофессиональную основу. Поэтому в конце того же 1924 года, 10 декабря Эдгар Гувер в возрасте 29

лет получил вожделенную должность директора Бюро расследований, которую затем сохранил за собой на всю оставшуюся жизнь.

Приверженность Гувера к масонству, его духу и обрядам в определенной степени отразились и на Бюро расследований. Принадлежность агентов к масонской ложе всячески приветствовалась, а со временем отчетливый привкус масонства обрел даже текст присяги, которую принимали новые сотрудники и которую завели по личному приказу Гувера. Вот лишь некоторые фрагменты из этого достаточно пространного текста: «Смиренно сознавая всю ответственность за дело, доверяемое мне, я клянусь, что буду всегда чтить высокое призвание нашей почетной профессии, исполнение обязанностей которой является как искусством, так и наукой… Исполняя свои обязанности, я буду, подобно священнику, источником утешения, совета и помощи… подобно солдату, я буду неустанно вести войну против врагов моей страны… подобно врачевателю, я буду стремиться к искоренению преступной заразы, которая паразитирует на теле нашего общества… подобно художнику, я буду стремиться к тому, чтобы выполнение каждого задания было истинным шедевром…»

В книге-исследовании Энтони Саммерса «Тайная жизнь Эдгара Гувера» со слов сотрудников ФБР представлен такой портрет «образцово-показательного агента» из тех, кто начал службу в середине 1920-х годов. Портрет срисован с одного из тогдашних молодых сотрудников, на долгие годы ставшего в глазах шефа достойнейшим примером для подражания. Эдвард Армбрусер прослужил в ФБР с 1926 по 1977 год, став высококлассным специалистом по банковским аферам. Это был типичный представитель нового поколения агентов, непьющий и некурящий, масон, учитель церковно-приходской воскресной школы, семь учеников которой стали впоследствии агентами ФБР. Агент более позднего поколения, Норман Оллестад, вспоминает облик своего коллеги-ветерана так: «Он окружал себя броней всяческих амулетов – колец, значков и заколок с драгоценными камнями. Он был весь увешан ими. Чтобы галстук не мялся, его скреплял с рубашкой зажим в виде львиной головы. На манжетах были запонки. На правой руке у него красовался университетский перстень, выделявший его среди людей необразованных. На той же руке он носил масонское кольцо, которое защищало его духовно. На среднем пальце левой руки у него было обручальное кольцо, служившее щитом против возможных поползновений женщин, которых ему придется допрашивать»… [AS93]

Гувер считал Эдварда Армбрусера образцовым работником и продолжал держать его на службе еще многие годы после того, как ветеран достиг пенсионного возраста.

Перекрестки и параллели истории

Библейский код

В начале 2003 года, накануне вторжения американской армии в Ирак, среди множества брифингов и совещаний, проводившихся в Пентагоне,

одно из мероприятий следует выделить особо. Необычность его заключается в том, что серьезные и ответственные люди из высшего эшелона военной власти США около часа своего драгоценного времени посвятили нетривиальной проблеме – как отыскать архиврага Америки Усаму бен Ладена с помощью текстов Ветхого завета, а еще точнее, расшифровав специальные тайные послания в Пятикнижии Моисеевом, у иудеев именуемом Торой [WJ03][BKO3].

Столь любопытное совещание организовал Пол Вулфовиц, заместитель министра обороны и один из главных «ястребов» в вашингтонской госадминистрации. Во встрече принимали участие около 10 высших чинов военного командования и разведки, включая вице-адмирала Лоуэлла «Джейка» Джекоби, директора разведуправления Министерства обороны, и Линтона Уэллса, начальника «нервного центра» Пентагона, известного как 3CI (Command, Control, Communications, Intelligence, т.е. «центр командования, управления, связи и разведки»). Главным же докладчиком выступал некто Майкл Дроснин, в прошлом журналист Washington Post и Wall Street Journal, а ныне автор книг-бестселлеров «Код Библии» и «Код Библии II: Обратный отсчет» [MD97][MD02].

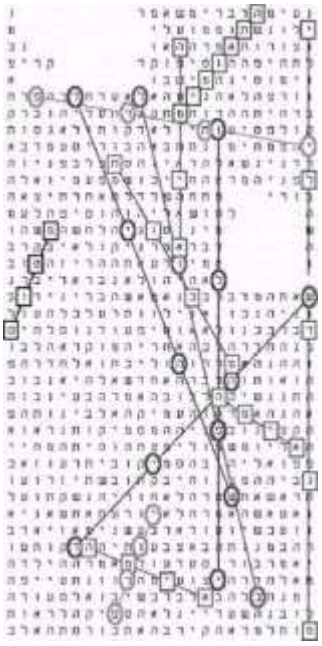
На страницах своих исследований Дроснин пытается доказать, что первые пять книг Ветхого завета – Бытие, Исход, Левит, Числа и Второзаконие – это на самом деле зашифрованная история мира от сотворения до последнего дня. Ну а сам Дроснин, понятное дело – дешифровщик этого великого кода. С помощью довольно нехитрых манипуляций с буквами текста на иврите (в древнем языке нет гласных, цифры также обозначаются согласными) автор демонстрирует, что в Библии предсказано все – и Вторая мировая война, и покушение на Кеннеди, и высадка человека на Луну и теракты 11 сентября 2001 года. Все что угодно, короче говоря. А отыскиваются эти предсказания так. Все 304 805 букв на иврите, составляющие Тору, загнаны в компьютер в виде одной большой строки. Дроснин («секуляризованный еврей», специально ради такого дела выучивший иврит) задает машине вопрос, к примеру, про Саддама Хуссейна. Для этого вводится строка «кто уничтожен?», а с ней вместе и ожидаемый ответ «Хуссейн». После чего компьютер перелопачивает весь текст и отыскивает страницы, на которых слова вопроса и ответа расположены как в кроссворде – в виде пересечения строчки и столбца. Тогда здесь же отыскивается и дата нужного события – расположенные неподалеку (желательно, поближе к перекрестью) строка или столбец с подходящим годом. Для Саддама, в частности, отыскивается 5763 – еврейский год, эквивалентный по христианскому календарю 2003… И все дела. Дешево и сердито, как говорится. Но впечатление эти «перекрестки истории» производят, как выяснилось, на очень многих – причем не только на домохозяек, но и на некоторых пентагоновских генералов.

У подобного жонглирования буквами-именами и цифрами-датами имеется очень длинная история. В текстах всех священных книг исстари принято выискивать пророчества. Традиции этой примерно столько же лет, сколько самим книгам, но лет десять назад данное занятие перешло в качественно иную категорию. В 1994 году группа израильских математиков во главе с Элияху Рипсом опубликовала в солидном научном журнале

Statistical Science статью под названием «Эквидистантные последовательности букв в книге Бытие» [ER94]. В этой статье был описан некий статистический эксперимент, демонстрирующий примечательные корреляции между именами знаменитых в израильской истории раввинов и годами их жизни, отыскиваемыми на страницах Торы, хотя текст Пятикнижия создан на несколько веков и тысячелетий раньше рождения этих раввинов. «Эквидистантные последовательности» означают то, что выбор букв из текста осуществлялся по принципу расположения символов на некотором равном расстоянии друг от друга. Ученый совет, отбирающий статьи для опубликования, счел данный материал хоть и необычным, но с научной точки зрения вполне добротным и заслуживающим внимания, поэтому и было принято решение о публикации статьи. Тут же породившей, надо отметить, волну протестов и работ-опровержений со стороны других математиков [BM98] [MB99].

Вообще говоря, данная история в который раз подтвердила расхожую житейскую мудрость, согласно которой ложь бывает трех видов – обыкновенная, чудовищная и статистика. Умело манипулируя данными и методами их обсчета, как известно, при желании можно доказать все, что угодно. Но если научные споры о тонкостях и дефектах избранной исследователями методики – это вещь для неспециалистов довольно туманная и труднопостижимая, то вот построение эффектных контрпримеров вполне понимают все, даже ничего не смыслящие в теории вероятностей и математической статистике. За прошедшие годы появилось в достатке всего – и разгромной критики избранной Рипсом сотоварищи методики, и убедительных контрпримеров, однако все это происходило по преимуществу в научных кулуарах, не привлекая особого внимания широкой публики.

Но тем временем за «высокотехнологичную» разработку жилы библейских пророчеств взялся репортер полицейской хроники Майкл Дроснин. Он, быть может, и мало что смыслил в теории вероятностей, но зато углядел в предмете споров потенциальную сенсацию, провел несколько собственных компьютерных экспериментов, в ходе которых и родилась описанная выше методика отыскания предсказаний. А несколько лет спустя появляется его сногсшибательный бестселлер «Код Библии», изданный к настоящему времени огромными тиражами и переведенный на множество языков. Ничего не поделаешь, народ страсть как любит все загадочное и непонятное, особенно подкрепленное математическими выкладками – практически столь же непостижимыми, но придающими аргументам дополнительную «научную» солидность.



Предсказание теракта 11-09-2001 в тексте романа «Война и мир» на иврите

Сами математики, правда, пришли от опуса Дроснина в ярость. Всячески отмежеваться от «Кода Библии» сочли целесообразным даже авторы исходной статьи в Statistical Science, Рипс и Вицтум. Другие же ученые, тщательно воспроизводя «метод декодирования Дроснина», продемонстрировали, что любые предсказания можно извлекать из какой угодно, в общем-то, книги, была бы у нее подходящая длина. В частности, те же самые «пророчества», что и в Библии, были выявлены в английском тексте романа Германа Мелвилла «Моби Дик»[http://cs.anu.edu.au/~bdm/dilugim/moby.html] и в переводе на иврит романа «Война и мир» Льва Толстого [http://cs.anu.edu.au/~bdm/dilugim/WNP/]. Ради смеха, те же самые результаты были продемонстрированы и на тексте книги самого Дроснина, где, к примеру, один из исследователей, Дейв Томас, обнаружил с помощью «шифра эквидистантных букв» такую фразу: «Этот код – глупая шутка и надувательство»… [http://www.nmsr.org/biblecod.htm].

Во всей этой истории поразительна, конечно, вовсе не популярность творчества Дроснина «в народе» (общие предпочтения публики известны достаточно хорошо). Любопытен здесь иррационально-обостренный интерес к мистическим предсказаниям в среде высшего военно-политического руководства США, и тому наверняка должны быть какие-то логичные объяснения. Возможно, причина кроется в следующем.

Череп и кости

Организовавший приглашение в Пентагон «эксперта по коду Библии» Дроснина, заместитель министра обороны и ультра-ястреб Пол Вулфовиц в 1970-1973 годах был преподавателем политологии Йельского университета. Библиотека этого университета известна своим примечательным собранием эзотерической и оккультной литературы, а также знаменитым, одним из крупнейших в мире собраний клинописи

цивилизаций Междуречья – так называемой «Вавилонской коллекцией Йеля» [http://www.yale.edu/babylon/]. (Имеется интересная параллель. При недавнем вторжении войск США в Багдад, мародерами был тут же разграблен местный музей, хранивший самое большое, вероятно, собрание клинописи в мире. Почти все разграбленное, заметим, было сразу найдено и взято в учет доблестной американской армией… Правительство Перу, к примеру, по сию пору просит у Иеля вернуть исторические реликвии, вывезенные в начале XX века из древнего высокогорного святилища Мачу-Пикчу его «первооткрывателем», йельским исследователем Хайрэмом Бингемом.

Но здесь речь не о том. По какому-то (видимо, случайному) стечению обстоятельств в 1959 году в Йельский университет поступил учиться другой ультра-ястреб, тогда совсем еще юный Дик Чейни, ныне 46-й вице-президент США, а в период 1989-1992 гг. министр обороны в администрации Джорджа Буша-папы. Чейни, правда, в Иеле не доучился, переведясь в университет Вайоминга, зато выпускником Иельского университета 1964 года является высокоморальный Джон Эшкрофт, нынешний министр юстиции и генеральный прокурор США, не так давно велевший задрапировать «похабно-полуголые» статуи в Большом зале Министерства юстиции. Ну, и чтобы стало совсем понятно, что все это вряд ли чистая случайность, следует напомнить, что выпускниками Иеля являются также Джордж Буш-папа (1948), Джордж Буш-сын (1968), а также дедушка 43-го и отец 41-го президентов США Прескот ТТТ. Буш, американский сенатор и в свое время видный деятель местного тайного общества «Череп и кости».

Созданное почти два века назад, в 1832 г, тайное «студенческое братство» Skull and Bones, или «орден», как именуют его сами члены, уже давно стало одной из самых больших загадок американской истории и своеобразным инкубатором высшей политической и экономической элиты США. Помимо трех президентов (два Буша и Уильям Говард Тафт), среди известных членов этого ордена множество сенаторов, государственных секретарей, генеральных прокуроров, глав разведслужб, председателей Верховного суда, директоров крупнейших транснациональных компаний, банков и так далее.

Одной же из главных особенностей «Черепа и костей» является режим строжайшей секретности, культивируемой членами ордена относительно всего, что происходит в «Могиле», как издавна принято именовать мрачновато вида старинный особняк, в котором проходят обряды инициации неофитов и регулярные встречи членов ордена. Интересно, что администрация Иельского университета уже очень давно и решительно не желает иметь с деятельностью Skull and Bones ничего общего, всячески осуждая подчеркнутую элитарность и закрытость этого общества. Члены общества отвечают взаимной неприязнью, так что в текстах многих нынешних политиков без труда можно найти тирады о «чопорности и снобизме йельской профессуры».

Как бы там ни было, но об очень своеобразной обстановке «масонского братства», о зловещих ритуалах с черепами, костями и кинжалами, о густой мистической ауре и жестких порядках в ордене легенды ходят еще с XIX века. Причем за все 170 с лишним лет истории

тайного общества, среди его членов не нашлось ни единого человека, решившегося публично раскрыть секреты Skull And Bones. Попытки же сторонних исследователей выведать хоть что-то существенное неизменно натыкаются на непрошибаемую железобетонную формулу стандартного ответа масонов: «Эти вещи мы не обсуждаем. Точка».

Кое-что, конечно, все же разузнать удается, тогда публикуются разной степени достоверности статьи и книги. В 1986 году была опубликован очень содержательный труд Энтони Саттона под названием «Тайные власти Америки. Введение в орден Skull And Bones» [AS86]. В апреле 1991 года в журнале ParaScope напечатано объемное исследование Голдстейна и Стейнберга «Джордж Буш, Skull Bones и Новый мировой порядок» [GS91]. Если говорить о последних работах, то глубоко удалось копнуть молодой журналистке Александре Роббинс, выпускнице Иельского университета 1998 года, сумевшей разговорить на условиях сохранения полной анонимности свыше 100 членов ордена и выпустившей в 2002 году книгу «Секреты Могилы» [AR02].

Особо интересна вся эта история именно сейчас, потому что, по оценкам ряда американских аналитиков, к президентским выборам 2004 года США подходят в таком состоянии, когда у кормила власти находится беспрецедентно много членов ордена Skull Bones. То есть столь насыщенной их концентрации в Вашингтоне, в высшем руководстве крупнейших корпораций и в наиболее влиятельных средствах массовой информации прежде еще не отмечалось.

Мрачные параллели

Тех, кто способен это видеть, более всего тревожит следующее обстоятельство. Последний раз наиболее заметный всплеск чего-то подобного – интереса к оккультным делам в рамках тайного ордена в среде высшего политического руководства мощной державы – наблюдался в нацистской Германии. Причем отчетливые параллели прослеживаются далеко не только здесь.

Эд Гернон, исполнительный продюсер телевизионного мини-сериала «Гитлер: Восход зла» (Hitler: The Rise of Evil), снимавшегося недавно в США по заказу компании CBS, когда окунулся в исторический материал, был просто шокирован тем, насколько нынешняя обстановка в США напоминает гитлеровскую эпоху в Германии: подавление гражданских свобод во имя укрепления национальной безопасности; появление новой правительственной спецслужбы, наделенной особыми полномочиями по защите отечества; решительное затыкание рта критикам режима с последующим их преследованием. Целую нацию зажимают в тиски страха, когда лишь жесткие порядки и активные военные действия против врагов начинают казаться напуганным людям единственным спасением. И люди в массе одобряют то, на что в здравом уме никогда бы не согласились.

Подобные параллели сегодня проводят многие, кто знаком с историей. Но отметить интересно другое. Когда Эд Гернон публично поделился своими наблюдениями с общественностью на страницах журнала TV Guide, сопоставив обстановку политической истерии в США накануне вторжения в Ирак и общий климат в предвоенной Германии, сопутствовавший восходу

Третьего рейха, то компания CBS разорвала с Герноном контракт и уволила продюсера с работы «за неверную подачу мотивации телевизионной сети при показе данного фильма» [JO03]. Увольнение за высказывание политических взглядов – событие очень серьезное для страны, привыкшей считать себя свободной.

Однако, большинство американцев словно ослепло и не замечает, что от свобод, гарантированных их конституцией, сегодня уже мало что осталось. Как остаются незамеченными и уже действующие в отношении гражданских лиц секретные трибуналы. Или концлагеря, созданные на заморских военных базах США, где не действуют основополагающие американские законы и где без предъявления обвинений, без контактов с близкими или адвокатами могут годами удерживать «подозреваемых в терроризме».

Один из ныне живущих классиков американской литературы, 77-летний писатель Гор Видал принадлежит к тем немногим, кто не только видит все происходящее, но и много лет громко предупреждает нацию о сползании страны к тоталитаризму: «То разложение, которое предвидел [Бенджамин] Франклин [предупреждая об угрозе деспотизма], приносит свои ужасные плоды. И никто не желает с этим ничего делать. Тут даже речи не идет о какой-то кампании. Как только в социуме, все дела которого – это бизнес, образовалась столь коррумпированная элита, то все, что может из этого получиться – это, несомненно, деспотизм. Это тот вид авторитарного правления, который принесли нам люди Буша. Их закон USA PATRIOT Act – столь же деспотичен, как и все, с чем пришел Гитлер, здесь даже язык во многом используется тот же самый, [причем страна шла к этому уже давно] В одной из моих прошлых книг, „Вечная война ради вечного мира", я продемонстрировал, что язык, применявшийся людьми Клинтона для запугивания американцев террористами, их призывы поступиться на короткое время своими гражданскими правами и свободами – это в точности язык, использовавшийся Гитлером после поджога Рейхстага» [MCO3].

Игры патриархов

В знаменитой «Книге джунглей» Редьярда Киплинга есть примечательный эпизод (в главе «Охота Каа»), словно срисованный с картины современной политической жизни США:

– Мы велики! Мы свободны! Мы достойны восхищения, как ни один народ в джунглях! Мы все так говорим – значит, это правда!

[некоторое время спустя]

– Вы слышите меня, бандерлоги? Хорошо ли вам видно?

– Мы видим тебя, о Каа!

– Бандерлоги, можете ли вы шевельнуть рукой или ногой без моего приказа?

– Без твоего слова мы не можем шевельнуться, о Каа!

– Хорошо! Подойдите на один шаг ближе ко мне… Еще ближе!…

В рассылках одного из довольно известных интернет-форумов (cypherpunks), где об инфотехнологиях и политике, по преимуществу, дискутирует нонконформистски настроенная интеллигенция, накануне

вторжения в Ирак появилось следующее наблюдение, констатированное с долей изумления. Совершенно очевидно, что США решительно намерены вступить в серьезную войну: на раскрутку военных действий уже потрачена уйма денег, в район Персидского залива стянута куча военных кораблей, 100 тысяч солдат переброшены к границам Ирака, ну и так далее. Однако законодательная власть страны в столь критический момент истории демонстрирует полнейшее бездействие. Словно мартышки под взглядом питона, конгрессмены, загипнотизированные ура-патриотической пропагандой, вообще не решаются обсуждать широкомасштабные военные приготовления президентской команды, не говоря уже о необходимом по американским законам официальном объявлении войны…

Далее речь пойдет совершенно о другом. Пример с «гипнозом» был выбран лишь потому, что чрезвычайно наглядно демонстрирует эффективность умелых манипуляций массовым сознанием, будь то сознание рядовой публики или сознание наделенных, казалось бы, властью политиков-парламентариев. При желании и наличии определенных навыков можно, как показывает практика, весьма долго заставлять людей видеть лишь «то, что надо» и абсолютно не замечать «то, что не надо». И хотя вокруг в изобилии происходят вещи, воистину достойные сильнейшего удивления и серьезных размышлений, публика реально ничего не замечает.

В подтверждение этого тезиса далее будет приведено несколько показательных примеров из жизни США за последние несколько лет. Все примеры, учитывая профиль исследования, так или иначе связаны со сферами информационных и высоких технологий. Имеет смысл сразу обратить внимание на очень почтенный возраст всех действующих лиц.

Так – победим!

В ноябре 2000 года практически безвестный 70-летний предприниматель Дэн Колласси вернулся с честно заслуженной пенсии на курортах Флориды и совершил небывалое экономическое чудо. Он спас от неминуемой, уже казалось, гибели подчистую разорившийся космический проект Iridium, задолжавший кредиторам свыше 6 миллиардов долларов. Одно лишь обслуживание созвездия из 66 спутников глобальной мобильной связи стоило компании Motorola около 50 миллионов долларов в месяц, отчего было принято решение разорительные аппараты сжечь в атмосфере, а их останки утопить в океане.

Но тут на сцене появляется некий «ветеран авиационных линий Дэн Колласси, в свое время руководивший такими компаниями как Canadian Pacific Airlines и Pan American World Airlines», и на корню выкупает гигантское многомиллиардное предприятие (армада спутников, наземная сеть станций в разных точках планеты, вся недвижимость и вся интеллектуальная собственность фирмы) за немыслимые 6,5 миллионов долларов наличными и за обещание заплатить еще 18,5 миллионов потом, попозже. За этот самоотверженный поступок американский суд по банкротствам освобождает предпринимателя от всех долгов старой компании Indium LLC, а новая фирма Iridium Satellite начинает чудесное возрождение провалившейся дорогостоящей затеи [ISOO].

Эксплуатация спутников под руководством нового директора сразу стала стоить на порядок меньше – всего 4 миллиона долларов в месяц. Стоимость звонков по мобильной спутниковой связи тоже вдруг упала очень ощутимо – до 1,5 долларов в минуту, что по сравнению с прежними 9 долларами просто смешные деньги. При этом, по прикидкам чудо-предпринимателя, для безубыточного существования переродившейся компании требуется всего-то 60 000 абонентов, а вовсе не миллион, декларировавшийся прежними хозяевами. Для разгона первоначальное денежное вливание в размере 72 миллионов долларов сделало Министерство обороны США, получившее в обмен неограниченное время доступа для 20 000 правительственных служащих (кто-то из недоброжелателей тут же назвал Iridium Satellite «частной спутниковой компанией ЦРУ») [MM01].

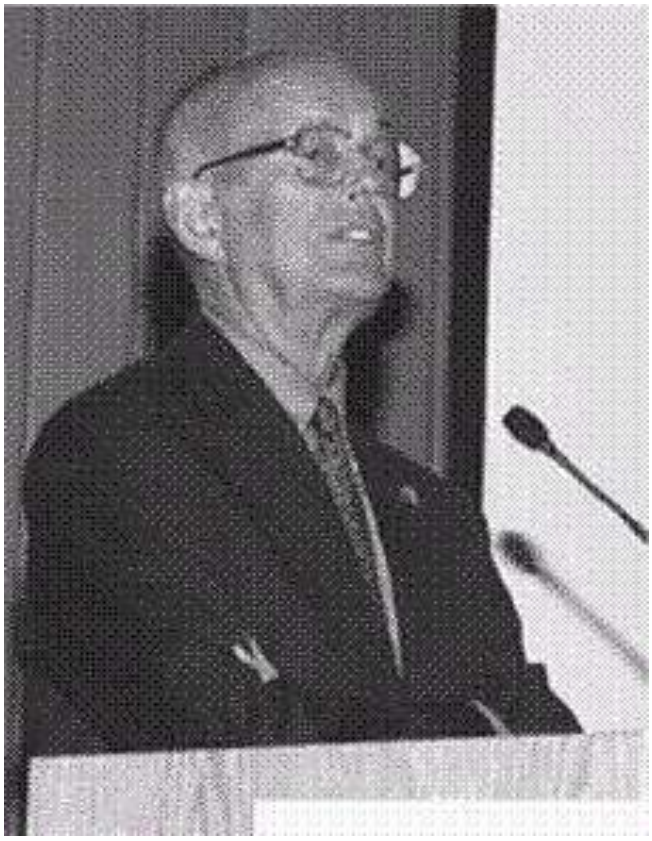
Точно нельзя сказать, откуда взялся намек на связи Колласси (на снимке) с ЦРУ. Но известно, что «ветераном авиалиний» этого человека можно называть весьма относительно, поскольку упомянутые авиакомпании он возглавлял довольно давно, в конце 1970-х годов, когда директором ЦРУ, кстати говоря, был небезызвестный Джордж Буш-папа. В 1990-е же годы, до ухода на пенсию, Колласси был председателем совета директоров крупной холдинговой фирмы CareFirst, подвизающейся на ниве здравоохранения, а одновременно (что тоже не совсем обычно) – еще и директором компании энергетического комплекса США Baltimore Gas Electric Co., владеющей, в частности, рядом энергоблоков крупнейшей атомной электростанции Calvert Cliffs.

Как известно, компания Iridium Satellite ныне функционирует вполне благополучно, весной 2002 года выведены на орбиту еще несколько новых спутников системы, а в начале 2003 года продлен долгосрочный контракт с Пентагоном. Да и свирепые кредиторы совершенно не донимают… Вот такие они, в общем, старики-ветераны, – и здравоохранение державе поднимут с атомными реакторами, и космическую связь спасут от полного

развала. Только вот почему-то никто не берется расследовать механизм столь грандиозного экономического чуда. Видимо, неинтересно.

Негласный надзор

Теперь вновь возвратимся в 2000 год и заглянем в совсем другую организацию, тоже занимающуюся космосом, но существенно в ином аспекте. Научно-исследовательский и разрабатывающий центр Jet Propulsion Laboratory (JPL) работает на базе Калифорнийского технологического института, и по долгосрочному контракту с НАСА отвечает за важнейшие космические миссии, выполняемые без участия человека, – исследования других планет с помощью автоматических кораблей-зондов и аппаратов-роботов. Одно из торжественных мероприятий, проходивших в тот год в JPL, почтил своим личным присутствием директор НАСА Дэн Голдин, начавший свою речь с традиционных славословий в адрес «организаторов всех побед». Первая благодарность была в адрес Дэвида Балтимора, директора Калтеха, а вот вторая прозвучала совершенно неожиданно: «Также я хотел бы поблагодарить адмирала Инмана, ***главу Комитета по надзору за JPL (JPL Oversight Committee) при Калтехе.*** Он не смог сегодня быть здесь, но я разговаривал с ним по телефону. Его преданность команде непоколебима». Выделенная жирным шрифтом часть фразы осталась лишь в тезисах доклада, хранящихся в архиве НАСА [DGOO]. В публикациях средств массовой информации данный фрагмент не появился, а если и был, то тут же исчез [SCOO].



Необычность этой тирады прежде всего в том, что никто и никогда вне JPL прежде не слышал о некоем высоком «Комитете по надзору» за сугубо

гражданской лабораторией, да еще возглавляемом не кем-нибудь, а знаменитым зубром разведки, четырехзвездным адмиралом Бобби Рэем Инманом (которому в 2003 году исполнилось 72 года, на снимке). Как говорилось в одном официальном документе – представлении Инмана на пост министра обороны США – за долгие годы военной карьеры адмирал занимал «наиболее ответственные для национальной безопасности посты», заслужив, по отзывам прессы, репутацию суперзвезды разведывательного сообщества и вообще одного из самых умных людей и проницательнейших администраторов, когда-либо появлявшихся в коридорах власти Вашингтона [WH93].

Директор военно-морской разведки в 1974 году и вице-директор Разведуправления Министерства обороны (РУМО) в 1976, Инман с 1977 года возглавлял Агентство национальной безопасности, которым руководил на протяжении 4 лет. Когда же Джордж Буш-папа занял пост вице-президента США, Инман в 1981 г. стал первым заместителем директора центральной разведки. Вскоре, правда, начался совсем иной этап жизни адмирала – в 1982 г. он ушел в отставку и занялся интенсивным подъемом хайтек-экономики родного отечества. За прошедшие с тех пор годы Бобби Инман был главой или членом совета директоров таких компаний, как Microelectronics and Computer Technology Corporation (MCC), Westmark Systems, Science Applications International Corporation (SAIC), SBC Communications и Xerox. В общей же сложности, как написано в одной из биографий этого неутомимого подвижника, Инман способствовал становлению примерно 30 высокотехнологичных компаний. Среди других интересных должностей адмирала можно отметить пост председателя Банка федерального резерва в Далласе, а также преподавательскую работу лектором в Техасском университете.

Когда к власти в Белом доме пришел демократ Билл Клинтон, то на пост министра обороны он почему-то предложил «республиканца голубых кровей» Бобби Инмана. На официальной церемонии представления в декабре 1993 г. адмирал честно заявил, что вовсе не испытывает желания вступать в столь высокую государственную должность, да и вообще – на последних президентских выборах голосовал не за Клинтона, а за «своего друга, прошлого президента Буша» [AS93]. Но – раз уж так надо – Инман согласен вернуться из бизнеса к кормилу военной власти. Правда, когда в начале 1994 года в Конгрессе начала назревать непростая процедура открытого обсуждения кандидата в новые министры обороны, сулившая массу крайне нелицеприятных вопросов о богатейшей закулисной деятельности адмирала, Инман неожиданно предпочел ретироваться и снял свою кандидатуру с весьма невразумительными объяснениями.

Адмирал практически не дает интервью прессе, но явно продолжает вести активную, хотя и не слишком заметную общественную жизнь, возглавляя разного рода фонды с ничего не говорящими названиями типа Public Agenda Foundation, и время от времени выступает в подшефных университетах с политологическими лекциями. Недавнее разглашение руководящего поста Инмана в тайном космическом «комитете по надзору» – это одна из не очень ясных, но скорее всего умышленных «утечек» информации, время от времени предпринимаемых высшим руководством государства с целями, ведомыми лишь ему одному.

Как бы там ни было, существование курируемого матерым разведчиком Инманом комитета хотя бы отчасти объясняет многие непонятные вещи, происходящие вокруг JPL и НАСА. Например, финансирование на деньги криптографической спецслужбы АНБ работ в JPL по созданию криоробота для глубоколедных бурений и исследований в Антарктиде [HM01]. Или инициативная, без просьб со стороны НАСА, помощь космической разведслужбы NIMA в анализе спутниковых снимков для поисков пропавшего при посадке на Марс спускаемого модуля Polar Lander [NN01]. Или обнаруженная комиссией Конгресса в недрах НАСА инструкция, где весьма профессионально и со знанием дела сотрудникам агентства даются рекомендации о том, как утаивать нежелательные для разглашения данные от запросов FOIA (Freedom Of Information Act – Закон США о праве граждан на доступ к информации) [IM89][KD92].

Впрочем, непонятно почему, предпринятая утечка информации о комитете Инмана не привела ни к каким заметным последствиям или расследованиям. За прошедшие с той поры годы практически ни одного содержательного упоминания о секретном JPL Oversight Committee ни в печатной прессе, ни в Интернете более не появилось. Публика просто не заметила ничего странного.

Планы Маршалла

В начале 2003 года проявился в прессе другой интереснейший старец – 81-летний «шеф-футурист» американских милитаристов Эндрю Маршалл, посаженный на пост директора Управления общих оценок Пентагона еще Ричардом Никсоном в 1974 году и исправно с тех пор переназначаемый каждым новым президентом вне зависимости от партийной принадлежности. В кулуарах Министерства обороны могущественного старца за глаза зовут Иодой, по имени бесконечно древнего предводителя рыцарей-джедаев в «Звездных войнах». А если без шуток, то Маршалла называют одним из наиболее влиятельных и в то же время наиболее неприметным персонажем в Пентагоне, отвечающим за прогнозирование и общее формирование военной стратегии США. Не секрет, что все главные «ястребы» в нынешней госадминистрации – вице-президент Дик Чейни, министр обороны Дон Рамсфелд, его заместитель Пол Вулфовиц – являются «птенцами»-протеже Эндрю Маршалла [DM03].

В 1990-е годы в кругах, близких к Пентагону и военно-промышленному комплексу, легендарную известность обрел небольшой [JD01] 7-страничный меморандум Маршалла (на снимке), скромно озаглавленный «Некоторые соображения о военных революциях». Меморандум призывал к «революции в военном деле» и к новым подходам в военной аналитической работе, когда информационные технологии в тесном увязывании с новаторской военной доктриной полностью изменяют саму природу войны. В эпоху Клинтона политики и генералы пытались игнорировать наставления Маршалла, однако с приходом к власти Джорджа Буша-сына авторитет многоопытного ветерана Холодной войны вырос необычайно. Достаточно сказать, что именно Эндрю Маршалл по просьбе Рамсфелда подготовил весной 2001 года программный доклад Буша о политике нынешней госадминистрации США в области обороны.

В контексте настоящего исследования вряд ли целесообразно углубляться в развернутое изложение взглядов столь влиятельного в США человека на войну. Но нельзя не упомянуть, что именно Маршалл был в свое время вдохновителем концепции затяжной ядерной войны – с постоянными модернизациями оружия, тщательной защитой государственных лидеров в надежных бункерах, выводом ядерного оружия и систем ПРО на земную орбиту. Сейчас у пентагоновского визионера новое увлечение – биоинженерная модификация солдат [GL02]. Выступая летом 2002 года в Дипломатической школе Университета Кентукки, Маршалл поведал, что уже разрабатываются препараты, модифицирующие поведение человека для выполнения спецзадач. Химикаты воздействуют на специфические рецепторы мозга, так что появляется возможность создавать абсолютно бесстрашных солдат, подолгу не спящих солдат, более бдительных и быстрых в реакциях воинов. Короче говоря – не людей уже, а суперсолдат. Еще одна задумка, греющая душу старцу, – оружие мощного психологического воздействия на лидеров стран, которые не нравятся США. Имеется в виду не информационное оружие, а некая способность к демонстрации эдаких грандиозных эффектов, вроде каких-нибудь крупномасштабных феноменов или взрывов в небесах. Ну, «просто показать, что мы могли бы с ними сотворить, если б захотели; просто визуально произвести на людей впечатление»…

Каким образом столь интересный во взглядах человек умудряется занимать немаловажный государственный пост при любых президентах и в сильно пенсионном возрасте – никто, понятное дело, не спрашивает.

Начинал же свою долгую творческую жизнь Эндрю Маршалл в далеком 1949 году, экспертом корпорации RAND по ядерным вооружениям. В высшие политические круги, а именно в члены Совета национальной безопасности при Никсоне, Маршалла привлек в свое время государственный секретарь Генри Киссинджер, о котором и будет следующий рассказ.

Он верну-у-улся!

Именно так – «He's Ba-a-ack!» – была озаглавлена колонка в New York Times, посвященная примечательному «всплытию» 79-летнего Киссинджера на поверхность политической жизни в конце ноября 2002 года [DW02]. Бурные эмоции здесь вполне объяснимы и связаны вот с чем. Как ни упирался и ни возражал президент Буш против создания независимой комиссии по расследованию действий правительства в связи с трагедией 11 сентября 2001 года, под мощным давлением общественности и семей пострадавших комиссию все же пришлось создать. Зато назначение Генри Киссинджера, наставника Буша во внешнеполитических делах, главой этой «независимой» комиссии стало весьма своеобразным ответом госадминистрации на настойчивость правдолюбов. По полному сарказма комментарию колумниста New York Times, кто же еще сможет лучше расследовать преступную атаку на Америку, чем человек, привыкший сам готовить беззаконные атаки Америки? Кто может лучше разоблачить двуличность и лживость правительства, чем человек, сам организовывавший тайные войны и свержения иностранных правительств, секретные бомбардировки, тайные прослушивания политических противников и секретные заговоры? Кто, однако, слывет при этом «столпом общества» и лауреатом Нобелевской премии мира? Суммируя, можно сказать, что в новейшей политической истории Америки нет, вероятно, человека, чье имя чаще связывалось бы со словами «тайны», «секретность» и «заговоры».

Генри Киссинджер

Характерно, что ныне, фактически сразу по назначении на столь чувствительный для общества пост, Киссинджер без обиняков дал понять,

что его комиссия намерена не столько выявлять ошибки и провалы правительства, не сумевшего предотвратить атаки 11 сентября, сколько «попытается помочь администрации лучше узнать тактику и мотивы врага». Откуда следует, что в представлениях бывшего госсекретаря пока у нынешней власти адекватного знания врага нет.

Интересно и то, сколь специфические представления имеет Генри Киссинджер относительно этических стандартов, которыми следует руководствоваться в работе возглавляемой им комиссии. В своих комментариях Киссинджер отметил, что не намерен в связи с новым постом отделять себя от деятельности своей консалтинговой фирмы и сам способен решать, могут ли интересы его клиентов (выплачивающих, заметим, консультанту весьма большие деньги) конфликтовать с интересами расследования. Более того, бывший госсекретарь даже отказался назвать клиентов своей нынешней компании Kissinger Associates. Однако и без того известно, что клиентами Киссинджера являются ведущие многонациональные корпорации, прибыли которых непосредственно зависят от теплых отношений с администрацией в Вашингтоне и правительствами других стран. Понятно, что работа независимой комиссии сопряжена с тем, чтобы задавать весьма неприятные вопросы людям, наделенным очень большой властью. И здесь любой конфликт интересов не только мощно вредит работе комиссии, но и вообще ставит под серьезное сомнение ее выводы.

В отличие от первых трех старых мудрецов, упомянутых в статье, Генри Киссинджер слишком хорошо знаком американской публике, причем далеко не с лучшей стороны. И в его случае никакие гипнотизирующие манипуляции властей с переносом внимания на более важные пустяки не сработали. Под мощным напором протестов и возражений Бушу пришлось-таки убрать Киссинджера из комиссии и назначить на его место бывшего губернатора штата Нью-Джерси Томаса Кина. Человек этот явно не столь знаменит как его предшественник своими заслугами перед отечеством, но, судя по всему, общему делу вполне предан.

Бильдербергский клуб

– Но что же все это значит? – спросил Маугли, который не знал ничего о притягательной силе удава. – Я видел только большую старую змею, которая выписывала зачем-то круги по земле, пока не стемнело…

– А мы с Балу потеряли разум, как малые птенцы, увидев пляску Каа…

Для тех, кто еще не потерял разум от гипнотического мельтешения средств массовой информации, было бы полезно сходить в Интернет на сайт какой-нибудь приличной поисковой машины, того же Google, и поискать там документы, содержащие сразу несколько имен перечисленных выше почтенных старцев. Почти наверняка отловится куча странноватых материалов о всемирном заговоре, тайных правительствах и международных секретных обществах, вроде МЛ2 или «Бильдербергской группы». Подобные тексты большинство трезвомыслящих и рациональных людей обычно отметает не читая – как бред и басни дешевых таблоидов. Но не все здесь так просто. Скорее, совсем наоборот – за массой дезинформации и полнейшей чепухи скрывается нечто чрезвычайно

серьезное.

Среди скандалов, мощно сотрясающих нынешнюю политическую жизнь Великобритании, практически незамеченной прошла новость о появлении в Интернете знаменитого документального фильма Би-Би-Си, который был запрещен в период правления Маргарет Тэтчер и никогда не показывался по телевидению [RC03]. Серия из шести телефильмов под общим названием «Тайное общество» в 1987 году без преувеличений произвела в Британии фурор. Генеральный директор Би-Би-Си Элисдер Милн был тогда с треском уволен, а создателям сериала грозили уголовным преследованием за разглашение государственных секретов. Журналисту Данкану Кэмпбелу, делавшему картину, полиция высадила дверь в его доме и устроила тотальный обыск. Аналогичный обыск с конфискацией магнитных лент «запрещенной» программы был проведен в шотландской штаб-квартире телерадиовещательной корпорации в Глазго.

В целом этот документальный мини-сериал рассказывал о тайнах закулисной политической кухни в высших эшелонах государственной власти. Когда страсти несколько поулеглись, полиция вернула конфискованное, и пять фильмов из шести даже были показаны по ТВ спустя какое-то время. Однако шестую, наиболее интересную ленту, на экраны так и не выпустили. В ней рассказывается о том, что британские премьер-министры вплоть до находившейся тогда у власти Тэтчер, сохраняют давнюю традицию тайных кабинетов, которые и принимают главные политические решения. Причем члены официального правительства зачастую не знают не только имен, но даже самого факта существования более высокой тайной структуры. В итоге совершенно анонимно, без публичного обсуждения и неизвестно кем делаются важнейшие стратегические ходы, вроде закупки атомных субмарин «Трайдент». А дорогущий шпионский спутник Zircon стоимостью свыше полумиллиарда долларов (400 млн фунтов стерлингов), к примеру, был вообще создан и запущен на космическую орбиту без ведома парламента страны.

В конце лета 2003 года видеокопии «запрещенной» серии инициативно, «без спроса инстанций» распространяются через известный веб-сайт BMerberg. org [http://www.bilderberg.org/videos.htm]. Как можно понять из названия, на данном сайте, созданном журналистом и правозащитником Тони Гослингом, накапливаются материалы о деятельности, происхождении и членах так называемой Бильдербергской группы. Так именуется в высшей степени скрытный международный «клуб», собирающий на своих ежегодных трехдневных встречах чрезвычайно влиятельных деятелей мировой политики – действующих и бывших глав ведущих государств и спецслужб, министров, руководителей крупнейших финансовых и индустриальных структур (давними членами этого клуба являются, в частности, Бобби Инман и Генри Киссинджер, причем последний уже многие годы входит в организационный комитет). Имеются очень серьезные свидетельства, что именно на конференциях Бильдербергской группы принимаются многие важнейшие для всей планеты решения. И хотя факт проведения ежегодных встреч этого «клуба» скрыть невозможно – слишком заметные фигуры в них участвуют – центральная пресса о конференциях «бильдербергеров» не пишет

никогда. С давних пор это, по сути дела, абсолютно табуированная тема.

Достоверно известно лишь то, что конференция каждый раз проводится в иной стране – в одном из укромных отелей, куда собираются порядка 100 человек для общения в обстановке строжайшей секретности. Как сообщает энциклопедия Британика, начиная с первой встречи в 1954 году, «конференция предоставляет неофициальную, непринужденную обстановку, в условиях которой те, кто оказывают влияние на национальную политику и международные дела, могут поближе познакомиться друг с другом и обсудить общие проблемы без взятия обязательств. После каждой конференции готовится неофициальный отчет о встрече, распространяемый исключительно среди прошлых и нынешних участников. В отчете докладчики обозначены только по своей стране. Международный оргкомитет каждый год обычно отбирает разных делегатов»… Постоянными же участниками и организаторами мероприятия, начиная с самой первой встречи, являются семьи Рокфеллеров, Ротшильдов и ряда других наиболее богатых и влиятельных кланов мира.

Главная цель сайта Гослинга – добиваться снятия плотной завесы секретности над съездами Бильдербергской группы. В частности, чтобы после каждой встречи столь влиятельной элиты проходила, как это повсеместно делается, пресс-конференция участников. А самое главное, чтобы оргкомитет официально принял и опубликовал декларацию, заверяющую мировую общественность, что любой консенсус, достигаемый при подобных встречах, служит всеобщим, а не их частным интересам.

Пока что никаких сдвигов в этом направлении «бильдербергеры» не демонстрируют. Ибо официально по-прежнему считается, что их как бы нет. Хорошо, что хоть Интернет есть.

Глава 3. Срамные истории

Страницы жизни героя, 1928. Союз до гробовой доски

В апреле 1928 года в Бюро расследований появился новый сотрудник – высокий привлекательный мужчина Клайд Толсон, уроженец штата Миссури и выпускник Университета Джорджа Вашингтона. Очень быстро Толсон стал не только ближайшим личным другом Эдгара Гувера, но и его правой рукой по службе, оттеснив с этих позиций прошлого фаворита Фрэнка Боумена (отдалившегося от шефа вследствие женитьбы).

Карьерный рост Толсона пошел на удивление быстро. Примерно года через два Гувер повысил его до своего помощника, а затем – и до заместителя директора Бюро. На протяжении всех последующих лет Клайд Толсон оставался вторым по влиянию человеком в спецслужбе. После смерти матери Гувера его ближайший друг стал сопровождать Босса буквально повсюду. Парочка вместе приезжала на работу и также дружно отъезжала, они вместе обедали, вместе проводили отпуск и даже одевались нередко одинаково. Если Гуверу надо было уехать в служебную командировку, вместе с ним отправлялся и Толсон. Для всех окружающих было совершенно очевидно, что прочные и нежные отношения заменили

двум закоренелым холостякам брак в его традиционном смысле. После смерти Босса Толсон унаследовал всю его недвижимость и переехал жить в дом Гувера. Когда же пришел и его срок, Толсона, который был на пять лет моложе Гувера, похоронили, словно верную жену, в соседней с сердечным другом могиле.

Поскольку вполне надежных документальных свидетельств у историков нет, принято считать, что гомосексуальные отношения Гувера и Толсона ничем не доказаны. Достоверно известно лишь то, что Дж. Эдгар Гувер всегда очень тщательно, даже щегольски одевался, но при этом фактически не интересовался женщинами. По свидетельству окружавших его людей, начиная с юных лет, еще со школьного возраста, за Гувером вообще не замечали каких-либо романтических свиданий с представительницами противоположного пола. В более же зрелом возрасте он украшал сад и интерьеры своего дома статуями обнаженных юношей. До 43 лет Гувер жил вместе с матерью, а после ее смерти – один, причем горничной было категорически запрещено по утрам входить в его спальню, поскольку, де, «хозяин спит голый». Есть еще, правда, многочисленные намеки на компрометирующие фотографии из нетрадиционной половой жизни Гувера, которыми его шантажировали разведслужбы и мафия. А также устное свидетельство жены психиатра Гувера, которому, будто бы, шеф ФБР в одной из доверительных бесед признавался в своей гомосексуальности. Ну и, наконец, знаменитая первичная реакция президента Ричарда Никсона на известие о смерти Гувера: «Господи Иисусе, этот старый хреносос!». Предполагается, что Никсон входил в круг достаточно близких Гуверу людей и кое-что знал об интимной жизни старого холостяка.

Однако строго говоря, все это весьма косвенные, ничего не доказывающие свидетельства. Да и кому какое дело, в нынешние-то либеральные и весьма терпимые времена, были там отношения интимно-сексуальные или исключительно платонические? Мало ли в истории известно прочных союзов, долгие годы объединявших гомосексуальные пары – от романистки Мэри Рено и Джули Маллард (50 лет) или писательницы Гертруды Стайн и Элис Токлас (34 года) до гения Возрождения Леонардо да Винчи и его ученика Джакомо Карпотти (30 лет). Список этот при желании можно сделать очень длинным, и ничего особенного не произойдет, если к нему добавится еще одна пара «тихих голубых» с 44-летним стажем (1928-1972) – Эдгар Гувер и Клайд Толсон (или, как их за глаза называли в ФБР, «Дж. Эдна и мама Толсон»).

Беда лишь в том, что Гувер не был «тихим голубым». Он всегда выставлял себя человеком высочайшей религиозности, добропорядочности и нравственности, приходя в дикую ярость, едва хоть кто-то намекал на его гомосексуальность. Стоило в 30-е годы репортеру Рэю Такеру позволить себе в самых обтекаемых выражениях затронуть в журнале Collier голубизну шефа ФБР, в Бюро тут же завели на Такера дело. Когда собрали компромат, то пустили в прессу такие подробности о не слишком безупречной жизни неосторожного журналиста, что далее последовал полный крах его карьеры. Остальные деятели прессы вполне поняли предупреждение и впредь крайне опасались хоть каким-то боком зацепить эту сторону жизни Гувера Всемогущего.

Обостренный интерес главы ФБР к чужой постельной жизни, нетрадиционной сексуальной ориентации людей и вообще к орально-генитальной тематике, глубоко запечатлен в секретных файлах Гувера. В этом тайном архиве десятилетиями наравне с фактами накапливались также и слухи, кляузы или домыслы, способные скомпрометировать кого угодно. Этим материалам либо давался ход, как было с компрометацией Эдлая Стивенсона, либерального губернатора Иллинойса и претендента на президентский пост, о ком Гувер запустил ничем не подтвержденный слух, будто Стивенсон – гей. Либо данные интенсивно накапливались для удобного случая, как это было с интенсивной слежкой за товарками первой леди государства Элеоноры Рузвельт, которая весьма не симпатизировала Гуверу, а тот в ответ набирал компромат, пытаясь уличить ее в лесбийских связях.

Впрочем, по оценкам самого Гувера, полномочий его ведомства в контроле за личной и интимной жизнью граждан было все же маловато. Вот одно из его знаменитых высказываний: «Должен с сожалением сказать, что мы в ФБР бессильны действовать в случаях орально-генитальных сношений людей, за исключением, правда, тех случаев, когда они каким-то образом начинают мешать международной торговле».

Большие маневры: Microsoft – Пентагон

Год 1998-й был одним из наиболее драматичных в многолетних отношениях другой, совершенно иного рода, пары – софтверной корпорации-гиганта Microsoft и Министерства обороны США. Этот союз, казалось бы, ну ни с какого, даже самого глумливого, боку нельзя называть «гомосексуальным», поскольку природа партнеров абсолютна различна. Главное предназначение Пентагона, сама его суть, – это обеспечение безопасности американского государства военными средствами. А Microsoft – это, как ни крути, самый большой и известный на данной планете изготовитель программного обеспечения, главная цель (и залог успеха) которого – сделать свои продукты максимально дружественными и легкими в употреблении. Уделяя, конечно, вопросам компьютерной безопасности определенное внимание, но не ставя их в ущерб бизнесу. И хотя американская софтверная индустрия в достатке имеет намного более защищенные программы других разработчиков, возлюбил-таки Пентагон горячей постыдной любовью именно Microsoft, на весь свет знаменитую бессчетным количеством дыр в защите своего ПО. Особо эта противоестественная связь не скрывается, да и как ее спрячешь, однако наиболее срамные эпизоды партнеры все же стараются хоть как-то прикрыть.

Нет человека – нет проблемы

Итак, год 1998-й. Некто Эд Карри, глава небольшой техасской фирмы Lone Star Evaluation Labs, специализирующейся на компьютерной безопасности, развернул весьма активную кампанию против корпорации Microsoft, по заказу которой прежде работал. Несмотря на несопоставимое,

просто-таки комичное различие в соотношении противостоящих сил, обвинения Карри были услышаны и подхвачены прессой, благо повод выглядел достаточно серьезным. Суть обвинений сводилась к тому, что Министерство обороны и другие правительственные ведомства США нарушают свои же собственные правила, широко применяя крайне небезопасную операционную систему Windows NT. В Пентагоне на этот счет предпочли отмалчиваться, а в Microsoft попытались все свести к личным обидам Карри на бывшего работодателя.

Проблема же, вокруг которой разгорелся конфликт, – это сертификация NT на соответствие уровню C2. Ныне эта классификация уже устарела, а прежде уровень C2 был одним из базовых уровней безопасности компьютерных систем, присваиваемых при соответствии ряду надлежащих критериев, определенных в «Оранжевой книге» Агентства национальной безопасности США. Серьезные правительственные ведомства, такие как Пентагон, могли устанавливать у себя компьютерное обеспечение лишь при наличии у того сертификата не ниже C2.

Поскольку Эд Карри был серьезным экспертом по компьютерной безопасности, в прошлом военным человеком и специалистом, аттестованным АНБ, в 1994 г. Microsoft выбрала именно его для помощи компании в получении сертификата C2 на Windows NT 3.5. В ходе этих работ Карри разработал специальные диагностические средства и по просьбе Microsoft создал тестовую программу RAMP для оценки уровня соответствия критериям C2. [NP98].

Вот тут-то и разгорелся конфликт, деликатные подробности которого так и остались тайной. Ясно лишь то, что тестовые средства эксперта упорно находили в NT массу трудноустранимых слабостей. Как результат, в 1995 году Microsoft разорвала контракт с Карри по причинам, «которые адвокаты компании рекомендовали не разглашать». В 1997 году Microsoft подрядила корпорацию Science Applications International (SAIC, с этой любопытной фирмой мы еще не раз встретимся далее) для продолжения работ по сертификации NT на C2. На одну из версий системы, уже к тому времени устаревшую 3.5, сертификат был-таки получен, а массовые закупки последующих, более современных версий NT (3.51, 4.0 и т.д.) обосновывались «скорым получением» соответствующего сертификата.

Ну а Эд Карри после потери контракта оказался фактически разорен, поскольку все средства вкладывал в разработку RAMP и ставшее никому ненужным тестирование. Тогда Карри и развернул кампанию, чтобы предупредить госадминистрацию и общественность в целом о «приобретении правительством миллионов копий несертифицированных версий Windows NT, которые не удовлетворяют критериям уровня C2 Министерства обороны и других агентств». К осени 1998 года он даже сумел добраться до высшего руководства Пентагона, написав лично министру обороны Уильяму Коэну. В этом письме говорилось, что его контракт по сертификации C2 был разорван Microsoft по той причине, что Карри отказался покрывать факты нарушения компанией базовых рекомендаций «Оранжевой книги»: «Microsoft умышленно скрывает информацию о дырах в защите, опасаясь, что признание таких недочетов сократит количество копий, заказываемых правительством… Я поднимал эти вопросы на внутренних обсуждениях в Microsoft, а в результате стал

объектом угроз и попыток подкупа» [MF98].

Пентагон откликнулся на это послание, и в октябре Эда Карри принял для беседы помощник министра обороны Дик Шэфер в компании с несколькими чинами из АНБ США. Никаких официальных решений после этой встречи не последовало, сам же Карри сообщил прессе лишь о своих впечатлениях от беседы: «Они знают, что я прав. И знают, что нарушают собственные правила безопасности. Но по сути дела, сказали они, все это неважно, и они будут продолжать использовать версию 4.0… Было сказано, что у них связаны руки, и в основном здесь решают деньги, а не соображения безопасности…» [JD99].

Ясно, что все эти объяснения совершенно не удовлетворили Карри, и он решает продолжить свою обличительную кампанию в прессе – однако в марте 1999 года скоропостижно умирает от сердечного приступа. И тут спустя несколько месяцев начинает происходить нечто необычное. Понятно, что более бить в набат стало некому, и текущие публикации прекратились, но одновременно в Интернете понемногу стали пропадать опубликованные прежде статьи об Эде Карри [GS98a][GS98b], само его имя в поисковых системах новостных сайтов, а также ссылки на соответствующие материалы в архивах. Наиболее ярко это было видно на примере веб-сайта журнала «Правительственные компьютерные новости» (Government Computer News, www.gcn.com), подразделения компании Washington Post. Осенью 1998 года там было опубликовано несколько заметок [GS98a][GS98b] обо всей этой истории, однако к сентябрю 1999 архив GCN (gcn.com/archives/) за предыдущий год представлял собой весьма странное зрелище: подборка всех выпусков с января по август, а затем – почему-то сразу за декабрь. Без каких-либо объяснений отсутствия номеров за осенние месяцы, когда был апофеоз скандальной истории с несговорчивым экспертом…

Подобный способ решения проблемы выглядел, конечно, чересчур вызывающе, поэтому впоследствии все ссылки на архивные номера GCN были вновь аккуратно восстановлены. Однако слова «Ed Curry» так и остались табуированным в поисковой системе сайта, так что поиски по имени вплоть до осени 2003 г. не приносили никаких результатов. Более того, аналогичный нулевой результат приносят и поиски любых публикаций репортера GCN Грегори Слободкина, освещавшего не только этот, но и другие срамные эпизоды из богатой истории отношений Microsoft и Пентагона.

Летом все того же 1998 года, например, Слободкин раскопал и опубликовал совсем неприличную историю о неприятностях ракетного крейсера ВМС США «Иорктаун». Это экспериментальный, так называемый «умный корабль» (smart ship), важнейшие системы жизнеобеспечения которого управляются компьютерами без участия человека. И что немаловажно – под руководством операционной системы Windows NT 4.0. Так вот, однажды вся эта махина, находясь в открытом море, на три без малого часа встала в полный ступор из-за наглухо зависшего программного обеспечения. Причем произошло это из-за совершенно пустяковой оплошности одного из операторов, занимавшегося калибровкой клапанов топливной системы и записавшего в какую-то из ячеек расчетной таблицы нулевое значение. Ну а далее пошла операция деления на этот самый

нуль. С подобной ерундой справляется даже самый дешевый калькулятор, однако здесь в терминале оператора система дала ошибку переполнения памяти. Причем ошибка быстро перекинулась на другие компьютеры локальной сети корабля, началась цепная реакция, и по известному принципу домино рухнула вся бортовая система. Которую удалось восстановить и перезагрузить лишь через 2 часа 45 минут, в течение которых здоровенный боевой корабль оставался по сути дела беспомощен и неуправляем [GS98c].

Когда это ЧП, которое почти год командованию флота удавалось скрывать, все же попало на страницы прессы, поднялся большой шум. Все недоумевали, почему военным кораблем управляет не заведомо более надежная ОС Unix, а Windows. Внятных ответов, правда, никто не дождался. А не в меру ретивый репортер Слободкин вскоре перестал работать в «Правительственных компьютерных новостях». Как говорил один известный политик, нет человека – нет проблемы. Поэтому и многочисленные прежде публикации Слободкина поисковая система сайта GCN ныне находить отказывается. Попутно, в точности по Оруэллу, скорректировано и прошлое «умного корабля» USS Yorktown – статьи про конфуз с упавшей операционной системой также не отыскиваются.

Такая трудная любовь

Если официальные представители Пентагона предпочитают очень уклончиво отвечать на прямые вопросы о причинах столь горячей любви военных к ненадежной продукции Microsoft, то это вовсе не значит, что обрисованная проблема мало кого здесь беспокоит. Многих специалистов очень беспокоит, но люди это дисциплинированные и шума в прессе предпочитают не поднимать. Лишь иногда, когда в Интернет или прессу просочится какой-нибудь документ-отчет о внутренних совещаниях, становится отчетливо ясна вся необычность ситуации, в которой оказались вооруженные силы. Не только в США, естественно, но и в других странах, поскольку операционные системы и программное обеспечение Microsoft безраздельно господствуют на компьютерах по всему миру (для настольных систем доля Windows, напомним, составляет более 90%).

Небезынтересно заглянуть на один из закрытых семинаров так называемого «Форума по сетевой безопасности» (Network Security Framework Forum, NSFF) – рабочей группы, созданной АНБ для обсуждения проблем и потребностей Министерства обороны США в области защиты информации. Эта группа из представителей армии, спецслужб, промышленности и исследовательских институтов собирается примерно раз в шесть недель. Обычно мероприятие проходит за закрытыми дверями, но по какому-то недосмотру (а может и умышленно) в интернет-издании IIEE Cipher был однажды опубликован обзор одного из таких семинаров, проходившего в памятном 1998 году и посвященного созданию системы многоуровневой компьютерной безопасности MLS (Multi Level Security). Система MLS, как предполагается, должна надежно защитить критично важные элементы информационной инфраструктуры США [JE98].

В контексте данного повествования нас, естественно, будут интересовать в этом документе лишь нюансы взаимоотношений Microsoft и

силовых ведомств США. Прежде всего, в выступлениях участников семинара NSFF отчетливо слышны громкая критика и осуждение недальновидной политики Пентагона в области закупок программного обеспечения. Так, представитель Sun Microsystems отметил, что Министерство обороны, в своей любви к Windows, совсем не закупает операционные системы Trusted Solaris, являющиеся одним из немногих коммерческих MLS-продуктов. Ситуация необычна вдвойне, поскольку американскую систему Trusted Solaris приобретают другие государства, озабоченные безопасностью своих компьютерных систем, включая Великобританию, Канаду, Южную Африку, Японию, Сингапур, Польшу и Чехию. Попутно выступавший язвительно заметил, что Австралия тоже начала было закупать Trusted Solaris, однако затем решила, что сойдет и NT.

Другой участник встречи (от независимой исследовательской компании) при обсуждении принципиальных сложностей в обеспечении защиты Windows NT заметил, что новейшая по тем временам операционная система NT 5.0 имеет 26 миллионов строк кода, из которых в среднем 20% заменяются ежегодно. В подобных условиях ожидать появления сколь-нибудь безопасного и надежно протестированного продукта, строго говоря, просто нереально.

Самый же пикантный момент семинара был в следующем. Хотя на встрече присутствовало около трех сотен участников, т.е. большинство представителей индустрии, не было ни одного представителя собственно от корпорации Microsoft. Причем отсутствие это было вовсе не случайным. Несколько ранее на одной из встреч на высшем уровне правительственные чиновники интересовались у руководства Microsoft относительно их планов участия в «многоуровневой системе безопасности», а в ответ услышали, что у Microsoft нет интереса к MLS. Корпорация «не видит для себя дел в MLS, так что от нее не следует ожидать ничего в этой области». Причины же полнейшего равнодушия – тривиально экономические: Министерство обороны США составляет менее 1% в гигантском бизнесе Microsoft, так что даже если бы MLS была единственной компьютерной системой Пентагона, этого все равно было бы недостаточно, чтобы Microsoft затрачивала на нее свои усилия…

Надо отметить, что за прошедшие с той поры годы высокомерное, как ни крути, отношение Microsoft к интересам военных претерпело существенные перемены. И политическая обстановка в мире сильно изменилась, и Windows-программы на рынке начало ощутимо теснить конкурирующее открытое ПО на основе ОС Linux. Да и сам Пентагон, как мы сейчас увидим, далеко не бездействовал.

Винтукей – для больших кораблей

Последующий ход событий лучше всего осветить на одном характерном примере, особо поразительном, если не забывать историю с «умным кораблем» Yorktown. Поскольку и этот сюжет тесно связывает Microsoft с американскими военно-морскими силами.

Итак, в 1999 году к руководству корпорации присоединятся ушедший в отставку боевой адмирал Роберт «Вилли» Уильямсон, поначалу в

качестве директора бизнес-стратегии, а несколько позже – директора правительственных программ Microsoft. Большой военный путь Уильямсона включает свыше 200 боевых операций в Юго-Восточной Азии (Вьетнам); на рубеже 1980-1990-х годов – командование авианосцем Nimitz, во времена президента Буша-папы поддерживавшим с моря операцию «Буря в пустыне»; затем, во время боевых действий НАТО на Балканах – командование средиземноморской авианосной группой «Джон Ф. Кеннеди». Под конец же военной карьеры именно адмирал Уильямсон был старшим военным советником министра ВМС, ведая исследованиями, разработками и технологическими закупками флота [MF02].

Приход Уильямсона в Microsoft несколько необычным образом отразился на характере личных финансовых вложений главы и основателя корпорации Билла Гейтса – самого богатого на этой планете человека, если верить статистике. Прежде его личная инвестиционная фирма Cascade Investment вкладывала деньги в транспорт, медицину, биотехнологии и прочие вполне мирные области. Однако в феврале 2000 г. стало известно о закупке Cascade большого пакета акций судоверфи Newport News Shipbuilding, специализирующейся на строительстве атомных авианосцев. В результате Билл Гейтс стал одним из двух крупнейших персональных инвесторов Newport News Shipbuilding, владеющим 2,6 миллионами (8%) акций этой компании на сумму свыше 70 миллионов долларов [APOO].

А через несколько месяцев, летом 2000 года пришла совсем удивительная весть: в новейшем авианосце ВМС США следующего поколения для управления коммуникационным оборудованием и вооружениями, системами запуска самолетов и прочей бортовой электроникой будет использоваться операционная система Microsoft Windows 2000 (или «Винтукей» на жаргоне компьютерщиков, от неформального названия ОС Win2K) [FCOO].

Атомный авианосец CVN-77 создается судоверфью Newport News Shipbuilding, спустившей на воду 10 из последних 12 авианосцев Военно-морских сил США. Для разработки интегрированной системы вооружений нового корабля была избрана фирма Lockheed Martin, а та, в свою очередь, пригласила в проект корпорацию Microsoft.

Атомный авианосец CVN –77

К февралю 2001 года судоверфь окончательно получила 3,8-миллиардный контракт на строительство нового супер-корабля CVN-77, который стал десятым и последним в ряду ядерных авианосцев класса «Нимиц» и должен вступить в строй в 2008 году. Microsoft тем временем подписала контракт на оснащение своим программным обеспечением,

создаваемым для CVN-77, и всех остальных кораблей этого класса – семи уже существующих и еще двух строящихся [FC01].

И, наконец, в конце 2002 года произошло еще одно примечательное событие, тоже, вероятно, неслучайное. Авианосцу CVN-77 было официально присвоено название «George H.W. Bush» в честь 41-го президента США и папы президента Джорджа Буша-сына [NS02].

Джордж Буш-папа (в центре) – человек и корабль

Что означают сертификаты?

Примерно в то же время, когда Буш-папа становился не только человеком, но и кораблем, корпорация Microsoft известила всех поклонников своей продукции, что ОС Windows 2000 получила от АНБ США сертификат соответствия «Уровню 4» по международной системе общих критериев компьютерной безопасности или кратко EAL4 (от «Common Criteria Evaluation Assurance Level 4 certification») [RE02]. Здесь заметим, что к 2002 г. в процедуре сертификации произошли существенные перемены: национальную «Оранжевую книгу» сменили международные «Общие критерии», а сам процесс государственной сертификации стали проводить не спецслужбы, а наделенные полномочиями коммерческие компании и институты.

Поскольку общие критерии безопасности разрабатываются совместно спецслужбами ведущих стран Запада, то новый сертификат признается по крайней мере в 15 государствах и формально открывает Windows 2000 дорогу для официального использования в правительственных учреждениях. По словам Крега Манди, главного директора Microsoft по технологиям, процесс сертификации занял три года и стоил корпорации «многие-многие миллионы долларов». От указания точной цифры затрат Манди, правда, воздержался.

Что же на деле означает сертификат EAL4? С точки зрения реальной безопасности – практически ничего. Программные продукты Microsoft слишком хорошо известны изобилием дыр в защите, никто, естественно, всерьез и не предполагает, будто от получения сертификата Windows 2000 стала вдруг «пуленепробиваемой». По сути дела, сертификат лишь признает, что тестирование независимыми экспертами третьей стороны (в данном случае – уже знакомой нам корпорацией SAIC) подтвердило – код

программ действительно работает так, как заявляет изготовитель.

Попутно нелишне отметить, что и прошлые (времен Эда Карри) сертификаты на соответствие уровню C2 «Оранжевой книги» также были чистой формальностью. Поскольку на самом деле уровень C2 никогда не присваивался операционной системе вообще, а только вполне конкретной конфигурации ОС, работающей на вполне конкретной машине. Так, Windows NT 3.5 была аттестована на уровень C2 в условиях компьютеров Compaq ProLiant 2000, ProLiant 4000 и DECpc AXP/150. Причем, что существенно, только в условиях автономной работы машины, без каких-либо подсоединений к сети. Понятно, что на самом деле Windows NT повсеместно используется именно как сетевая операционная система.

Как бы там ни было, но для правительственных заказчиков наличие сертификата крайне важно, поскольку официально во многих государственных ведомствах работать с документами можно лишь на тех компьютерах, где установлено ПО, сертифицированное на соответствия принятым стандартам безопасности. Ныне это Common Criteria (CC). Конкретно о том, что означает уровень CC EAL4, лучше всего процитировать мнение сведущего эксперта. Вот что говорит Джонатан Шапиро, профессор Университета Джонса Хопкинса, участвующий в обкатке новых, еще далеких от завершения CC, и много лет занимающийся вопросами тестирования ПО на предмет безопасности:

Номер уровня оценки от 1 до 7, по идее создателей критериев, выражает степень доверия конкретной системе. Самый низший уровень EAL1 означает, по сути дела, что изготовителю просто достаточно показаться на официальной встрече в инстанциях. Высший уровень EAL7 означает, что все ключевые части системы строго протестированы математическими методами (правда, общедоступного описания этих методов нет). Уровень же EAL4 означает, что документация по архитектуре системы была оценена с применением нетребовательных критериев. Эту оценку можно уподобить поверхностной аудиторской проверке бухгалтерии, когда аудитор просматривает оформление бумаг на предмет соответствия общепринятым стандартам, однако совсем не углубляется в проверку правильности каких-либо цифр. Оценка EAL4 не требует исследования собственно программ, и никаких исходных кодов здесь не проверяется. Что же здесь реально оценивается, так это огромное количество документации, описывающей процесс работы программного обеспечения. Причем документация эта в принципе не может ничего сказать о качестве самого программного обеспечения.

Если же говорить в терминах компьютерной функциональности, то система с конкретным сертификатом EAL4, полученным на Windows 2000, не подразумевает ни подключение к Интернету; ни работу с электронной почтой; ни установку программ от разработчика, к которому нет 100-процентного доверия (сама корпорация Microsoft, кстати говоря, замечена в рассылке клиентам компакт-дисков с ПО, зараженным вирусом).

Таким образом, заключает Шапиро (после существенно более развернутого объяснения), в данном конкретном случае сертификат соответствия EAL4 свидетельствует лишь о следующем: корпорация Microsoft потратила многие миллионы долларов на создание документации,

демонстрирующей, что Windows 2000 четко удовлетворяет неадекватному набору требований безопасности, а всякий пользователь может быть вполне уверен, что именно так дела тут и обстоят [JS02].

Дело государственной важности

Закупки продукции Microsoft продолжаются Пентагоном во все возрастающих количествах. Летом 2003 года пришла новость о рекордном, «крупнейшем в истории единовременном контракте, в рамках которого главный в мире изготовитель программного обеспечения поставит Армии США программ на 471 миллион долларов для 494 000 персональных компьютеров» [RE03].

Нехитрые арифметически подсчеты показывают, что оснащение каждой машины программами обходится почти в тысячу (953,4) долларов. Если учесть, что новое ПО устанавливается, как правило, на новые машины, которые закупаются с уже предустановленной продавцом (и, соответственно, также оплаченной) ОС Windows, то по сути дела оплата происходит дважды…

В августе всеамериканская Ассоциация компьютерной и коммуникационной индустрии (CCIA) выступила со специальным обращением, призывающим новый Департамент безопасности отечества (DHS) не применять программное обеспечение Microsoft. Мы полагаем, говорится в этом обращении к главе DHS Тому Риджу, что действительно безопасные программы должны изначально создаваться в такой системе приоритетов, где безопасность поставлена на самое высокое место. В Microsoft же намного больше заинтересованы в экономическом маркетинге и конкурентноспособности, нежели в безопасности. Последние примеры с тяжелейшими последствиями от воздействия компьютерной инфекции, такой как черви Slammer или Blaster, свидетельствуют, что это следствие особенностей плохо защищенного программного обеспечения Microsoft. Исключительно из-за опоры на это ПО, в частности, за последнее время серьезно пострадали интранет-сеть морской пехоты США, железнодорожная система CSX, автомобильный департамент Мэриленда, авиакомпания Air Canada и одна из ядерных электростанций… [ТЮЗ].

Как показывают последующие события, ни подобные призывы, ни еженедельно появляющиеся сигналы о все новых дырах в микрософтовском ПО, ничто вообще не в силах поколебать преданную и многих озадачивающую любовь американских властей к продуктам Microsoft. В массовых количествах их покупает армия, покупает флот, авиация и все остальные. Вот и Департамент безопасности отечества США уже выбрал Windows-программы для своих настольных систем и серверов, подписав с Microsoft контракт на 90 миллионов долларов.

Конца у этой занятной истории явно не наблюдается, а для достойного завершения главы отлично подойдут слова Стюарта Оукена, одного из ответственных деятелей корпорации Microsoft, ведающего вопросами безопасности. Комментируя новые решительные инициативы корпорации по укреплению защиты своего ПО от хакеров и вирусов-червей, в октябре 2003 года Оукен поведал, что благодаря новым мерам защиты операционных систем Windows теперь программы скорее будут

обрушиваться, нежели позволять хакерам проникновение в систему. Иными словами, раз не получается защитить, постараемся обеспечить надежный ступор [SO03].

Особо заманчиво эта перспектива выглядит, вероятно, для экипажей атомных авианосцев США и прочих военных пользователей ОС Windows.

Жертвы аборта

Этот сюжет совсем, казалось бы, не подходит для раздела «срамные истории», поскольку ничего позорного здесь нет совершенно. Скорее наоборот, речь пойдет о выдающемся достижении научной и инженерной мысли, бесспорно заслуживающем всяческих восторгов и дифирамбов. Однако пресса об этом достижении который уже год упорно молчит, а малейшие следы, ниточки и подробности данного сюжета столь тщательно уничтожаются в Интернете, что и прочесть-то о нем больше негде, кроме как здесь. И, что любопытно, каким-то боком эта история, как и предыдущая, тоже связана с военно-морскими силами США.

Голоса в пустоте

На рубеже лета и осени 2003 года в бескрайнем потоке пресс-релизов компьютерных фирм промелькнула пара любопытнейших документов, на которые новостные агентства не обратили абсолютно никакого внимания. Столь полное и дружное молчание СМИ представляется явно несправедливым, особенно если учесть, что за документами этими на самом деле стоит намного более значительная, по-детективному закрученная история.

Первый из проигнорированных пресс-релизов выпущен калифорнийской компанией Irvine Sensors, сообщившей о разработке и демонстрации «полного упакованного компьютера» (Complete Stacked Computer), ужатого до объема 1/2 кубического дюйма (платформа площадью 1 кв. дюйм и высотой пол-дюйма). О микрокомпьютерах, встраиваемых в наручные часы, пресса уже сообщала неоднократно, однако то, что удалось сделать Irvine Sensors с помощью своей фирменной технологии упаковки чипов Neo-Stacking, не делал точно еще никто. В данном случае в комплект вошли интеловский 206-мегагерцевый процессор StrongARM SA-1110, его сопроцессор SA-1111, чип с перепрограммируемой логикой Xilinx Coolrunner, 256 Мб загрузочной флэш-памяти Intel StrataFlash, I Гб оперативной памяти Micron SDRAM, 8 Гб твердотельного ЗУ на основе 16 чипов флэш-памяти Samsung. Плюс массив необходимых для полноценной работы резисторов и конденсаторов, а также множество самых разных интерфейсных портов для подключения монитора, клавиатуры и прочей периферии: USB, UART, IrDA, SSP, PS/2, аудио/видео и проч. Работает все это хозяйство под управлением «стандартной операционной системы», позволяющей использовать широко доступное коммерческое ПО [IS03].

Поскольку фирма Irvine Sensors, существующая с 1974 года, уже очень давно страдает от недостатка внимания прессы, президент компании Джон Карсон даже в релизе отметил, что «за последнее время в индустрии

наблюдались анонсы и намного менее впечатляющих достижений, поэтому мы полагаем своевременным привлечь внимание мира к нашей технологии»… Увы, внимание мира не удалось привлечь и на этот раз, судя по тотальному отсутствию реакции СМИ за прошедший с момента публикации месяц.

Чтобы хоть отчасти объяснить столь удивительное равнодушие к Irvine Sensors и ее выдающейся технологии упаковки чипов, обратимся к пресс-релизу совсем другой компании, на первый взгляд никакого отношения к первой не имеющей. Но при этом столь же несправедливо обделенной вниманием информационных служб к своей безусловно неординарной разработке. Речь идет о небольшой английской фирме Aspex Technology, много лет безуспешно продвигающей на рынок массивно-параллельную (SIMD) процессорную архитектуру собственной разработки – «ассоциативный стринг-процессор Linedancer».

В совсем недавнем, сентябрьском пресс-релизе Aspex извещается о создании нового программируемого микропроцессора Linedancer-HD, предназначенного для обработки изображений высокой четкости, и на этот раз содержащего 8192 «ассоциативных процессорных элемента» с рабочими частотами до 400 МГц. [ATO3].

Заметим, что даже предыдущий, двухлетней давности 266-мегагерцевый чип Linedancer, содержавший 4096 «элементарных процессоров», представлял собой нечто выдающееся – полностью программно, на C/C++ управляемая архитектура, легко масштабируемая и в разы превосходящая по быстродействию остальные, намного более дорогие решения аналогичного класса – заказные микросхемы (ASIC) и чипы перепрограммируемой логики (FPGA). Но почему-то впечатляющие достоинства этого высокопроизводительного и одновременно сравнительно дешевого процессора вполне очевидны лишь для самой Aspex, руководство которой в 2000-м году уверенно обещало «скорое и повсеместное распространение» своей технологии и скромно претендовало к 2002-году примерно на 10% от 15-миллиардного рынка широкополосных (ADSL) и беспроводных (3G) коммуникаций [ETOO].

Ныне уже понятно, что никакого покорения рынка не произошло. О фирме Aspex никто как и прежде знать не знает, а нынешнее позиционирование нового чипа Linedancer-HD как технологии обработки изображений, а не высокоскоростных телекоммуникаций, – это очевидное свидетельство перепрофилирования компании. Подобных историй в индустрии случается каждый день по дюжине, однако Aspex – случай особый. Хотя бы по той причине, что ресурсоемкой обработкой графики, задачами трехмерной визуализации и объемного моделирования здесь занимались давным-давно, причем весьма успешно. Но только это о-очень большая тайна (неразрывно связанная, заметим, с корпорацией Irvine Sensors и военно-промышленным комплексом США).

Ложь, ложь и снова ложь

Если сегодня кто-то попытается установить, что же представляет собой фирма Aspex Technology, то наткнется на трехэтажную ложь, завуалированную двусмысленными формулировками. Вот тому типичный

пример – подробный профиль компании из каталога стартапов специализированного издания Semiconductor Times. Читаем: «Джон Ланкастер, Анаргирос Крикелис и Иэн Яловецки основали Aspex в ноябре 1999 года, чтобы стать ведущим поставщиком высокопроизводительных процессоров для коммуникационных приложений на рынках DSL и 3G…» [ST02].

В действительности фирма эта вовсе не стартап, поскольку создана она почти 20 лет назад – в середине 1980-х, всего года на три позже Sun Microsystems, к примеру. И называлась она тогда, кстати, похоже – Aspex Microsystems. Учредили ее в ту пору действительно три перечисленных человека, но – и это очень существенное умолчание – под руководством четвертого, Р. Майка Ли. Все эти люди работали в университете Brunei (г. Аксбридж, графство Мидлэсекс) и организовали свою фирму для коммерческого продвижения перспективной разработки Майка Ли – «ассоциативного стринг-процессора сверхбольшой интеграции» или кратко VASP-чипа (от Very large scale integration Associative String Processor).

Если заглянуть еще раз в профиль компании из Semiconductor Times, то прочтем, что «Linedancer (VASP-4096) – это первый из серии процессоров Aspex». И это вранье, ибо к 1998 году в истории фирмы уже были созданы и 256-, и 1024-элементные чипы. Причем в 1990-е годы эти разработки весьма активно и успешно внедрялись в практические приложения – правда, в США, причем в военно-космической области. Именно это обстоятельство, судя по всему, стало причиной безвременной кончины Aspex Microsystems в 1999 году и труднообъяснимого иначе рождения «стартапа» Aspex Technology безо всякой благородной родословной и каких-либо связей с американским ВПК [AM97].

Сокрушительный успех

К середине 1990-х годов у Aspex установились крайне плодотворные деловые отношения с американской корпорацией Irvine Sensors (ISC), разработавшей весьма специфический процесс трехмерной (3D) упаковки кремниевых чипов, обеспечивающий очень плотные и быстрые межсоединения. Первоначально технология была изобретена в ISC для микросхем памяти, получила названия Chip-stacking или Cubing, и разрабатывалась по контрактам НАСА и Министерства обороны США. Технология «кубирования» оказалась для военных на редкость хороша – обеспечивала увеличение скоростей обработки данных, а также резко снижала размеры чипов при одновременном уменьшении энергопотребления и веса.

Весьма успешные итоги работы ISC по заказу НАСА привлекли внимание корпорации ШМ, увидевшей в 3В-упаковке памяти большие коммерческие перспективы. Итогом сотрудничества ШМ и Irvine Sensors стал их совместный «Центр разработки процесса кубирования» (Cubing Process Development Center при заводах IBM Essex Junction, штат Вермонт), начавший выпуск «коротких стеков» упакованной DRAM-памяти в 1994 году [SC96].

А чуть позже произошло совсем интересное событие, когда в Irvine Sensors появилась технология трехмерной искусственной нейросети 3DANN

(3D Artificial Neural Network) и родилась идея упаковывать в плотные кубики десятки VASP-процессоров Aspex, имеющих вполне подходящие для 3DANN характеристики. Расчеты показывали, что есть шанс создать терафлопсный суперкомпьютер размером примерно с обычную рабочую станцию. Заказчик на подобный проект нашелся быстро, и в июле 1996 г. одним из специализированных изданий (Electronic News) было дано краткое сообщение, что между корпорацией Irvine Sensors и НИИ Военно-морских сил США (Office of Naval Research, ONR) заключен 18-месячный контракт на разработку «трехмерного (3D) VASP-пакета» на основе имеющихся в продаже процессорных чипов. Цель проекта – разработка массивно-параллельного процессорного модуля, позволяющего достигать гигантской, триллионы операций в секунду производительности, находясь в пределах стоимости и физических ограничений коммерческих рабочих станций. Стоимость контракта между Irvine Sensors и ONR, заметим, составляла смехотворные 750 тысяч долларов [LG96].

Проект был сугубо военный, больше о нем никто не сообщил. Но, судя по всему, процесс разработки прошел вполне успешно, поскольку весной 1998 года в неофициальном, но весьма авторитетном и широко цитируемом «Списке наиболее мощных компьютерных центров мира» (так называемый список Гюнтера Арендта) солидное третье место занял НИИ ВМС США в г. Арлингтоне, штат Вирджиния, с двумя своими машинами Irvine 3D VASP суммарной производительностью 2 терафлопса [GA98].

Со стороны было весьма странно наблюдать, как о столь выдающемся технологическом достижении не сообщило тогда ни одно компьютерное издание мира – ведь суперкомпьютеры терафлопсной производительности в те времена только-только начали появляться и занимали (да и сейчас занимают) залы размером примерно с баскетбольную площадку. А тут рабочая станция… Но самое удивительное началось впоследствии.

Чудеса дематериализации

Очень скоро, в конце 1998 года, и без каких-либо широковещательных деклараций, линию производства процессорных модулей 3D VASP у компании Irvine Sensors выкупил близкий партнер и богатый инвестор, корпорация ШМ. Пресс-релиз об этом событии повисел на сайте Irvine Sensors всего несколько месяцев, после чего пропал. Примерно тогда же, в начале 1999 года, необычные терафлопсные суперкомпьютеры Irvine 3D VASP (а также и сам Office of Naval Research) напрочь исчезли из списка Гюнтера Арендта.

Вскоре на сайте Irvine Sensors не осталось вообще никакой информации о совсем недавнем столь многообещающем проекте по пакетированию процессоров VASP. А в ноябре 1999 года произошла поразительная метаморфоза с Aspex Microsystems: «рождение» под новым именем Aspex Technology, «новые-старые» фамилии основателей без отца архитектуры VASP Майка Ли (он оставил пост исполнительного директора фирмы и целиком обратился к преподаванию в университете Brunei), изъятие в документах и на сайте самого термина VASP с заменой его на новые слова, обозначающие то же самое по сути, – «архитектура ASProCore» и «первый чип компании» Linedancer.

Короче говоря, в результате этих решительных и явно согласованных усилий было сделано так, что никаких следов-документов о революционной совместной разработке Irvine Sensors и Aspex в Интернете практически не осталось. В отдельных местах, правда, сохранились еще кое-какие старые документы, упоминающие большие планы военных на использование высокопроизводительных 3О-стек-чипов Irvine Sensors в инфракрасных датчиках и системах наведения-опознания противоракетной обороны [MP97][MDOO]. Но без какого-либо упоминания VASP (это слово применительно к процессорам вычищено почти тотально). Кроме того, на сайте НАСА даже в обычной заметке о передовой технологии 3DANN на всякий случай изъято название ее разработчика и не помещен, как положено в галерее иллюстраций, снимок высокого разрешения [TA01].

Генетическая идентификация

Скорее всего, теперь уже и не узнать, что посулил Пентагон (или кто-то еще?) за «аборт и молчание» небогатым родителям – сравнительно небольшой корпорации Irvine Sensors и совсем маленькой (25 человек) фирмочке Aspex. Но вполне очевидно, что радужные надежды этих фирм на близкую славу и успех без их чудо-ребенка – Irvine 3D VASP – так и не оправдались.

Зато корпорация ШМ вскоре после покупки у Irvine линии 3D VASP (и всего через пару-тройку недель после «перерождения» Aspex), в начале декабря 1999 года объявила о запуске весьма амбициозного 100-миллионного проекта Blue Gene – за пять лет, к 2004 году построить петафлопсный (1015 операций в секунду) суперкомпьютер для моделирования процессов сворачивания белка. Согласно закону Мура столь выдающийся вычислительный рубеж обычные кремниевые процессоры смогут достичь лишь где-то к середине второго десятилетия века, и для столь ощутимого обгона традиционных темпов роста требовалось предложить какую-то новую, революционную архитектуру. Однако в ШМ элегантно ушли от разъяснений особенности чудо-процессоров, положенных в основу Blue Gene, скромно отметив лишь, что в новой архитектуре «нет ничего экзотического – она целиком опирается на старую добрую технологию кремниевых чипов, которая просто примерно на поколение опережает нынешние процессы массового производства»…

О специфических особенностях нового производственного процесса можно было судить только по косвенным данным. Известно, например, что в рамках проекта Blue Gene неким хитрым образом в одну микросхему плотно упаковывается 32 гигафлопсных процессора вместе с DRAM-памятью (объявленный в 2000-м году чип Linedancer-4096, кстати говоря, имеет производительность 1 гигафлопс), а 64 таких чипа помещаются на единую системную плату размером 60х60 см. Несложные подсчеты показывают, что лишь 1 такая плата должна обладать производительностью в 2 терафлопса. Чем-то знакомым веет от всех этих цифр…

Как известно, во всех пресс-релизах ШМ, посвященных проекту Blue Gene [BG99], ни словом не упоминаются ни Irvine Sensors, ни Aspex

Technology. Ничем закончились и мои собственные, предпринятые года два назад, попытки связаться с разработчиками ШМ и непосредственно у них, по-простому, уточнить особенности происхождения терафлопсных системных плат. Неведомо откуда всплывшего русского журналиста с настырными вопросами элементарно проигнорировали.

Но время идет, в ШМ продолжают темнить, и к осени 2003 года, по прошествии четырех (из отведенных пяти) лет уже стало ясно – что-то в проекте Blue Gene пошло сильно не так. В мае 2003 года было признано, что выделенные изначально 100 миллионов долларов уже полностью израсходованы, давно запущен и движется к финишу альтернативный 200-терафлопсный проект Blue Gene/L на базе традиционных процессоров IBM PowerPC, а вот чудо-чипов для петафлопсного компьютера в наличии как не было, так и не появилось [ST03]. Спустя еще несколько месяцев, в июле, директор IBM Deep Computing Institute сообщил, что чипы для петафлопсной машины «вот-вот» появятся [BI03]. Выпуска пресс-релиза по этому поводу, правда, не замечено. Зато зафиксировано интересное совпадение. Почти одновременно с обещанием ШМ (несколькими неделями позже) компания Aspex Technology, никогда не имевшая собственных производственных мощностей, объявила, что получила заказы на Linedancer и лицензировала свою фирменную технологию массивно-параллельных процессоров некоему неназванному «изготовителю чипов». Нынешний исполнительный директор Aspex Пол Гринфилд довольно туманно поведал, что процессоры Linedancer будет теперь изготовлять их «большой брат», получивший к тому же OEM-лицензию на перепродажу чипов под своим собственным именем. В обмен Aspex получает доступ к производственным линиям «брата» и к его интеллектуальной собственности. Имя же своего таинственного благодетеля компания пообещала назвать, как она надеется, месяца через два, т.е., надо понимать, в октябре текущего года [EW03].

Ничего не сказала рыбка...

Позволит загадочный «брат» раскрыть свое имя или нет – пока неясно. Не исключено, что завеса тайн так и будет окружать всю эту историю. А потому при подготовке данного материала я решил связаться непосредственно с профессором Майком Ли, благо он, с одной стороны, вроде как давно уже не при деле, а с другой стороны просто не может не знать, что там происходило на самом деле вокруг Irvine 3D VASP и Blue Gene.

К моему, честно говоря, удивлению господин Ли ответил на первый же краткий запрос практически моментально – в тот же день. Ответ его, правда, оказался весьма скупым на подробности и практически неинформативным (по сути дела, он лишь вежливо поинтересовался, что мне вообще известно о Irvine 3D VASP). Относительно же моих предположений о прозрачной связи между сворачиванием совместного терафлопсного проекта Irvine Sensors/Aspex Microsystems и последующим запуском программы Blue Gene, профессор Ли выразился так: «Ваши построения выглядят интригующе, но, вероятно, они безосновательны».

Тогда мне пришлось «обосновать»: развернуть аргументацию и

подробно рассказать то, что известно – и о тотальном молчании прессы про Irvine 3D VASP, и об изъятии в Интернете всех страниц с информацией о пакетировании процессоров Aspex, и вообще об отсутствии содержательных упоминаний о технологии VASP (даже на сайте университета Brunei, где она рождалась). Ну и о весьма похожих характеристиках аппаратной части Blue Gene, естественно.

Ничего не ответил на это профессор. Да и что тут может ответить порядочный человек, желающий оставаться честным, если на правду – словно на постыдную историю – почему-то наложен запрет.

Глава 4. Важнейшее из искусств

Страницы жизни героя, 1935. Ревность и ложь

Начало 1930-х годов в Америке – это полный упадок экономики, бездеятельность коррумпированных властей и мощный расцвет криминальных империй, чувствующих свою безнаказанность. Как естественное следствие – общий «кризис ценностей» в обществе. Газеты, журналы и фильмы переполнены историями о героях-гангстерах и об их громких преступлениях – похищениях миллионеров с целью выкупа, грабежах банков средь бела дня и прочих дерзких налетах. Правоохранительные органы на этом фоне выглядят тупыми и неэффективными, так же как, впрочем, и все остальные правительственные структуры.

В 1933 году, пообещав американскому народу «новый курс», к президентской власти приходит Франклин Делано Рузвельт. Для ведомства Гувера (который в этот раз умудрился сохранить свой пост буквально чудом) новый курс означал прежде всего необходимость каких-то эффективных, ярких действий по обузданию преступности. И случилось так, что именно в это время в Бюро расследований находится весьма подходящий человек – глава чикагского отделения ФБР Мелвин Первис. Под руководством спецагента Первиса проводится целая серия успешных операций, в ходе которых были застрелены самые знаменитые в ту пору бандиты – Джон Диллинджер, «Красавчик» Флойд и «Мордашка» Нельсон.

Наряду с успешными рейдами Бюро против гангстеров, в средствах массовой информации Гувером разворачивается активнейшая пропаганда нового образа доблестных служителей закона. На радио создали серию радиопередач под общим названием «G-Men» («джи-мены», от Government Men, как начали называть федеральных агентов), содержание которых взялся контролировать лично Гувер. Правда, у директора ФБР не оказалось ни малейших драматургических талантов, и он все время норовил заменить драки – погони – перестрелки тонкой аналитической работой сыщиков и криминалистов. В результате радиосериал получился сухим и скучноватым, посему долго не протянул.

Чуть позже, в 1936 году была запущен комикс «Война преступности» и пара бульварных журнальчиков под названиями G-Men и The Feds («феды», так называли федеральных агентов гангстеры). Вся эта

незамысловатая печатная продукция предельно доступным для детей и простых людей способом всячески прославляла деятельность ФБР, а его шефа Эдгара Гувера изображала просто-таки национальным героем номер один.

Вообще-то поначалу главнейшим героем в глазах американской прессы был спецагент Мелвин Первис. Ведь именно он непосредственно возглавлял главные операции по захвату и уничтожению преступников. (В ходе этих рейдов Первис вопреки всем полицейским инструкциям неоднократно лично добивал раненых гангстеров.) Естественно, на первых порах столь энергичный и успешный в делах сотрудник был любимцем Гувера, остро нуждавшегося в эффектных результатах. Но по мере роста восторгов публики и обостренного внимания прессы к личности Первиса, уже успевшего заслужить в народе титул «ас джи-менов», шефа ФБР начала обуревать ревность. Гувер стал поручать Первису совершенно безнадежные дела, засовывать в нудные бюрократические комиссии, превращая некогда яркую службу в невыносимую своим занудством пытку.

Не желая сносить унижения, Мелвин Первис довольно скоро, летом 1935 года, уволился из ФБР. Однако ревнивый и злопамятный шеф приложил максимум усилий, чтобы и вне его ведомства бывший фаворит не нашел себе сколь-нибудь приличной работы. Преследования и тихая месть Гувера продолжались до конца жизни Первиса в 1960 году. Сначала шеф ФБР мощно надавил на Голливуд, заставив киношников отказаться от мысли взять Первиса консультантом по криминальным вопросам. Далее же делалось все, чтобы не подпускать Первиса к работе, хоть как-то связанной с деятельностью правоохранительных органов. В 1952 году Гувер помешал Первису стать федеральным судьей, а когда Первиса пригласили на работу в Сенат, директор ФБР приказал своим сотрудникам подготовить на него компромат.

Но все это будет много лет спустя, а в 1935 году, убрав на пути к славе досадное препятствие в виде этого «аса джи-менов», Гувер еще активнее занялся рекламой собственной персоны и возглавляемого им ведомства. Особая роль здесь отводилась кинематографу, поскольку Голливуд и сам был готов оперативно реагировать на перемены. В 1935 году было начато производство целой серии кинофильмов под общим названием «Джи-мен». Отважный и бескомпромиссный облик борцов с преступностью из ФБР стал особо удаваться еще и потому, что новые американские законы о цензуре теперь дозволяли изображение гангстеров на экране лишь в тех случаях, когда их в конечном счете либо арестовывают, либо убивают федеральные агенты.

Поворотной точкой в развитии жанра гангстерских фильмов историки кино чаще всего называют картину «G-Men» режиссера Уильяма Кейли. Фильм был, в общем-то, рядовой по всем художественным параметрам, но вплоть до этой ленты в подавляющем большинстве такого рода картин главными героями были сами гангстеры. В этом же фильме, напротив, настоящими героями становятся федеральные агенты, преследующие бандитов. Причем главную роль – опытного адвоката, поступившего в ФБР, чтобы отомстить преступникам за смерть друга-агента – исполняет кинозвезда тех лет Джимми Катни, прославившийся именно в ролях благородных и неуловимых гангстеров.

Влияние средств массовой информации и особенно кино на оценку обществом Гувера и его ведомства было огромным. К 1937 году миллионы американцев посмотрели уже несколько фильмов о бравых агентах ФБР и прочитали десятки книг на ту же тему. Дети стали носить игрушечные значки агентов Бюро, играть такими же, как у настоящих федеральных агентов, игрушечными пистолетами, и даже спать в пижамках с фирменной эмблемой «G-Men».

Дж. Эдгар Гувер и ФБР вступили в совершенно новую фазу своей истории – эру славы. Публика увидела в Бюро некую самостоятельную, очень важную для общества структуру, а не просто часть министерства юстиции. Многие университеты и общественные организации начали осыпать шефа ФБР наградами. Альма-матер Гувера, университет Джорджа Вашингтона присвоил ему степень почетного доктора права.

Этому же примеру вскоре последовал университет города Нью-Йорка. Сам же Гувер совершенно серьезно стал рассматривать себя главным стражем законов страны, ее граждан и моральных устоев.

При этом шефу ФБР не только очень нравилось купаться в лучах собственной славы, но и при всякой возможности он старался приписать себе также заслуги, принадлежавшие другим. Так, еще в 1932 году, когда случилась громкая трагическая история с похищением и убийством бандитами ребенка знаменитого летчика, пионера авиации Чарльза Линдберга, Гувер пытался, правда совершенно безуспешно, сыграть ведущую роль в поимке похитителей. Когда же организатор похищения Бруно Гауптман был все-таки вычислен и задержан полицией города Нью-Йорк, туда немедленно поспешил и Гувер, чтобы на месте сообщить прессе и публике об аресте преступника. Такие маневры должны были формировать у общественности мнение, что федеральные органы правопорядка и лично великий сыщик Эдгар Гувер оказались, как и положено, на высоте. Хотя конкретно в данном случае Бюро не сделало фактически ничего для отлова бандита.

После устранения с первых планов Мелвина Первиса, дабы укрепить в глазах публики собственный героический облик проницательного детектива и отважного человека дела, Гувер решает принимать личное участие в захвате важных преступников. В 1936 году в списке «врагов общества» под номером один проходил некто Элвин Карпис, последний из главарей знаменитой банды «мамаши» Баркер. Когда полиция выявила в Новом Орлеане апартаменты, где скрывался Карпис, туда срочно вылетели Гувер и Толсон. И как только федеральные агенты Херт и Брэнтли повязали гангстера, на сцене тут же возник лично директор Гувер, объявивший преступнику, что он арестован. Видеть на первых страницах газет свою фотографию в обрамлении заголовков-славословий, набранных жирным шрифтом, было так приятно, что уже на следующей неделе Гувер отправляется в другой конец страны, в штат Огайо, где в г. Толедо лично возглавляет захват Гарри Кэмпбелла, еще одного гангстера из той же банды Баркер.

В череде подобных историй были и такие, что отличались не только откровенным лицемерием, но и выдающимся вероломством. В 1937 году при весьма темных обстоятельствах Гувер арестовал гангстера Луи «Лепке» Бухалтера, возглавлявшего организацию наемных киллеров –

знаменитую «Корпорацию Убийство» (Murder, Incorporated). Известно, что арест прошел без стрельбы и, по слухам, федеральным властям сдали Лепке сами мафиози, надеявшиеся таким образом ослабить давление со стороны ФБР. (Похоже, именно тогда между Гувером и высшими боссами мафии начинали формироваться деловые отношения, которые длились не только до смерти первого директора ФБР, но и, как будет видно дальше, много лет спустя.) Как бы там ни было, но переговоры о сдаче Лепке велись через посредника – приятеля Гувера журналиста Уолтера Уинчела, хотя гангстер был уверен, что получает гарантии лично от шефа ФБР. В итоге Бухалтер сдался Гуверу в обмен на обещание 10-летнего тюремного заключения. Когда же дело подошло к суду, то никаких гарантий Гувера в деле не фигурировало, нью-йоркские власти приговорили гангстера за убийства к смертной казни и действительно посадили его на электрический стул.

Для постоянной пропагандистской поддержки работы ФБР, прославления всяческих успехов Бюро и лично Эдгара Гувера, в структуре организации было создано специальное 8-е управление, формально именовавшееся «управлением учета и архивов». Возглавил это подразделение Луи Николс, еще один выпускник юридического факультета университета Джорджа Вашингтона и ближайший сподвижник Гувера. После второй мировой войны именно Николсом был организован коллектив авторов, написавших развернутый панегирик под названием «История ФБР». Книга вышла из печати в 1956 году, чуть позже на ее основе вышел и голливудский фильм под тем же названием, причем съемки картины проходили под личным контролем Эдгара Гувера. Интересно (хотя и неудивительно), что ни в книге, ни в фильме, претендовавших на правдивое изложение событий, вообще нет персонажа по имени Мелвин Первис.

Зависть и ревность шефа ФБР простирались столь далеко, что и спустя много лет после смерти Первиса он всячески пытался принизить даже самые очевидные заслуги некогда самого блестящего из спецагентов Бюро. В воспоминаниях Аниты Колби, известной в американских светских кругах дамы, приводится эпизод о том, как Эдгар Гувер под конец своей жизни интерпретировал историю с Джоном Диллинджером – одно из самых громких дел Первиса. Теперь выходило, что на Диллинджера вышел вовсе даже и не Первис, а Клайд Толсон. Просто, мол, так уж ими было решено – подарить всю славу Первису, но в действительности все сделал Клайд.

Подобное заявление – лишь один из рядовых примеров редкостной лживости и лицемерия Гувера. Даже если не брать в учет то, что Клайд Толсон оперативной работой в Бюро практически не занимался (значительно больше интересуясь кадровыми вопросами), историками по документальным материалам из архивов ФБР установлено, что в день смерти Диллинджера сердечный друг Гувера находился в штаб-квартире ФБР, т.е. весьма далеко от Чикаго.

Имеется, кстати, весьма характерное высказывание Эдгара Гувера по поводу правдивости и лживости, сделанное им в одной из своих многочисленных нравоучительных лекций. В статье для семейного журнала Family Weekly, озаглавленной «Что я рассказал бы сыну», Гувер изрекает следующее: «Прежде всего, я научил бы его говорить правду… Я пришел к

выводу, что говорить правду – это определяющий фактор ответственного гражданина. Те тысячи преступников, которых я повидал за 40 лет работы в правоохранительных органах, все имели одну общую черту – каждый из них был лжецом»… [EH63].

Reality Show : Спасая рядового Джессику Линч

Горячая новость

Раннее утро 2 апреля 2003 года. В Дохе, столице арабского эмирата Катар, где разместилось центральное командование военной операции в Ираке, поднялся сильнейший переполох. Всех журналистов, освещающих ход боевых действий, словно по тревоге подняли с кроватей для срочной пресс-конференции в CentCom, военном и информационном центре операции. Целую ночь не смыкавший глаз Джим Уилкинсон, главный здесь представитель Белого дома, многозначительно известил репортеров, что имеется очень «горячая новость, о которой уже извещены президент США и министр обороны».

Журналисты поспешили в Центр, полагая, что не иначе как удалось изловить самого Саддама Хусейна. Однако в действительности история оказалась намного круче, поскольку положила начало спектаклю, который уже успел войти в историю как один из наиболее выдающихся образцов пропагандистской лжи и фабрикации желательных для власти событий в реальном масштабе времени. Центральной фигурой этого шоу стала, сама того не желая, совсем молоденькая субтильная девушка по имени Джессика Линч – рядовой 507-й группы материально-технического снабжения Армии США. Она находилась в составе автоколонны, доставлявшей через иракскую пустыню провиант бойцам на передовой. Но при подходе к г.Насирия командир колонны неверно сориентировался на местности, машины свернули не туда и вышли прямиком на линию обороны иракских сил, где попали под обстрел. Девять сослуживцев Линч погибли, а сама она была тяжело ранена и попала в плен. Иракские солдаты отвезли ее в местную больницу, служившую опорным пунктом федайхинов, где девушка провела 8 дней.

В ночь с 1 на 2 апреля, сразу после полуночи, группа американского спецназа высадилась с вертолетов на вражеской территории и взяла штурмом больницу Насирии. Эту отважную атаку снимали несколько военных телекамер с техникой ночного видения – как на земле, так и с воздуха, с помощью беспилотного самолета-разведчика Predator. После непродолжительной стрельбы снаружи здания рейнджеры ворвались в больницу, отыскали там Линч, отнесли ее к вертолету и вернулись на базу. Комментируя продемонстрированный журналистам в Дохе видеоролик, смонтированный буквально сразу по окончании операции освобождения, американский бригадный генерал Винсент Брукс так резюмировал его содержание: «Чтобы это случилось, несколько храбрецов ставят на кон свои жизни, свято веруя, что никогда не оставят товарища, попавшего в беду».

Передавая службам теленовостей пятиминутный видеофильм обо всей

этой истории, представители Пентагона сообщили, что у освобожденной Линч были колотые и пулевые ранения, а на больничной койке ее били и допрашивали. Спасли же несчастную девушку лишь благодаря мужественному иракскому адвокату по имени Мохаммед Одех аль Рехайеф, который с риском для жизни выбрался из города и известил американцев о том месте, где содержат Линч [TG03].

Она сражалась до последнего

Еще через сутки, 3 апреля центральная американская газета Washington Post публикует вдохновенно-патриотическую статью под названием «Она сражалась до последнего. Подробности о пленении и освобождении солдата из Западной Вирджинии». В этой статье сотрудники редакции WP, получив дополнительную информацию от неназванных официальных источников в госадминистрации США, уже в красках расписали подвиг хрупкой девочки из городка Палестина. О том, как Джессика Линч, в составе группы попавшая во вражескую засаду, яростно отстреливалась и прикончила несколько иракских солдат. И даже сама получив несколько пулевых ранений, она не прекращала сопротивления до тех пор, пока у нее не кончились все патроны. «Она сражалась до смерти», – цитирует газета слова осведомленного источника, – «она не хотела сдаваться живьем». Когда же иракцы смогли к ней приблизиться, добавил тот же источник, девушка получила еще и несколько колотых ранений холодным оружием [SL03].

В каких именно официальных инстанциях журналисты Washington Post получили всю эту информацию, так и осталось загадкой (представители Пентагона были намного более сдержаны и лишь сообщили, что осведомлены о «слухах» про героизм Линч, но подтвердить их не могут). Самим военным было вполне достаточно, что команда спецназа провела фактически образцово-показательный рейд в тыл противника, к тому же задокументированный в видеоматериалах: стремительная атака и решительная высадка с вертолетов Black Hawk, краткая перестрелка, спасение товарища по оружию и ни одного потерянного в бою человека. Восхитительная же история из центральной газеты многократно была воспроизведена во множестве других американских изданий, и, в сочетании с коротким видеороликом об операции освобождения в ТВ-новостях, произвела именно тот эффект, который и ожидался. На фоне затянувшихся боевых действий в Ираке, роста боевых потерь и жертв среди мирного населения, не говоря уже о полном отсутствии обещанных счастливых иракцев, в восторге встречающих освободителей, подобный сюжет реально повлиял на подъем угасавшего энтузиазма американской публики.

В подаче всей этой истории с самого начала чувствовалась какая-то постановочность, искусственная «киношность». И уже первичные, самые поверхностные раскопки независимых журналистов показали, что подобное ощущение возникало вовсе не на пустом месте. Новый подход Пентагона к подаче информации – сконцентрировать внимание на визуальном ряде и сопровождающем его «общем послании», не вдаваясь в излишние подробности, – в значительной степени построен на том, кто

именно снимает и редактирует видеоматериал. Поэтому все чаще военные используют своих собственных телеоператоров и монтажеров, передавая ТВ-сетям уже подготовленные к показу ролики. В значительной степени это было сделано под влиянием голливудских продюсеров, занимающихся постановкой реальных ТВ-шоу и художественных экшн-фильмов.

В частности, еще в 2001 году с подобной идеей в Пентагон пришел Джерри Брукхаймер, продюсер знаменитых блокбастеров героико-патриотической тематики «Высадка Черного ястреба» (Black Hawk Down), «Перл Харбор» и «Армагеддон». Для начала Брукхаймер предложил сделать документальный телесериал «Портреты с передовой» об американских солдатах, сражающихся в терроризмом в Афганистане. Идея «реального» ТВ-сериала получила одобрение и активную поддержку министра обороны Дональда Рамсфелда, фильмы с успехом прошли в эфирный прайм-тайм как раз накануне иракской войны, и Пентагону весьма понравилось, как это все было показано. Такой же подход было решено применить и в репортажах о боевых действиях в Ираке [JK03].

Не исключено, что на рождение героического сюжета «спасая рядового Линч» повлияло и еще одно обстоятельство. Для правильного освещения новой жизни в Ираке американское правительство решило создать новую национальную медиа-сеть Iraqi Media Network (IMN). Контракт на разворачивание в Ираке IMN получила американская корпорация SAIC, имеющая обширные деловые связи с Пентагоном и разведслужбами США, а также с их психологическими и специальными операциями. В частности, вице-президентом SAIC, ведающим «критичными вопросами национальной безопасности», является Уильям Гаррисон, прежде занимавший руководящий пост в американском спецназе (U.S. Army Special Forces), где – какое удивительное совпадение – именно он возглавлял в 1993 году ту самую операцию с вертолетной высадкой в Сомали, что затем легла в основу фильма Брукхаймера Black Hawk Down (режиссер Ридли Скотт) [ЮОЗ][РКОЗ].

Как это было

Но жизнь реальная – это все же не кино, и от служб новостей люди обычно ожидают несколько более правдивого изложения событий, нежели от голливудских боевиков, пусть и построенных на живом материале. Факты, свидетельствующие о том, что в истории про Джессику Линч концы не сходятся с концами и вообще много сомнительного, внимательные наблюдатели заметили уже в самом начале. Так, в тот же день 3 апреля, сразу вслед за баснями «Вашингтон Пост», агентство Франс Пресс (AFP) передало из США в корне иную информацию, исходившую непосредственно от родителей девушки. В телевизионной пресс-конференции из родительского дома Джессики в г. Палестина, Зап. Вирджиния, ее отец Грегори Линч рассказал, что он и жена уже побеседовали с дочерью, срочно доставленной для хирургического лечения в военный госпиталь в Ландштуле, Германия. По результатам медосмотра у Джессики на теле не выявлено ни пулевых, ни ножевых, ни вообще каких-либо проникающих ранений. Эту же информацию чуть позже подтвердили и американские военные врачи, сообщившие, что у рядового

Линч выявлены множественные переломы и ушибы, но ни одно из повреждений не вызвано огнестрельным или холодным оружием [FP03].

Странно было и то, что вся информация о «геройствах под Насирией» исходила только из неназываемых конкретно государственных инстанций – очевидно, из разведслужб, поскольку базовым источником материалов для журналистов WP стали «разведданные с поля боя, перехват коммуникаций и другие иракские источники». В то же время официальные представители Пентагона весьма тщательно выбирали выражения и нигде ни словом не обмолвились о сути подвига Линч или о ее ранениях. Но при этом власти не предприняли абсолютно никаких усилий для коррекции истории, так что романтическая версия «Вашингтон пост» была подхвачена американской прессой и широко разнесена по стране, причем с добавлением новых возбуждающих подробностей о спасении героини. Как, скажем в газете Los Angeles Times: «А затем, под покровом тьмы армейские рейнджеры и морские пехотинцы… пробили себе путь в здание под ураганным огнем противника»… Далее в том же духе [LG03], [WM03].

Лишь спустя две недели другой репортер WP, Кит Ричберг, находившийся непосредственно в Ираке, впервые для большой прессы США подверг сомнению не только версию своих коллег в Вашингтоне, но и версию Пентагона о блестящей операции спасения. Медперсонал той самой больницы Насирии поведал журналисту совершенно иную историю о происходившем. Иракские доктора сообщили, что спецназу США здесь не оказывали, да и не могли оказать абсолютно никакого сопротивления, поскольку в районе больницы уже не было никаких иракских солдат или вооруженных боевиков, которые к тому времени покинули город. Что же касается Джессики Линч, то бедную девушку доставили в больницу действительно в плохом состоянии – с переломами обеих ног, руки, других костей и ушибом головы. Но ни капли крови, следов пуль или осколков. Все травмы были результатом серьезного дорожно-транспортного происшествия… Впрочем, этот неудобный материал Ричберга был опубликован глубоко внутри газеты, а не на первой полосе, так что никакого резонанса он не получил [KR03].

Последующие раскопки правды вели, главным образом, иностранные журналисты непосредственно в Ираке. В первых числах мая корреспондент канадской газеты Toronto Star написал о том, что рассказали ему «три иракских доктора, две медсестры, один сотрудник больничной администрации и несколько местных жителей». Весьма интересную деталь добавил официант ресторанчика «аль-Диван», дом которого расположен рядом с больницей. Выяснилось, что непосредственно накануне высадки вертолетного десанта на месте сначала побывала разведывательная группа американского спецназа в сопровождении араба-переводчика из Катара. У этого официанта они выясняли, много ли осталось в больнице военных, на что тот им ответил «никого не осталось, они все уже ушли». Вскрылись и другие любопытные подробности. Один из докторов рассказал, как за два дня до операции рейнджеров сотрудники больницы пытались сами вернуть Джессику Линч американцам. Девушку погрузили в машину скорой помощи, а водителю дали инструкции довезти ее до блок-поста войск коалиции. Однако, когда машина приблизилась к блокпосту примерно метров на 300, американские военные открыли предупредительный огонь,

заставив машину вернуться в город.

Затем появилось еще несколько публикацией с аналогичными результатами расследований журналистов в европейской прессе. Общий же итог всей этой истории, можно считать, подвел документальный фильм английской съемочной группы, показанный по второму каналу BBC 19 мая 2003 года. Иракские врачи рассказали журналистам о том, как они лечили несчастную девушку от множественных переломов, выделив ей единственную в больницу специальную ортопедическую кровать. О том, что через три дня после десанта в больницу специально заезжал пожилой американский военврач, чтобы поблагодарить местный персонал за отлично сделанную операцию и квалифицированную помощь солдату США. И, конечно, о недоумении врачей, зачем нужен был весь этот цирк с шумным штурмом больницы – 12 выбитых дверей, ослепляющие световые гранаты, куча солдат с лазерными прицелами и криками «go, go, go» носящихся по зданию, разломанная спецкровать, на которой лежала Джессика Линч. Всю сцену освобождения снимали находившиеся в группе захвата два оператора с видеокамерами и один фотограф. У сотрудников больницы, хоть и натерпевшихся страху, было такое впечатление, словно идут съемки голливудского боевика с Сильвестром Сталлоне или Джеки Чаном – ведь в здании не было ни одного вооруженного иракца…

Еще несколько месяцев спустя, 17 июля 2003 года, американское военное командование опубликовало официальные результаты расследования того, что же в действительности произошло с автоколонной Джессики Линч в иракской пустыне. На 15 страницах подробного отчета в деталях воспроизводится история о том, сколь грустным, жестоким и бездарным занятием является война. О том, что после 60 часов марша в песках пустыни 5-тонный грузовик, которым должна была управлять Джессика Линч, уже был неисправен, и в автоколонне его тащил на буксире 10-тонный тягач. О том, что даже со сверхсовременной техникой навигации и карманными GPS-приемниками на дороге в пустыне очень легко заблудиться, особенно когда из-за барханов в тебя стреляет невидимый противник. О том, что при попытке развернуться на узкой дороге тяжелые машины тут же безнадежно увязли в мягком песке, перегородив к тому же остальным дорогу к отступлению. Под нараставшим огнем противника выяснилось, что почти все оружие американских солдат из группы техснабжения стрелять не способно – его тут же заклинило, скорее всего из-за песка и неверного ухода. Джессику и еще нескольких солдат в застрявших грузовиках подобрал более легкий джип Hummer. На повышенной скорости машина стала уходить из зоны обстрела, но после одного из попаданий потеряла управление и врезалась в стоявший на дороге тягач. На этом сильнейшем ударе, собственно, война Джессики Линч закончилась, поскольку при столкновении ей переломало кости ног, рук, лопатку и ребра. В столь ужасном состоянии девушка попала в плен – ее подобрали иракские солдаты и отвезли в госпиталь [SR03].

В заключении армейского отчета подведен итог этой грустной истории, ни в каком ракурсе не тянущей на героическую. Из 33 солдат в 18 машинах хозяйственной автоколонны, попавшей 23 марта под обстрел у города Насирия, 11 человек погибли, 7 попали в плен (шестерых нашли и освободили позже), остальные смогли выбраться из-под огня и вернуться к

своим. Но особо следует выделить самую последнюю фразу отчета:***«Сражение за г. Насирия длилось вплоть до 31 марта, когда Корпус морской пехоты в конечном счете взял город под контроль».***

А затем, как все помнят, в ночь с 1 на 2 апреля доблестный американский спецназ продемонстрировал миру реальное ТВ-шоу по захвату центральной больницы Насирии, где никого, кроме врачей и больных, не было. Министр обороны Дональд Рамсфелд в своих похвалах назвал операцию по освобождению Линч «блестящей и отважной» [RM03].

Мемуары из амнезии

Несмотря на доступность всех этих материалов в Интернете, основная часть американских средств массовой информации продолжает придерживаться начальной, романтическо-героической версии событий.

Самое главное в таких условиях – чтобы непосредственные участники событий не сболтнули ничего лишнего. Учтя самый первый прокол с «неуместной» пресс-конференцией отца Джессики Линч, с родней, близким и сослуживцами героини провели, похоже, надлежащую работу, так что больше никаких интервью, противоречащих генеральной линии, в прессе уже не появлялось.

Но самая трудная роль, конечно же, выпала на долю самой девушки. После перевода в американский военный госпиталь Джессику строжайшим кордоном охраны оградили от всех журналистов, а врачи поведали прессе, что у их подопечной наблюдается сильнейшая амнезия. После всего пережитого Линч, де, практически ничего не помнит из происходившего с ней в Ираке. Причем есть вероятность, что память об этом не вернется уже никогда… [FN03].

Далее последовала целая череда наград для новой национальной героини, всколыхнувшей в американском народе волну патриотизма, – «Бронзовая звезда за отвагу», медаль «Пурпурное сердце» за ранение в бою, медаль военнопленного. Компания NBC изготовила о подвиге Джессики Линч художественный телефильм в жанре «героический экшн». Ну и, наконец, солидный приз в денежном выражении – гонорар в 1 миллион долларов за книгу воспоминаний, которые подготовлены совместно с бывшим репортером газеты New York Times Риком Брэггом. То, что идея амнезии и мемуары как-то неважно друг с другом стыкуются, никого в данной ситуации особо уже не волнует. Известны состыковки и покруче.

Подмена реальности

Не верь глазам своим

Зимой 2000 г., вскоре после грандиозных новогодних празднеств по поводу вступления человечества в новый миллениум, в американских средствах массовой информации произошла небольшая, но по-своему знаменательная потасовка. Одна гигантская компания, CBS, вполне

умышленно прищемила другую гигантскую компанию, NBC. Конкуренция есть конкуренция, и подобных историй, в общем-то, случается на рынке по дюжине в день, но у этой имеется один весьма примечательный аспект. Суть его такова, что телекомпании новостей уже на регулярной основе используют компьютерные технологии цифровой обработки изображений, чтобы в реальном масштабе времени «корректировать» видеоряд, подаваемый под видом живой, якобы, трансляции. Причем делается это безо всякого уведомления зрителей [ВНОО].

Конкретно в данной ситуации произошло следующее. Во время трансляции массовых гуляний в новогоднюю ночь на нью-йоркской Таймс-сквер компания CBS News тщательно вычищала с экрана светящиеся рекламные щиты конкурирующей фирмы NBC, подменяя их собственной рекламой. В NBC эти манипуляции, естественно, заметили и подняли шум в прессе. Тут же выяснилось, что CBS News занимается этим регулярно и по меньшей мере несколько месяцев, с тех пор, как 1 ноября 1999 г. в студии было установлено новое компьютерное оборудование. Вообще-то цифровое редактирование видеоизображений применяется практически всеми телекомпаниями, особенно в отношении рекламных щитов на спортивных состязаниях, но еще никто столь откровенно не использовал заманчивую технологию в теленовостях [В США среди разработчиков систем виртуальной вставки рекламы в ТВ-передачи наиболее популярны фирмы PVI (www.pvi-inc.com) и Sportvision.].

Припомнили, правда, случай 1994 года, когда тележурналистка ABC Коки Роберте, не покидая студию, вела якобы репортаж с Капитолийского холма, накинув плащик и поместив на заднем фоне картинку здания парламента. Но в тот раз и журналист, и продюсер передачи получили нагоняй за злоупотребление технологиями, а компания публично извинилась за умышленное введение общественности в заблуждение. Теперь же обсуждение истории с CBS News свелось к нудноватой дискуссии об «этичности или неэтичности» ситуации, когда одна богатая компания не желает задаром рекламировать другую богатую компанию, применяя для этого новейшие цифровые технологии. Но попутно многие задались и более животрепещущим вопросом: куда же вообще может завести общество подобный подход к подаче новостей? Тем более, что рекламные трюки CBS News по небольшому «исправлению» реальности – это ведь так, детские шалости. Технологии, лежащие в основе манипуляций видеоизображением, позволяют организовывать и куда более серьезные трюки.

Глаз Тигра

Весной и летом 1999 г. команда инженеров американской корпорации Sarnoff (Принстон, шт. Нью-Джерси) интенсивно работала в итальянском городе Виченца, где на военной базе был развернут Оперативный центр союзных сил НАТО, ведущих боевые действия в Югославии. Работа инженеров была сосредоточена на трансформации их экспериментальной компьютерной технологии в эффективный военный инструмент для быстрого обнаружения и позиционирования сербской военной техники в Косово. Проект получил название TIGER– как звучное сокращение от

несколько кучерявого словосочетания «targeting by image georegistration», т.е. «целеуказание по георегистрации изображений» [IAOO].

Задача системы TIGER – быстро обрабатывать живую видеосъемку, осуществляемую камерой беспилотного самолета-разведчика Predator, который парил над зоной боевых действий в Косово на высоте примерно 500 м. Суть обработки в общем-то похожа на трюк с подменой рекламы, но здесь объекты реальной боевой обстановки накладывались на цифровые карты местности, заблаговременно созданные с помощью средств воздушной и космической видовой разведки. Система TIGER автоматически выявляла движущиеся цели и практически мгновенно (за 1/30 секунды) передавала операторам-наводчикам точные географические координаты сербской техники, попавшей в поле зрения «Предатора». В принципе, вычисленные координаты можно было бы сразу автоматически вводить в систему наведения высокоточного ракетного оружия, однако, учитывая экспериментальный характер системы, окончательное решение перед ударом здесь всегда принимал оператор-человек. По свидетельству DARPA, агентства передовых военных исследований США, технология TIGER весьма активно использовалась последние три недели военных операций в Косово, когда были поражены от 80 до 90 процентов подвижных целей.

Люди, хорошо знакомые с возможностями современных технологий захвата цели и манипуляций видеоизображением, прекрасно осознают, что «живая» телевизионная трансляция ныне может становиться сколь угодно далекой от реально происходящих событий. Как говорит Норман Винарски, вице-президент по инфотехнологиям в корпорации Sarnoff, «видеть – это больше не означает верить, сейчас вы уже не можете знать, чему доверять».

Демонстрация подобных технологических чудес пока что способна производить на публику весьма сильное впечатление. В 1999 году на геополитической конференции о плюсах и минусах спутниковой видовой разведки интересно выступил профессор-политолог Стивен Ливингстон из Университета Джорджа Вашингтона. Для максимальной наглядности в подтверждение все того же тезиса «видеть – это не значит верить», он просто продемонстрировал аудитории видеоролик – выступление на льду знаменитой фигуристки Катарины Витт. Спортсменка изящно скользила по льду и вдруг в прыжке полностью исчезла с экрана. Камера все так же продолжала скользить по пустой площадке, ее бортам и трибунам со зрителями, пока столь же волшебным образом Витт опять не появилась на экране через десяток секунд. Конечно, в кино подобные спецэффекты применяются десятилетиями, но теперь то же самое без труда можно делать и с телетрансляцией в реальном масштабе времени.

Новая эра в информационных операциях

Понятно, что секретные спецслужбы проигнорировать подобные захватывающие возможности никак не могли.

В мае 1998 года в г. Арлингтон проходила конференция военной разведки США, как обычно секретная. Однако, на открытой части мероприятия в тот раз удалось побывать репортеру еженедельника Federal Computer Week. Он-то и рассказал о весьма впечатляющей презентации, с

которой здесь выступил уже знакомый нам по первой главе д-р Джон Юречко, начальник «отдела поддержки информационной войны» Разведуправления МО США (РУМО). Суть доклада Юречко, если пользоваться его собственным речевыми оборотами, сводилась к тому, что «разведывательное сообщество США плодотворно комбинирует компьютеры с теориями когнитивной психологии, а использование информационных технологий возвещает для них новую эру в информационных операциях» [DV98].

По свидетельству этого эксперта, разведслужбы тщательно изучают способы использования компьютеров и глобальную сеть Интернет с целью формирования и распространения информации, предназначенной для склонения в нужную сторону общественного мнения по наиболее горячим политическим вопросам. В качестве составной части своей так называемой программы «управления восприятием» (perception management) разведывательное сообщество в течение десятилетий формирует дезинформацию для стимулирования политических изменений без прямого политического или военного вмешательства в тех странах, где США имеют значительные интересы, таких как Ирак или Северная Корея.

Опираясь на современные достижения в области информационных технологий, разведслужбы обращаются к ПК для разработки более сложных средств по манипуляции и распространению цифровых фотографий, видеоклипов и звукозаписей для распространения через Интернет документов о непроисходивших событиях в надежде спровоцировать желательные реакции. Юречко рассказал, к примеру, что разведывательные службы могут пытаться убедить лидера какой-нибудь страны в надвигающемся массированном вторжении, распространяя клипы видеоновостей, изображающие разворачивание больших военных сил, намного превосходящих реально существующие.

Для более наглядной демонстрации своих слов, Юречко продемонстрировал аудитории советскую фотографию 1938 года, на которой изображен Иосиф Сталин в компании Николая Ежова, тогдашнего главы госбезопасности СССР. На другой версии того же снимка Ежов «техническими средствами ретуши» удален с фотографии без каких-либо следов его присутствия. В эпоху кровавых репрессий, как многие помнят, эта процедура входила в стандартный набор советских средств для постоянного внесения коррективов в историю государства. Как выразился Юречко, на сегодняшний день точно такой же процесс «распыления» РУМО может применяться к видеозаписям.

Столь циничные параллели с тоталитарным режимом Сталина показались, вероятно, кому-то в американском руководстве чересчур откровенными. И, невзирая на иронию происходящего, технологию «распыления» применили к откровениям Юречко – с сайта еженедельника Federal Computer Week довольно поспешно убрали краткий репортаж с памятной конференции разведслужб в Арлингтоне. (Спустя несколько лет, правда, то ли одумались, то ли забыли о прежних указаниях, и публикация вновь «всплыла» на сайте, см. www.fcw.com/fcw/articles/1998/FCW_052598_483.asp).

Трудно сказать, какие еще изыскания и эксперименты разведслужб на поприще манипуляций изображением произвели на американские власти

решающий эффект, но в конце 1999 года в недрах клинтоновской госадминистрации США родилась новость несколько иного рода. Было официально объявлено, что в министерстве обороны изучили вопросы применимости международного права к «информационным операциям», практикуемым военными, и пришли к выводу, что сгенерированные с помощью компьютера изображения в определенных обстоятельствах могут стать военным преступлением. Буквально, было сказано следующее: «[хотя] Используя технику компьютерного морфинга, имеется возможность создавать образ главы вражеского государства, информирующего свои войска о заключении перемирия или соглашения о прекращении огня», однако если это фабрикация, то подобный трюк «был бы военным преступлением». По всем параметрам подобный ход следует расценивать как «вероломство», иными словами – как явное нарушение общепринятых законов войны. Таким образом, американские военные сочли необходимым широко объявить, что на кибернетических полях сражений «вооруженные силы США будут сражаться в полном соответствии с законами войны»… [DV99].

Осталось неизвестным, какие именно конкретные причины или факты побудили военно-политическое руководство к подобным заявлениям. Но зато достоверно известно другое. В первых числах января 2000 г. германская газета «Франкфуртер Рундшау» сообщила, что видеолента НАТО, демонстрировавшаяся в предыдущем году по телевидению с целью оправдания убийства по меньшей мере 14 гражданских лиц в Косово, на самом деле была сфабрикована. Погибшие люди находились в поезде, который уничтожили в апреле 1999 г. самолеты НАТО, бомбя мост через реку Южная Морава. В оправдание убийства мирных жителей, представители военного блока тогда заявили, что поезд двигался слишком быстро, и траектории запущенных с самолетов ракет изменить было уже невозможно. Для документального подтверждения были продемонстрированы видеоленты, снимавшиеся телекамерами, установленными в боеголовках двух ракет, уничтоживших мост и поезд [FPOO].

В действительности же, как было установлено сотрудниками немецкой газетой, эти видеоленты демонстрировались со скоростью, в три раза превышающей реальную. Представители командования НАТО в Брюсселе были вынуждены признать данный факт, объяснив происшедшее «технической проблемой». Но самым пикантным в этой технической проблеме оказалось то, что счетчик хронометража, постоянно «щелкающий» в кадре видеоленты, показывал при этом вовсе не утроенную, а вполне нормальную скорость. Понятно, что никто из военных не пожелал вдаваться в подробности того, каким образом в видеолентах могут происходить столь удивительные метаморфозы. Но, учитывая возможности компьютерных технологий, подмена какого-то там счетчика – задача просто тривиальная.

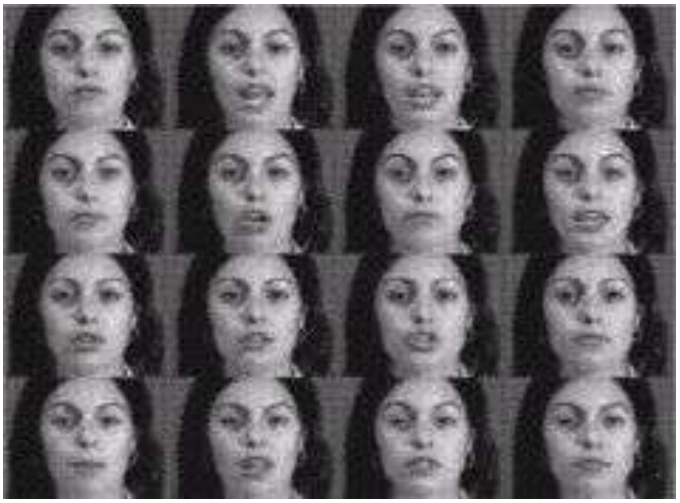
Говорит и показывает

Сегодня успешно решаются задачи куда более сложные. На конференции Siggraph-2002, традиционно собирающей мировую элиту

компьютерной графики и анимации, группа разработчиков из Массачусетского технологического института (МТИ) представила новую программу обработки видеозаписи, позволяющую имитировать произнесение человеком слов и фраз, которые в действительности тот никогда не говорил.

Нечто подобное делалось другими и раньше. Например, в конце 1990-х разработчики технологии Video Rewrite, совместно созданной в университете Беркли и компании Interval, обработали кинохронику с записью одного из выступлений президента Джона Кеннеди в 1962 году. В результате этой цифровой модификации речь президента пополнилась довольно забавными фразами, например, «Я никогда не встречался с Форестом Гампом» [EG02].

Главная же особенность новой программы МТИ – небывалая прежде реалистичность морфинга, в результате чего зрители, принимавшие участие в тестировании, оказались уже не в состоянии отличать реальную запись от сгенерированной компьютером. Кроме того, нынешняя техника компьютерной анимации обычно требует ручной доработки при «склеивании» комбинируемых фрагментов изображения говорящего, в то время как технология МТИ уже практически полностью автоматизирована.



Формирование «базовых» лиц программы речевого морфинга

Программа построена на основе самообучающейся системы искусственного интеллекта, которая после анализа 2-4-минутного видеоролика (необходимый для работы минимум) выделяет кадры, представляющие полный спектр возможных движений рта и окружающих его областей. После чего компьютер становится способен синтезировать любое выражение лица как комбинацию из примерно полусотни «базовых» лиц объекта. Затем программа просматривает всю имеющуюся видеозапись, обучаясь тому, как лицо отображает произнесение каждого звука и как оно двигается от одного звука к другому. Теперь, получая новую последовательность звуков, компьютер может сгенерировать точную картину движений области рта и аккуратно наложить эти движения на лицо объекта.

Разработчики признают, что в настоящее время высокая реалистичность образа достигается лишь на протяжении одной-двух фраз, после чего становится заметным отсутствие эмоциональности в лице

говорящего. Однако уже ведутся работы по созданию и более сложной модели, способной обучаться выражению базовых эмоций человека. Так что генерация эмоциональной окраски и все более достоверного звукового сопровождения синтезируемых сцен – дело лишь времени. Новая программа разработчиков МТИ уже применяется на телевидении для формирования более правдоподобной мимики при дубляже читаемых диктором новостей с английского языка на испанский. Потенциал подобной технологии в кино и компьютерных играх поистине неисчерпаем, поскольку позволяет реалистично возродить на экране любого из уже ушедших из жизни актеров или знаменитых людей.

Яркий тому пример – инициатива южнокорейского продюсера Чул Шина, возвращающего на киноэкраны легендарного Брюса Ли, героя целой серии культовых фильмов 1970-х годов о мастерах восточных единоборств. Скоропостижная смерть от кровоизлияния в мозг оборвала карьеру артиста в 1973 году, когда после картин «Кулаки ярости» и «Путь Дракона» он находился в самом зените славы. Несмотря на прошедшие годы, фильмы с Брюсом Ли по-прежнему пользуются популярностью у зрителей Азии, Америки и Европы. Поэтому в 2001 году Чул Шин объявил о начале съемок новой картины, в которой благодаря современным компьютерным технологиям в главной роли вновь будет выступать легендарный артист. Сгенерированный компьютером персонаж будет на равных участвовать в действии вместе с живыми актерами и актрисами. Для этого тщательно подобран список азиатских актеров-спортсменов, чрезвычайно похоже имитирующих манеру боя и движений Брюса Ли. С помощью хорошо известной в компьютерной анимации технологии «захвата движения» с максимальной реалистичностью моделируются все сцены схваток «цифрового Ли». Что же касается речи, то предполагается, что за Брюса Ли будет говорить актер с похожим голосом, а окончательное доведение тембра и прочих голосовых нюансов до оригинального звучания возьмет на себя программа синтеза речи [MS01].

Отдельного упоминания заслуживает и нынешний уровень наиболее продвинутых программ синтеза речи. С лета 2001 года научно-исследовательский центр ATT Labs занимается коммерческими продажами своего программного обеспечения Natural Voices (www.naturalvoices.att.com). По свидетельству экспертов, на сегодняшний день у этой программы нет конкурентов в правдоподобности воспроизведения тембра, нюансов интонирования и прочих особенностей натурального человеческого голоса. При этом программа, основная цель которой – перевод печатного текста в синтезированную речь, способна говорить не только заранее выбранным голосом, но и обучаться воспроизведению хорошо всем знакомых голосов знаменитостей, как ныне живущих, так и давно ушедших из жизни [АВОЗ].

На примере Natural Voices уже очевидно, что клонирование человеческого голоса достигло такого уровня совершенства, когда на слух разница с оригиналом становится неощутима. В своей «базовой» версии это программное обеспечение вышло на рынок с тремя голосами профессиональных актеров, двух мужчин и одной женщины. Затем были добавлены еще два голоса– «ребенка» и «бабушки». Активно ведутся работы над версиями программы для разных языков и диалектов. Уже

выпущены варианты «естественных голосов» на испанском, английском, французском и британском английском языках. Пока что комплект такого программного обеспечения стоит несколько тысяч долларов, и ориентировано оно на корпоративных клиентов, таких как телефонные компании; фирмы, занимающиеся созданием программ для чтения разного рода текстовых файлов; изготовители встраиваемых автоматизированных речевых устройств и тому подобное. Ясно, что перед бизнесом открываются захватывающие перспективы – привлечение толп новых клиентов с помощью легко узнаваемых голосов самых знаменитых актеров, телеведущих или политиков, бодро читающих нужные тексты абсолютно произвольного содержания. Но тут же встают многочисленные «скользкие» вопросы. Кто владеет правами на голос знаменитости? Наряду с полностью синтезированными актерами, проникающими ныне в кинематограф, не вытеснят ли синтезированные голоса живых артистов? Конечно же, всплывает сложнейшая проблема с имитацией голоса в мошеннических операциях, поскольку в телефонных переговорах начинается полное размытие границ между «настоящим» и «поддельным».

В настоящее время процесс обучения программы нужному – «заказному» – голосу выглядит следующим образом. Обладатель голоса приходит в студию, где в течение достаточно продолжительного времени – от 10 до 40 часов – начитывает специально подобранные тексты, от бессмысленной чепухи до бизнес-отчетов. Все сделанные записи нарезаются на крошечные звуки-фрагменты и в отсортированном виде хранятся в базе данных. Теперь, когда программа зачитывает произвольный текст, нужные фрагменты быстро извлекаются из базы, рекомбинируются и формируют требующиеся предложения. Данная технология именуется «конкатенативный синтез речи». Для тех ситуаций, когда в качестве обладателя заказного голоса фигурирует давно почившая знаменитость, подбирается массив архивных записей требуемого объема. Понятно, что если вдруг злоумышленники решат подделать чей-то голос, от них потребуется «всего лишь» накопить нужный объем достаточно качественных записей жертвы…

По сути дела, такие программы как Natural Voices и компьютерный морфинг видеоизображения предоставляют неисчерпаемые возможности для преступных злоупотреблений в целях фабрикации ложных улик, дезинформации, провоцирования и просто обмана публики. И сегодня многие эксперты по анализу изображений все чаще предполагают, что судам в ближайшее время придется, возможно, вернуться к средневековой практике и принимать во внимание лишь показания тех свидетелей, которые видели произошедшее собственными глазами.

Нейромаркетинговое мозготраханье

В условиях, когда очень многие осведомлены о возможностях злоупотребления компьютерными технологиями, всем – и политикам, и бизнесу – приходится действовать в этой области весьма осторожно.

Ведь противники-конкуренты не дремлют, и малейшая оплошность может самым сокрушительным образом сказаться на репутации. Но слишком уж заманчивые перспективы открывают научные и

технологические достижения на пути к установлению тотального контроля за мыслями «человека из народа» – а ведь это предел мечтаний идеологов и маркетологов. Разница лишь в том, что одним нужна послушная кукла для воплощения идей политического руководства, а другим – для непрерывной и интенсивной покупки потребительских товаров.

Вполне естественно и объяснимо, что и стратеги идеологического программирования, и специалисты маркетологи обычно бывают весьма скрытны, когда речь заходит о подробностях кухни манипулирования человеческой психикой. Как правило, конкретная и содержательная информация становится общедоступна лишь в тех нечастых случаях, когда изобретают и начинают раскручивать какой-нибудь новый перспективный метод «мозготраханья».

В конце 2002 года о намерении произвести революцию в маркетинге громко возвестило интересное научно-коммерческое заведение из города Атланта (шт. Джорджия, США) под названием «Институт наук о мышлении Брайтхаус» [BrightHouse Institute for Thought Sciences, http://www.thoughtsciences.com]. По сути своей, это маркетинговая компания нового типа, помимо психологов собравшая под своей крышей ученых-нейрофизиологов и специалистов-медиков по ядерно-магнитно-резонансному сканированию мозга. Здесь разработан особый метод «нейромаркетинга» на основе изучения ЯМР-снимков головы, когда тайные предпочтения потребителя устанавливаются по особой окраске специфических областей мозга, реагирующих положительными или отрицательными эмоциями на предъявляемую к оценке рекламу. Прагматичные руководители компании прямо заявляют, что при изучении реакции человека их абсолютно не интересует, нравится тому собственно реклама или нет. Главное – это установить, насколько она эффективна в подсознательной стимуляции покупки конкретного товара или в выработке большей лояльности к брэнду фирмы-заказчика исследования [JL02].

Принято считать, что концепция нейромаркетинга родилась в 1990-е годы в Гарвардском университете. В основе метода лежат результаты психологов, согласно которым около 95 процентов всей познавательной деятельности человека и всего мышления, включая эмоции, происходят ниже уровней нашего осознания, в подсознательной области. Поэтому основная задача, которую ставят себе психологи от маркетинга (и от политики, естественно), – это как подобраться к эффективному манипулированию подсознательной деятельностью мозга. В конце 1990-х гарвардский профессор-маркетолог Джерри Залтмен разработал общие методы нейромаркетинга, а также запатентовал специальную технологию, получившую название ZMET, от Zaltman Metaphor Elicitation Method – «метод извлечения метафор Залтмена». В методе ZMET для прощупывания подсознания человека используются наборы картинок, вызывающие у клиента положительный эмоциональный отклик и запускающие скрытые образы-«метафоры», стимулирующие покупку. После чего на основе выявленных метафор с помощью компьютера конструируются графические коллажи, закладываемые в основу рекламных роликов. Известно, что маркетинговая технология ZMET весьма популярна у заказчиков, ее используют более 200 фирм, таких как Coca Cola, Procter&Gamble, General

Motors, Eastman Kodak, General Mills, Bank of America, Nestle. Новый метод нейромаркетинга на основе магнитно-резонансного сканирования также использует специально подобранные картинки и фотографии, но реакция на них клиента устанавливается не беседой психологов, а непосредственным анализом снимков мозга.

Неизменно превосходный результат

Сколь же замечательными могут быть результаты непрерывной промывки мозгов населению, наглядно свидетельствуют результаты опросов общественного мнения. Вот, к примеру, поразительные цифры опроса американцев, проведенного газетой Washington Post в августе 2003 года по поводу войны в Ираке.

Почти 7 из каждых 10 опрошенных (точнее 69%) заявили о своей вере в то, что иракский лидер Саддам Хусейн принимал личное участие в подготовке террористических атак 11 сентября 2001 года… Подобной «веры» придерживаются большинство как республиканцев, так и демократов, а также прочих людей, считающих себя независимыми от главных политических партий [PR03].

И это на фоне того очевидного факта, что за два прошедших года администрация президента Буша не смогла представить ни единого доказательства, свидетельствующего о каких-либо связях между Ираком и организацией Аль-Каида, предположительно несущей ответственность за теракты. Нужны ли здесь более убедительные свидетельства того, насколько эффективно можно программировать массы на веру в любую чушь?

Глава 5. Плюсы и минусы перехвата

Страницы жизни героя, 1940. Шпионы и мафиози

Когда Уинстон Черчилль в 1940-м году стал премьер-министром Великобритании, то для установления тесных связей с высшим руководством США, вовлечения нейтральной Америки в войну с Гитлером и для разворачивания крупномасштабной разведывательной / контрразведывательной работы в Западном полушарии, он послал весьма неординарного человека – канадца Уильяма Стивенсона. Боевой летчик Первой мировой войны, удачливый изобретатель и предприниматель-миллионер в послевоенный период, Стивенсон активно сотрудничал в 1930-е годы с британской разведкой SIS (иначе именуемой MI-6), передавая ей ценные данные о разрабатываемых в Германии вооружениях и шифровальной технике. Незадолго до начала Второй мировой войны Стивенсон вызвался лично убить Гитлера, причем помогать ему в этой миссии намеревался британский военный атташе в Берлине полковник Мэйсон-Макфарлейн. Столь дерзкий план спецслужб был зарублен лишь личным вмешательством лорда Галифакса, тогдашнего министра иностранных дел Великобритании.

Весной 1940 г. Стивенсон (получивший с подачи Черчилля псевдоним Intrepid, «Бесстрашный») был назначен начальником нью-йоркской резидентуры SIS, которая вместе с существенным расширением функций вскоре получила и новое название – Британский центр координации безопасности (BSC). Ни один человек, вероятно, не сделал в 1940-е годы больше для стратегического военно-политического сближения Америки и Великобритании, нежели Уильям Стивенсон, выполнявший роль личного доверенного посредника между премьер-министром Черчиллем и президентом США Ф. Д. Рузвельтом. Он отвечал за координацию общих усилий союзных спецслужб и за обмен разведывательными данными между союзниками. Кроме того, Стивенсон отвечал и за особо деликатный участок – классификацию и распределение среди английских, американских и канадских государственных структур суперсекретных материалов радиоперехвата сил Германии, в массовых объемах дешифровавшихся британской криптослужбой.

Насколько деликатной была вся сфера вскрытия немецкой переписки, наиболее ярко свидетельствует то, что сам факт этой деятельности продолжал сохраняться в строжайшей тайне почти тридцать лет после окончания войны. И даже затем, в 1970-е годы впервые об этом стало известно вовсе не благодаря рассекреченным государственным архивам, а из мемуарной книги «Тайна Ультра», выпущенной в 1974 году на основе личных воспоминаний одним из непосредственных участников сверхсекретной программы, Фредериком Уинтерботемом [FW74].

Исследование всего спектра причин, по которым на секретах дешифрования пытаются удержать покров вечной тайны, выходит далеко за пределы данной книги. Но одна из главных причин в том, что в действительности главы великих держав часто знают много больше, нежели признают официально. А если информация об этом все же всплывает, то обнажаются вся лживость, лицемерие и бесчеловечность высокой политики. Самый типичный тому пример – уничтожение армадой германских бомбардировщиков английского города Ковентри, где в результате двух массированных авианалетов было уничтожено свыше 50 000 зданий и тьма мирного населения. В книге Уинтерботема впервые было раскрыто, что Черчилль заранее знал о готовящейся массированной бомбежке Ковентри, однако не сделал ничего для предупреждения и эвакуации населения, опасаясь, что это косвенно раскроет немцам факт дешифрования их секретной переписки. В воспоминаниях Уильяма Стивенсона, опубликованных несколько лет спустя, также упоминается данный эпизод. Причем Стивенсон, с присущим шпиону цинизмом уточняет, что это именно он рекомендовал колебавшемуся Черчиллю сохранить информацию в тайне – слишком уж ценным был источник, чтобы им рисковать [WS76]. Война есть война – жертвы неизбежны. (Интересно, что несмотря на независимое свидетельство двух непосредственных участников событий – высокопоставленных сотрудников разведки – многие современные историки Великобритании подвергают этот эпизод сильному сомнению. Чересчур он неприятен для официальной, лакированной истории.)

Центр BSC интенсивно занимался вербовкой агентуры в США, а в Канаде создал секретную разведшколу, где готовили диверсантов для

действий в тылу противника. Стивенсон возглавлял (а нередко и финансировал из собственного кармана) самые различные операции британской разведки в странах Северной, Центральной и Южной Америки. Среди этих операций BSC, в частности, были не только регулярные взломы посольств германских союзников с целью хищения шифрключей или систематический перехват и перлюстрация дипломатической почты, но также срыв атомных экспериментов Германии и «нейтрализация» выявленных агентов разведки стран Оси. Под последним обычно подразумевались убийства – германских шпионов просто отстреливали, давили в подстроенных автомобильных происшествиях, выбрасывали из окон высоких зданий. Отчеты о подобных операциях впоследствии вдохновляли авторов многих шпионских романов, включая и знаменитый цикл историй про Джеймса Бонда, созданный коллегой Стивенсона по британской разведке Яном Флемингом [OI89].

По причине чрезвычайно строгих требований к засекречиванию «государственных тайн» в Британии, США и Канаде, многие из дел Стивенсона и его команды так и остаются, похоже, нераскрытыми по сию пору. В 1945-46 годах большой архив документации BSC был перевезен на двух грузовиках из Рокфеллеровского центра, где была нью-йоркская резидентура англичан, в «Лагерь Икс», секретную разведшколу в канадской провинции Онтарио. Здесь под руководством Стивенсона был подготовлен итоговый суперсекретный документ The BSC Papers, мыслившийся как единственный официальный отчет о достижениях BSC в годы Второй мировой войны. После чего вся документация, лежавшая в основе отчета, была уничтожена. Сам же отчет размножили всего в 40 экземплярах, из которых 24 были также уничтожены еще до рассылки. Уильям Стивенсон оставил себе на память 2 копии, а остальные были разосланы главам США, Британии и Канады. Все присвоили документу гриф Top Secret и упрятали поглубже в секретные архивы.

За последующие 52 года упоминание об этом документе промелькнуло всего в нескольких работах исследователей, которым позволили ознакомиться с документом под строгим присмотром. И лишь в 1998 году Найджел Уэст, плодовитый автор шпионских романов и исторических исследований о Второй мировой войне, исхитрился приобрести копию отчета The BSC Papers и в 1999 году опубликовал ее, не испрашивая разрешения ни в каких инстанциях, под названием «British Security Coordination: тайная история британской разведки в Америках, 1940-1945» [WS98]. (Даже этот отчет, заметим, никак нельзя считать полным, поскольку в нем ни словом не упоминается операция Ultra. В 1946 году даже в совсекретных отчетах разведки говорить об успехах дешифрования запрещалось.)

Возвращаясь же в год 1940, к первому прибытию Стивенсона в США в качестве руководителя особо секретной миссии и личного посланника Черчилля, важно подчеркнуть, что в Америке в тот период были еще очень сильны не только нейтралистские, но и прогерманские настроения. Поэтому тесные связи Рузвельта, известного своим антинацизмом, с уже ведущей войну Англией могли вызвать серьезнейший политический кризис и даже несли в себе угрозу импичмента. Все было решено организовать в строгой тайне, в качестве же надежного канала Черчилль и Стивенсон

выбрали шефа ФБР (а теперь уже и контрразведки) Эдгара Гувера. Без участия этого человека развернуть в стране тайные операции и сотрудничество спецслужб было немыслимо.

Несмотря на секретную переписку Черчилля и Рузвельта, «подойти» к Гуверу англичане должны были самостоятельно, чтобы уже он вывел их на президента. Всю эту комбинацию Уильям Стивенсон провернул достаточно быстро, и в апреле 1940 года Гувер пригласил важного посланника для переговоров к себе домой, в новый особняк, куда он недавно переехал после смерти матери. От цепкого взгляда разведчика не могли ускользнуть развешанные повсюду портреты и фотографии самого Гувера, а также многочисленные снимки, картины и скульптуры других особей мужского пола. «Там были статуэтки обнаженных мужчин, – вспоминал впоследствии Стивенсон в мемуарах, – скульптуры на лестнице, изображавшие мужчин в довольно двусмысленных позах»…

Шпионы, как известно, всегда обращают внимание на нетрадиционную сексуальную ориентацию людей, поскольку здесь всегда заложен потенциал для будущих манипуляций. Однако первичные задачи посланника были совсем иные – Гувер согласился на сотрудничество, но непременным условием выдвинул информирование и санкцию президента, для чего устроил Стивенсону встречу с Рузвельтом. Дальнейшее, как говорится, известно.

Совместно с Гувером англичанам пришлось работать достаточно тесно, и вскоре Стивенсон сильно разочаровался в шефе ФБР. По мнению британских разведчиков, тот не умел извлечь пользу из информации, которую они ему поставляли. Или, выражаясь достаточно деликатными словами одного из шпионов, «Гувер умел мыслить только как полицейский». Другой шпион, сотрудник британской разведки А. М. Росс-Смит, работавший в США в годы Второй мировой войны, вспоминал об этом в значительно более крепких выражениях: «Гувер был маньяком, эгоистом и подлецом высшей пробы. Он был нашей постоянной головной болью».

Зато прекрасные и доверительные отношения быстро сложились между Стивенсоном и полковником Уильямом Донованом, которого традиционно принято считать «отцом-основателем» внешней разведки США. Ныне, правда, по мере раскрытия секретных архивов, на свет извлекается несколько иная версия рождения Центрального разведывательного управления.

В 1996 году, к примеру, вышла книга-исследование Томаса Троя, бывшего аналитика и штабного офицера ЦРУ, под названием «Дикий Билл и Бесстрашный: Донован, Стивенсон и происхождение ЦРУ». На основе документальных материалов Трои показывает, как английские разведчики углядели в Доновaне именно того, кто был им нужен в верхнем эшелоне власти США – влиятельного, решительного, агрессивного и умнейшего человека, с большой симпатией относившегося к действиям британской разведки. И именно Стивенсон подбросил Доновану идею о создании еще одной, новой разведывательной службы в дополнение к полудюжине уже имевшихся, слабых и малоэффективных. Донован передал эту идею президенту Рузвельту, в результате чего в 1941 году родился «Координатор информации». Главой этой новой структуры стал Уильям

Донован, в 1942 году служба преобразовалась в OSS, или Управление стратегических служб, на базе которого в 1947 году было создано ЦРУ [TT96].

Особый интерес для британской разведки представляла Испания, поскольку было чрезвычайно важно знать, насколько серьезно Франко намерен помогать войскам Германии в Северной Африке и других регионах. Английские агенты проникли в посольство Испании в Вашингтоне и похитили (тайно скопировали) криптоключи, что позволило Британии читать испанскую шифрованную переписку. Однако испанцы меняли ключи к шифрам каждый месяц, так что и англичанам приходилось ежемесячно наносить ночные визиты в посольство. Но в 1942 году в США был принят закон Маккеллара, радикально ужесточивший наказание для иностранцев, схваченных за подобными занятиями. Стивенсон уже отлично понимал, что представляет собой Эдгар Гувер, и знал, что полюбовно уладить эту проблему с шефом ФБР ему не удастся.

Англичанам не оставалась ничего иного, как раскрыть данную сторону своей работы Уильяму Доновану и попросить помощи у молодой американской разведки. Шансы на успех здесь были достаточно велики, поскольку отношения между Донованом и Гувером издавна были откровенно враждебными и ни для кого не были тайной. (Еще в 1924 году, когда Донован был помощником министра юстиции и фактическим боссом Гувера, он тоже был среди тех, кто рекомендовал назначить молодого и амбициозного человека на пост и.о. директора Бюро. Но очень скоро Донован понял, что сильно ошибся, и когда речь зашла об окончательном утверждении Гувера в директорском кресле, не только высказался решительно против, но вообще предлагал уволить того из министерства. В последующие годы, во времена правления Рузвельта Донован, имевший значительное влияние в республиканской партии, не раз повторял, что если республиканцы вернутся к власти, то он сделает все, чтобы Гувера с треском выгнали.)

В итоге Донован, не желавший видеть в Гувере помеху своей работе, пошел англичанам навстречу, и теперь уже специалисты УСС взяли на себя работу по регулярному проникновению в испанское посольство и похищению шифров. Но на четвертом заходе ФБР арестовало тихих взломщиков – ревнивый Гувер не без оснований считал подобные оперативные мероприятия внутри США исключительно своей прерогативой, а потому решил наказать зарвавшуюся внешнюю разведку. Взбешенный Донован (известный своей кличкой «Дикий Билл») в ответ отправил своих людей собирать компромат лично на Гувера и, в частности, на его гомосексуальные отношения с Клайдом Толсоном [JP01].

Много лет спустя Уильям Стивенсон туманно намекал, что им удалось получить некий компрометирующий материал на Гувера. Это помогало всякий раз, когда директор ФБР начинал упрямиться и не хотел сотрудничать с разведкой. Советник президента Рузвельта Эрнест Кунео, также причастный к секретам англо-американской дипломатии, откровенно говорил о том, что Стивенсон «безжалостно шантажировал Гувера» [AS93].

Еще одной организацией, подобравшей ключик к самому слабому месту директора ФБР, была мафия. А конкретнее – ее главный мозг, «финансовый гений преступного мира» Мейер Лански. Практически все его

соратники, возглавлявшие легендарный гангстерский синдикат 30-х годов, кончили плохо. Лаки Лючано провел больше 10 лет в тюрьме, благодаря сотрудничеству с американской разведкой в годы войны был досрочно освобожден и депортирован в Италию, где умер сравнительно нестарым человеком. Багси Зигеля и Арнольда Ротштейна убили киллеры. Лепке Бухалтер закончил жизнь на электрическом стуле в тюрьме Синг-Синг. А вот Мейер Лански, замешанный чуть ли не во всех преступлениях мафии, прожил на редкость благополучную жизнь и умер баснословно богатым человеком под ласковым солнцем Майами в 80 с лишним лет. При Гувере ФБР вплоть до 1970-х годов не трогало Лански, и, естественно, тому должны были иметься очень веские основания.

В книге-исследовании Энтони Саммерса «Тайная жизнь Эдгара Гувера» собраны свидетельства гангстеров из близкого окружения Лански, которые отзывались о боссе как о гении, как о человеке, который «собрал всех и вся вместе» и который «прижал к ногтю Эдгара Гувера». По их словам, у Лански были снимки, запечатлевшие Гувера в пикантной ситуации с Клайдом Толсоном. Поэтому Лански заключил сделку с Гувером, который обязался не трогать его. Это, по их словам, и было той причиной, по которой им долгое время не приходилось опасаться ФБР.

В то же время все гангстеры признавали, что никто из них этих фотографий не видел, а сам Лански никогда и ни с кем эту тему не обсуждал. Но среди своих все же мог отпустить по адресу Гувера глумливую ухмылку и замечание типа: «Ведь этот сукин сын у меня в кармане, не так ли?». Ходили также разговоры не только о фотографиях, но и о взятках, которые Лански давал не самому Гуверу, а людям из его близкого окружения.

Все это, конечно, лишь разговоры не самых достойных членов общества. Но, к примеру, в 1960-е годы канадская Королевская конная полиция перехватила разговор между одним из преступников, находившимся в Канаде, и Мейером Лански в США, где главарь мафии зачитывал выдержки из доклада ФБР, написанного всего за день до этого [AS93].

В 1979 году специальный комитет американского Конгресса, два года занимавшийся перерасследованием обстоятельств убийства Джона Кеннеди, установил связи между Мейером Лански и Джеком Руби, владельцем ночного клуба, застрелившим Ли Харви Освальда, предполагаемого убийцу президента. Ничего сверх этого, правда, комитет установить не смог, поскольку Руби был уже давно в могиле, а Мейер Лански был не только очень умным, но и всегда умел держать язык за зубами. Благодаря чему и прожил долго.

Служба гибкой морали

И суд присяжных, и адвокат, и экзекутор

В марте 2000 года американское правительство устроило для иностранных журналистов не совсем обычный информационный брифинг, в рамках которого выступил бывший директор ЦРУ Р. Джеймс Вулси.

Необычность мероприятию обеспечивала сама тема разговора, наиболее кратко формулируемая так – «Почему Америка шпионит за своими союзниками». Спустя несколько дней под этим названием Джеймс Вулси опубликовал еще и статью в солидном Wall Street Journal [JWOO]. По сути дела, и брифинг, и статья стали ответом американских властей на брожения и недовольство в Европе, возбужденные публикацией и официальным представлением в Европарламенте большого исследовательского отчета «Возможности перехвата 2000» (кратко, 1С 2000) [ICOO], русский перевод документа см., например, http://66.84.27.122/contra/intercept/interc.html].

Этот документ, подготовленный британским журналистом Данканом Кэмпбелом, из множества разнообразных, но вполне достоверных источников собрал информацию о деятельности суперсекретной автоматизированной системы электронной разведки Echelon. Систему «Эшелон», глобально охватывающую планету пунктами перехвата и анализа коммуникаций, на протяжении нескольких десятилетий сооружало содружество разведслужб пяти англоязычных стран: США (основная сила проекта), Великобритании, Австралии, Канады и Новой Зеландии.

Первые упоминания об этой системе начали появляться в печати еще в 1980-е годы [DC88], однако наиболее содержательный материал был собран в книге новозеландского исследователя Ники Хагера «Тайная власть» [NH96]. Как показали последующие парламентские разбирательства, о существовании «Эшелона» знали разведслужбы многих западных стран. Однако, все они предпочитали помалкивать, поскольку система радиоперехвата и дешифрования коммуникаций всегда считалась важнейшим форпостом борьбы с коммунистическим блоком, а тотальная секретность вокруг этой работы была главным залогом успеха.

Но в 1990-е годы в Европе стала расти обеспокоенность. Годы после развала «лагеря социализма» шли, а огромные (давно занятые американцами) станции радиоперехвата Менвит Хилл в Великобритании, Бад Айблинг в ФРГ, также как и прочие подобные базы помельче в других местах, совершенно не проявляли никаких признаков увядания или сворачивания. Поскольку явный противник с поля битвы исчез, в Старом свете зародились сильные подозрения, что теперь мощности станций в значительной степени используются для шпионажа за европейскими гражданами и компаниями. Все эти опасения и подтвердил доклад Кэмпбела 1С 2000, всколыхнувший правительства и парламенты многих стран Европы, поскольку в этом документе на конкретных примерах показано, что «Эшелон» не только нарушает право миллионов европейских граждан на приватность, но и, судя по всему, используется для промышленного шпионажа в пользу американских корпораций.

Волны от этого доклада пошли настолько сильные, что весной 2000 года вопрос о масштабах экономической разведки американских спецслужб особо обсуждался в американском конгрессе. Здесь, впрочем, и директор ЦРУ Джордж Тенет, и директор АНБ генерал-лейтенант Майкл Хейден в своих выступлениях всячески заверили законодателей, что не занимаются подобными вещами. Вся же их «дополнительная» разведдеятельность, помимо основной задачи по военно-политической разведке, направлена против террористов, наркоторговцев и незаконных

каналов отмывания денег.

Как выразился Тенет, «что касается обвинений в промышленном шпионаже, то просто неверна сама идея, будто мы занимаемся сбором разведывательной информации для продвижения американского бизнеса. Мы не нацеливаемся на иностранные компании, чтобы поддерживать интересы национальной индустрии». Однако, хотя Тенет и отрицал, что иностранные компании могут быть непосредственными целями ЦРУ, он все же признал, что в случаях, когда разведка США обнаруживает иностранные державы, пытающиеся «помешать американскому бизнесу играть честно», то эта информация передается в другие правительственные ведомства, отвечающие за соблюдение американских законов [RWOO]. При этом Тенет предпочел не вдаваться в подробности о том, что же делают эти «другие правительственные ведомства» с полученной информацией и какие выгоды в конечном счете получают от этого американские компании.

Тенет и Хейден, что называется, по долгу службы обязаны помалкивать о нюансах своей разведывательной работы, однако чиновники других ведомств госаппарата США более разговорчивы, и они значительно понятнее объясняют, что же скрывается за столь обтекаемыми и туманными формулировками главных шпионов страны. Например, имеются вполне официальные подтверждения, что, помимо прочего, за годы администрации Клинтона американская разведка помогла «Боингу» обойти консорциум «Аэробус» и продать партию авиалайнеров 747 Саудовской Аравии, компании Raytheon – обойти французскую CSF-Thomson и продать Бразилии дорогую и сложную систему наблюдения, а компании Hughes Network Systems – продать Индонезии систему связи. Но начинались такого рода операции еще раньше.

Рэндол Форт, один из бывших членов руководства Бюро госдепартамента по разведке и исследованиям, рассказывает в интервью, что задачи экономического характера начали ставить перед разведывательным сообществом США в период администрации Джорджа Буша [DC01]. По словам Форта, первый такой случай (явно продемонстрировавший Белому дому, насколько ценна подобная информация) произошел при обстоятельствах, когда США, «используя обычные методы разведки в системах связи», обнаружили, что «японцы занимаются подкупом в Сирии», пытаясь продать там свои электростанции. На данный случай обратили внимание, поскольку этот же контракт стоимостью около полумиллиарда долларов пыталась выиграть и американская компания. В результате «был предпринят тихий подход к сирийскому правительству» и сообщено, что если Сирия заинтересована в улучшении отношений с США, то ей не по пути с взяточничеством. В итоге контракт выиграла американская компания.

В разведку попадает масса всякого рода «побочной информации» в ходе глобального слежения за каналами связи. Для радиоперехвата используются орбитальные разведывательные аппараты, отводы от кабельных магистралей, множество секретных баз по всей планете, берущих информацию от спутников связи и радиосетей, а также прочие подобные средства, чтобы в автоматическом режиме накапливать и обрабатывать телефонные переговоры, телеграфные и факсимильные

сообщения, электронную почту и другие всевозможные виды телекоммуникаций. Фактически, из этого источника, по словам Форта, добываются около 85 процентов всех разведданных США. Но после истории с Сирией, если в потоке добываемой информации обнаруживалось нечто в том же духе, то в разведке «стали предпринимать упреждающие меры», накапливая в базе данных по этой теме уже все, что можно собрать. На основе накопленной информации далее стали проводить и соответствующие политические шаги.

Представитель госдепартамента США отправлялся к «номинально чистому» человеку в иностранном правительстве и сообщал тому, что «кое-кого схватили за руку непосредственно в банке с вареньем, поэтому не мешало бы обратить внимание и на компанию из США, участвующую в конкурсе». В некоторых случаях это приводило к передаче части контракта американской компании, в других – американцам советовали бороться с собственными взяточниками. Но иногда фирме из США доставался и весь контракт целиком. «Уровень успеха зависит от взаимоотношений США и данной страны… Это часть общей политической динамики. А не что-то такое, что ею управляет», – отмечает Рэндол Форт.

В документах, сопровождавших передачу власти, администрация Буша советовала команде Клинтона уделить этому направлению повышенное внимание, и благодаря усилиям новой администрации здесь продвинулись значительно дальше. Сбор экономических разведданных стал политикой. В ЦРУ стали издавать новый ежедневный разведывательный сборник под названием «Daily Economic Intelligence Briefing». Получивший высший уровень секретности, он печатается всего в 100 экземплярах и рассылается высшему руководству в Белом доме и руководителям департаментов в правительстве. Из четырех ежедневных сборников, готовящихся в ЦРУ, более ограниченный круг допущенных лиц имеет лишь брошюра «President's Daily Briefing» с тиражом в 32 экземпляра. На страницах «Экономического разведывательного ежедневника» на регулярной основе появляется информация об иностранном взяточничестве. В Министерстве торговли, в свою очередь, эти разведданные объединяются вместе с другой информацией других источников в специальном отделе под названием «Центр защиты», учрежденном в свое время министром Рональдом Брауном. Позаимствовав терминологию у ЦРУ, Браун говорил, что этот Центр «выравнивает игровое поле и содействует открытому соревнованию на международной арене торгов» [RWOO].

Но ни у кого, пожалуй, данное направление работы не вызывало столь бурного энтузиазма, как у директора ЦРУ Джеймса Вулси, который следующим образом описывал работу разведки в своей речи в вашингтонском Центре стратегических и международных исследований в июле 1994 года [JW94]: «То, что мы делаем в коммерческой области, – это очень специфическая вещь. Американские корпорации обязаны действовать в соответствии с законом, именуемым Foreign Corrupt Practices Act (запрещающим всем гражданам, компаниям и представительствам США предлагать взятки любым государственным чиновникам иностранных государств). Это очень жесткий закон. Он заставляет американские корпорации играть честно в 99 процентах всех состязаний за получение

зарубежных контрактов. Ни в одной стране нет закона, хотя бы отдаленно напоминающего Foreign Corrupt Practices Act. Множество стран в других частях света, включая некоторых из наших лучших друзей, очень глубоко вовлечены во взяточничество для получения тех контрактов, которые им не удалось бы выиграть обычным путем».

Далее Вулси примерно в тех же деталях описал уже известную схему с подходом американского посла, снабженного разведданными, к главе иностранного государства и то, что за этим обычно следует… «Так что довольно часто – не всегда – контракт пересматривается, и американская компания получает или весь контракт, или его часть. Мы подсчитали, причем очень консервативно, что сбором соответствующей разведывательной информации мы приносим на этих контрактах американскому бизнесу по несколько миллиардов долларов в год. И мы намерены продолжать этим заниматься. Это относительно новая вещь. Но нам это, честно говоря, очень, очень хорошо удается. И мы оказываем весьма позитивное воздействие на контракты для американского бизнеса. Порой я улыбаюсь, читая в газете, что какая-нибудь из этих корпораций, которым мы устроили очень, очень крупные контракты действиями подобного рода, выводит на публику одного из своих директоров и тот говорит „нам не требуется никакой помощи от американского разведывательного сообщества". Что ж, чудесно, это именно то, как работает разведка»…

Примерно те же самые мысли Вулси повторил и 6 лет спустя, в упомянутой в начале главы статье в Wall Street Journal за 2000-й год, оправдывая использование «Эшелона» для экономического шпионажа США против Европы. Естественно, далеко не все согласились с позицией скромного бойца невидимого фронта Джеймса Вулси. Автор 1С 2000 Данкэн Кэмпбел сразу же отметил, что Вулси заострил внимание лишь на двух (связанных со взятками) случаях из 7 зафиксированных в отчете свидетельств о шпионаже Америки против Западной Европы, где остальные 5 никакого отношения ко взяткам не имеют. Но также в такой интерпретации, по замечанию Кэмпбела, эта информация взъярит пол-Европы. Данные, что компании США получили заказов на миллиарды долларов, просто поразительны и многих приведут в бешенство. Но не потому, что кто-то из европейских политиков станет отрицать, будто некоторые из компаний не переступают черту, а по той причине, что у США нет никакого права быть здесь одновременно и судьей, и судом присяжных, и исполнителем приговора [DCOO].

Но больше всего беспокоит то, добавляет журналист, что вся эта свара из-за перехвата бизнес-коммуникаций затмит проблему, которая значительно серьезнее и, я полагаю, в равной степени должна заботить и американцев, и европейцев. Речь идет о гигантских масштабах вторжения в частную жизнь граждан. Вторжения, осуществляемого службами электронной разведки, будь они американскими, британскими или чьими-то еще. Я совершенно согласен, что то же самое делают и спецслужбы Франции, говорит Кэмпбел, и делают они это столь же бесстыдно, как делал это господин Вулси, когда работал в ЦРУ [KPOO].

Бизнес на страхе

Главная суть скандала, разгоревшегося вокруг «Эшелона» и вообще деятельности разведслужб, сводилась в тому, что прослушивание и перехват линий связи ведутся тотально, без каких-либо санкций судебных органов и вне зависимости от того, виновны в чем-то люди или нет. Ведь главный объект внимания разведок – это иностранные ведомства, компании и граждане, права которых национальные законы государств четко не регламентируют, а законы международные в данном случае никто обычно в расчет не берет. Все это, конечно, никакая не новость, однако подобную «беззаконную» ситуацию удавалось поддерживать до тех пор, пока широкую огласку не получили факты о реальных масштабах слежки и технических возможностях спецслужб.

С лета 2000 года в рамках Европарламента был создан специальный «Временный комитет по системе перехвата Echelon», занявшийся расследованием всех аспектов деятельности англоязычных союзников-шпионов. Правда, на работе комитета сразу же отразились слишком уж разные интересы стран-участниц – если Германия и Франция, к примеру, изначально были настроены очень сердито и решительно, то Британия (как член Эшелона) или Испания (сильно заинтересованная в перехвате баскских сепаратистов, обещанном США), напротив, всячески старались сгладить конфликт с Америкой. Как обычно, результатом столь сильного расхождения мнений стали длинные и не особо плодотворные дискуссии, из-за чего к комитету вскоре прилепился ярлык «беззубой говорильни» [SK01].

Пытаясь выработать сбалансированный подход к решению проблемы, Европарламент не только заслушал свидетельства информированных госчиновников и частных лиц, но также договорился с властями США о визите в страну представителей Комитета для непосредственной встречи с руководством американских спецслужб. Этот визит состоялся в мае 2001 года и завершился весьма характерно, даже не успев начаться. Несмотря на все предварительные договоренности и не опускаясь до объяснения причин, полдюжины американских разведслужб – ЦРУ, АНБ и т. д. – дружно прислали письменные уведомления, в которых кратко сообщили об отказе от встречи. Кто именно выдал такое указание, осталось неизвестным. По сути же дела, американцы бесцеремонно и демонстративно «захлопнули дверь» перед самым носом друзей-европейцев. Тем в ответ оставалось лишь прервать в знак протеста визит и вернуться домой раньше намеченного срока. Более никаких подобных встреч уже не организовывалось, так что официально сам факт существования «Эшелона» по сию пору официально не признан.

Зато главные выводы комитета Европарламента, изложенные и опубликованные летом 2001 года в большом 100-страничном отчете [EP01], свелись к тому, что у следствия нет никаких сомнений относительно существования глобальной системы перехвата телекоммуникаций, поддерживаемой совместными силами США, Великобритании, Канады, Австралии и Новой Зеландии, участвующими в данном проекте пропорционально своим возможностям. Система эта, скорее всего, реально именуется «Эшелон», но данная деталь представляется маловажной. Важно же то, что целью системы

действительно является перехват не военной связи, а частных и коммерческих коммуникаций.

Для противодействия промышленному шпионажу, членам Евросоюза было рекомендовано выработать единую стратегию защиты на основе европейских криптотехнологий, а самое главное – поддержать проекты, направленные на разработку дружественных пользователю программ шифрования с открытыми исходными кодами. Как организациям и фирмам Европы, так и обществу в целом комитет рекомендовал систематически прибегать к шифрованию электронной почты, дабы в конечном счете закрытие переписки становилось нормой. Одновременно прозвучал призыв к странам-участницам Европейского Союза заключить совместную декларацию о недопустимости промышленного шпионажа друг против друга (здесь следует принять во внимание, что ряд важнейших американских станций радиоперехвата находится непосредственно на территории Великобритании и Германии).

Летом того же 2001 года начали появляться и первые конкретные результаты. В частности, Министерство обороны США объявило, что после консультаций с местными властями Баварии решено закрыть одну из крупнейших в Европе американских станций электронной разведки в Бад Айблинге, расположенную юго-восточнее Мюнхена [DR01]. Полностью работу станции наметили прекратить к сентябрю 2002 года, после чего объект подлежал возвращению германскому правительству. Представители АНБ США и Пентагона не стали углубляться в подробности причин закрытия станции, заметив лишь, что после консультаций с германскими властями ликвидация объекта была сочтена «мудрейшим из решений», а высвобождающиеся при этом силы будут «сгруппированы и переориентированы». Всего на 2001 г. в Бад Айблинге работало 1800 человек американского персонала, включая представителей разведок армии, ВМС и ВВС, а также гражданский персонал АНБ. От германской стороны здесь работало лишь 150 человек. Оценивая наметившуюся тенденцию, ряд аналитиков стал выдвигать предположения, что в обозримом будущем участь Бад Айблинга вскоре, вероятно, может постичь и базу Менвит Хилл в Англии…

Но вскоре за этим наступило 11 сентября 2001 года, а вместе с известными событиями радикально изменилась и обстановка в Европе вокруг «Эшелона». Станции радиоперехвата вновь стали важнейшим форпостом борьбы «свободного мира»– на этот раз в войне с мировым терроризмом. Ни о каком сворачивании присутствия АНБ в Бад Айблин-ге уже и речи быть не могло. Более того, теперь американские власти очень быстро смогли убедить и граждан собственной страны, и Европейское сообщество, и прочих своих союзников, что ради укрепления безопасности следует пожертвовать некоторыми из традиционных гражданских свобод и прав на тайну личной жизни – ведь страшный враг-террорист у порога.

Любопытно отметить, с чем теперь (в очередной раз) в средствах массовой информации всплыл Джеймс Вулси. Теперь он провозглашает, что США, оказывается, ведут с боевиками исламского фундаментализма «Четвертую мировую войну» (третьей мировой, в классификации Вулси, была Холодная война). И эта четвертая мировая, по оценкам бывшего директора ЦРУ, будет длиться десятилетия [GC03]. А пока она идет,

подчеркнул Вулси, гражданам США придется пойти на определенные компромиссы между гражданскими свободами и безопасностью, поскольку важную позитивную роль могут сыграть такие технологии, как составление «профилей риска» на авиапассажиров, накопление и проходка данных в базах вроде TIA, ну и более тщательный перехват-анализ коммуникаций, естественно.

Как только раздаются подобные речи о перспективах «трудной и долгой войны», тертые в политике и бизнесе люди сразу вспоминают древний принцип – «смотри, где деньги». В конкретной ситуации в Джеймсом Вулси даже искать ничего не надо – все лежит на поверхности.

Вскоре после начала боевых действий США в Ираке, в издании Wall Street Journal появилась публикация, демонстрирующая, что многие члены влиятельного Консультативного политического совета Пентагона (Defense Policy Board) в финансовом отношении лично заинтересованы в расширении масштабов войны и в мощном укреплении силовых структур государства [НВОЗ]. Поскольку этот консультативный совет экспертов дает рекомендации министру обороны по широкому кругу политических и стратегических вопросов, общепринятые нормы этики предполагают, что личные бизнес-интересы членов совета не должны пересекаться с военно-политическими делами. В действительности же все обстоит с точностью до наоборот.

По крайней мере десять членов совета могут извлекать из своих консультаций серьезную личную прибыль. В частности, входящий в Defense Policy Board советник Джеймс Вулси одновременно является вице-президентом крупной консалтинговой фирмы Booz Allen Hamilton Inc, которая за один лишь 2002 год получила от Пентагона контрактов на 688 миллионов долларов. Помимо этого, Вулси – один из трех владельцев-руководителей совсем молодой, но уже ворочающей сотнями миллионов долларов инвестиционной фирмы Paladin Capital Group. Эта фирма финансирует проекты и компании, ориентированные на заказы нового «управления имперской безопасности» (точнее, Department of Homeland Security – Управление безопасности отечества) с заманчивым госбюджетом в 47 миллиардов долларов. Другим основателем-совладельцем фирмы Paladin, кстати говоря, является еще один бывший высокопоставленный шпион, генерал-лейтенант Кеннет Минихен, возглавлявший в 1990-е годы Агентство национальной безопасности США [ШОЗ].

Возвращаясь к составу Консультативного политсовета Пентагона, среди его членов отмечено множество фигур, для которых война – просто золотая жила. Так, отставной адмирал Дэвид Джеримайя входит также в совет директоров по меньшей мере пяти корпораций, которые за 2002 год получили от Пентагона контрактов на сумму свыше 10 миллиардов долларов. Другой «консультант», отставной генерал ВВС Рональд Фоглмен тоже заседает в руководстве пяти оборонных фирм, за год получивших на военных заказах свыше миллиарда долларов. Если же все эти цифры просуммировать, то оказывается, что десяток членов Политсовета тесно связан с компаниями, получившими за 2001-2002 гг. на контрактах Пентагона свыше 76 миллиардов долларов [DC03].

Интереснее же всех, возможно, устроился глава Defense Policy Board

ястреб Ричард Перл, которого называют одним из главных архитекторов иракской войны. С одной стороны, Перл, как и Джеймс Вулси, возглавляет собственную инвестиционную фирму Trireme Partners, специализирующуюся на контрактах по укреплению имперской безопасности. С другой же стороны, как выяснилось, Ричард Перл также получает приличные деньги и от компании, которая своими действиями потенциально этой самой безопасности угрожает [НВОЗ].

Суть истории такова. Крупная, но находящаяся на грани банкротства телекоммуникационная фирма Global Crossing положила Ричарду Перлу зарплату в размере 750 000 долларов, чтобы он порадел за нее в Пентагоне и добился разрешения на продажу фирмы азиатским инвесторам. Министерство обороны США, в частности АНБ, категорически возражало против этой сделки, поскольку Global Crossing – это гигантская, длиной в сотни тысяч километров система оптоволоконных кабелей, по дну океана опоясывающих земной шар и обеспечивающих широкополосную магистраль для множества стран. Понятно, что новый владелец Global Crossing непременно узнает, кого и как перехватывает здесь разведка США, а кроме того и у других стран появятся заманчивые возможности для расширения шпионажа за военными и промышленными секретами Америки… [ВВОЗ].

Короче говоря, возражений и аргументов против продажи крупно задолжавшей фирмы азиатскому капиталу было в достатке. Разбирательства с этим вопросом шли более полугода, однако в итоге, в сентябре 2003 года, президент Буш все же дал окончательное разрешение на продажу основной доли Global Crossing (62%) сингапурской компании Singapore Technologies Telemedia [KN03]. А Ричард Перл, соответственно, честно заработал на этой сделке свою долю (по условиям найма, из положенных ему 750 тысяч основная часть суммы – 600 000 долларов – выплачивалась только в случае успешного завершения мероприятия).

Неизвестно, что сказал по этому поводу кристально чистый страж морали и ярый враг взяточничества Р. Джеймс Вулси, но схема честного бизнеса по-американски здесь предельно ясна. Зачем давать кому-то пошлые (и противозаконные) взятки, если можно вполне легально сидеть *сразу* в нескольких креслах, одной рукой выписывая деньги из казны, а другой их получая в собственный карман.

Сюрпризов не избежать

В первых числах марта 2003 года журналисты британского издания Observer опубликовали совсем свежий и совершенно секретный документ американской разведслужбы АНБ [ВВОЗ]. В этом неведомо как добытом материале раскрывались «грязные трюки» (так называлась публикация), на которые идут США ради одобрения Советом безопасности ООН запланированной войны в Ираке. Документ представлял собой инструктивное письмо, разосланное одним из высших чинов АНБ в адрес начальников региональных подразделений, занимающихся радиоперехватом в разных точках планеты, и руководителей иностранных спецслужб разведывательного содружества. В письме даны подробности о весьма агрессивной операции по плотному отслеживанию всех

коммуникаций иностранных дипломатов, представляющих свои страны в штаб-квартире ООН в Нью-Йорке, с особым упором на непостоянных членов Совета безопасности – Анголу, Болгарию, Гвинею, Камерун, Чили и Пакистан.

В своем циркулярном меморандуме начальник «штаба региональных объектов» АНБ Фрэнк Коза (Frank Koza) извещал о запуске особого плана по усилению целенаправленного прослушивания «членов Совета безопасности (исключая США и Великобританию, конечно) для понимания того, как эти страны будут реагировать на дебаты вокруг Ирака, каковы планы их голосования по соответствующим резолюциям, возможные союзы/зависимости и т.д. – т.е. полный спектр информации для достижения нужных США целей и избежания сюрпризов». Публикация этого письма, датированного 31 января 2003 года, интересным образом дополнила разговоры в политических кулуарах о неафишируемом, но настойчивом давлении США на неопределившиеся в своей позиции к войне страны, которым стали грозить неприятные экономические последствия в случае несогласия с точкой зрения Америки.

До публикации, для подтверждения подлинности раздобытого меморандума, журнал Observer показал его трем бывшим сотрудникам разведки, которые подтвердили аутентичность языка, формы и общего содержания документа. Более того, журналисты даже дозвонились в АНБ и установили реальное существование там начальника по имени Фрэнк Коза. Однако, когда их соединили по внутреннему коммутатору с административным аппаратом Козы, там, узнав цель звонка («взять интервью о прослушивании дипломатических миссий в ООН») сразу же ответили, что это «не тот номер» и повесили трубку.

Естественно, многие дипломаты в ООН предполагают наличие «жучков» в своих офисах, компьютерах и телефонах, однако просочившийся в печать меморандум впервые столь конкретно раскрыл масштабы и цели радиоперехвата коммуникаций, глобально осуществляемого АНБ США и их ближайшими союзниками. Неудивительно, что этот материал получил мощный резонанс в СМИ многих государств – кроме США. Здесь центральные информационные агентства словно воды в рот набрали. Точнее, многие новостные службы, включая CNN, NBC и Fox TV поначалу спешно договорились об интервью с Мартином Брайтом, опубликовавшим документ журналистом из Observer, но затем дружно, словно по команде запланированные встречи отменили [NS03]. Так что если в американской прессе кое-где и прошли маленькие сообщения о скандальной публикации, то, как правило, в тоне сильных сомнений относительно подлинности данного циркуляра.

Основания для сомнений действительно имелись, поскольку содержание письма явно предназначалось для руководства высшего звена, т.е. имело узкий круг ознакомления, а значит вычислить источник утечки не представляло особого труда. Другими словами, если кто-то в разведке и решился «сдать» документ в прессу, то сделал это из принципа, вполне понимая грозящие за разглашение последствия. Такое в разведке бывает крайне редко, однако несколько дней спустя действительно поступили сообщения об аресте одной из сотрудниц в Штаб-квартире правительственной связи Великобритании (ШКПС), спецслужбе-аналоге

американского АНБ. Полиция сообщила, что ею арестована 28-летняя женщина по обвинению в разглашении государственных секретов, и «впоследствии будут произведены другие аресты»… [MBO3].

Впрочем, за все последующее время никаких арестов больше не было, а женщину – переводчицу ШКПС Кэтрин Терезу Гюн – вскоре выпустили под залог на свободу, дожидаться суда. В июне, после внутреннего разбирательства в спецслужбе, ее уволили. Следствие закончилось к ноябрю, когда Кэтрин Гюн было официально предъявлено обвинение в нарушении Закона о государственных секретах, на основании которого в Британии обычно привлекают к ответственности людей за допущенные утечки информации. В своем ответном заявлении Гюн, которой грозит до двух лет тюрьмы, назвала свои действия попыткой предотвратить неправедную войну. Цитируя ее слова дословно: «Любые раскрытия информации, которые здесь можно сделать, оправданы уже тем, что они демонстрируют серьезную противозаконность и преступления той части правительства США, которая пытается разложить наши собственные службы безопасности. Они оправданы тем, что способны помешать массовой гибели и потерям среди обычных иракских людей и вооруженных сил Великобритании в ходе этой преступной войны».

Защищать бывшую переводчицу ШКПС в суде вызвалась лондонская правозащитная организация Liberty, где полны решимости превратить дело Кэтрин Гюн в общественный форум для более широкого и критического разбора причин, втянувших Великобританию в иракскую военную кампанию. Это дело, говорят в Liberty, можно обратить в судебные слушания о законности войны в Ираке [AS03].

GSM : Что показало вскрытие

Весной 2001 года на страницах респектабельных американских журналов New Yorker и New York Times Magazine стала появляться большая, размером во всю полосу реклама, отличавшаяся весьма необычным для столь коммерческого жанра содержанием. Над крупной фотографией сотового телефона была помещена надпись: «Теперь оборудован для 3 сторон: вы; те, кому вы звоните; правительство».

Это заявление– ни в коей мере не преувеличение, говорилось в дальнейшем тексте рекламы, поскольку оборотной стороной стремительного развития компьютерных коммуникаций стала для людей повышенная уязвимость их частной жизни. От звонков по сотовому телефону до электронной почты в Интернете– всюду право граждан на тайну личной информации находится ныне под угрозой. В этом, собственно, и состоял основной посыл рекламного объявления, опубликованного Американским союзом гражданских свобод (American Civil Liberties Union, ACLU) в нескольких ведущих национальных изданиях США. В ACLU убеждены и доказывают, опираясь на факты, что правительственные спецслужбы постоянно нарушают конституцию, защищающую граждан от несанкционированной правительственной слежки.

Правда, после 11 сентября 2001 года разведывательные и правоохранительные органы получили массу дополнительных санкций на

усиление электронной слежки, а вести разговоры о чрезмерном вторжении государства в тайну личной жизни стало как бы несвоевременно и «антипатриотично». А потому после 2001 года в Интернете заметно сократился объем новой содержательной информации о серьезных и явно искусственно созданных слабостях в защите коммуникационных компьютерных программ или, к примеру, в популярнейшей системе сотовой телефонии GSM.

Но и в 2000 году про защиту GSM практически все наиболее существенное стало уже известно, несмотря на многолетние попытки окружить подробности схемы завесой секретности.

Либо ложь, либо некомпетентность

Для начала – две цитаты. Две диаметрально противоположные точки зрения, которые сразу же дадут читателю представление об остроте проблемы.

Вот что говорил в конце 1999 г. Джеймс Моран, директор подразделения, отвечающего в консорциуме GSM за безопасность и защиту системы от мошенничества: «Никто в мире не продемонстрировал возможность перехвата звонков в сети GSM. Это факт… Насколько нам известно, не существует никакой аппаратуры, способной осуществлять такой перехват» [DM99].

А вот реакция Питера Гутмана, весьма известного хакера-криптографа из Оклендского университета (Новая Зеландия): «Имея ситуацию, когда целый ряд компаний продает оборудование для перехвата GSM (причем делается это уже в течение определенного времени и с весьма открытой рекламой в Сети), этот директор по безопасности „либо лжет, либо некомпетентен, либо и то, и другое разом" (цитируя строку из книги Deep Crack). Интересно то, что сейчас все рекламирующие данное оборудование фирмы устроили ограниченный доступ на свои сайты, по-видимому, для поддержания мифа о том, что „не существует аппаратуры, способной осуществлять такой перехват"» [PG99].

Всю вторую половину 1990-х годов в Интернете и СМИ не раз вспыхивали дискуссии как вокруг самой защиты системы мобильной связи GSM, так и вокруг многочисленных случаев ее компрометации. К концу десятилетия почти всем уже, по сути дела, стало ясно, что GSM – это классический пример провала стратегии, именуемой на англоязычном Западе SbO, что в зависимости от чувства юмора расшифровывают либо как Security by Obscurity (безопасность через неясность), либо как Security by Ostrich (безопасность по-страусиному). На протяжении примерно десяти лет постепенно обнажались типичные пороки и неудобства стратегии, согласно которой степень защиты системы в значительной степени увязывается с сохранением в тайне как особенностей конструкции, так и случаев ее компрометации. То, что система GSM от рождения несет в себе перечисленные порочные черты, является вполне естественным. Просто потому, что рождалась GSM в соответствующих исторических условиях и от вполне определенных родителей.

Что такое защита GSM и как она создавалась

В принципе, по своему замыслу, цифровая система GSM вполне могла бы быть чрезвычайно защищенной. В основе ее лежит свод документов под названием «Меморандум о понимании стандарта GSM» или MoU Groupe Special Mobile standard. Этот Меморандум был подготовлен на излете Холодной войны по инициативе ведущих телекоммуникационных компаний Западной Европы. Разрабатывал техническую документацию GSM Европейский институт стандартов по телекоммуникациям (ETSI), а в создании схемы безопасности, в целом призванной защитить новую систему от перехвата, прослушивания и мошенничества, активное участие приняли спецслужбы стран НАТО [КВ93].

Основу системы безопасности GSM составляют три секретных алгоритма (вплоть до конца 2003 г. официально так и не раскрытые, сообщаемые лишь тем, кому это требуется по необходимости – поставщикам оборудования, операторам связи и т.д.):

- A3 – алгоритм аутентификации, защищающий телефон от клонирования;
- A8 – алгоритм генерации криптоключа, по сути дела, однонаправленная функция, которая берет фрагмент выхода от A3 и превращает его в сеансовый ключ для A5;
- A5 – собственно алгоритм шифрования оцифрованной речи для обеспечения конфиденциальности переговоров. В GSM используются две основные разновидности алгоритма: A5/1 – «сильная» версия шифра для избранных стран и A5/2 – ослабленная для всех остальных. (В 2000-е годы для следующего поколения мобильной связи, G3, создан совершенно новый криптоалгоритм, получивший название A5/3. Еще имеется вариант A5/0 – это когда режим шифрования вроде как включен, но в действительности его нет, поскольку вместо битов ключа используются одни нули.)

Мобильные станции (телефоны) снабжены смарт-картой (SIM), содержащей A3 и A8, а в самом телефоне имеется чип с алгоритмом A5. Базовые станции также снабжены чипом с A5 и «центром аутентификации», использующим алгоритмы A3-A8 для идентификации мобильного абонента и генерации сеансового ключа шифрования.

Вся эта архитектура при надлежащем исполнении и качественных алгоритмах призвана гарантировать надежную аутентификацию пользователя, обеспечивая защиту мобильных станций от клонирования и прочих методов мошенничества, а также качественное шифрование конфиденциальных переговоров. Собственно говоря, именно это и декларируется компаниями, успешно занимающимися разворачиванием GSM по всему миру и уже охватившими услугами удобной связи многие сотни миллионов человек на планете.

Но реальность такова, что спецслужбы, занятые защитой правительственной связи, одновременно вовлечены и в деятельность противоположного рода: перехват и дешифрование коммуникаций в разведывательных целях. По этой причине, как свидетельствуют очевидцы, вокруг степени защиты GSM бушевали немалые страсти, поскольку спецслужбы стран НАТО имели довольно разные точки зрения на этот счет. Германия настаивала на сильных алгоритмах, поскольку

имела самую длинную границу с коммунистическим блоком, другие же страны склонялись к ослабленному варианту. В конце концов в качестве основы криптосхемы для A5 была избрана французская военная разработка [RA94].

Первые утечки, первые тревоги

Как бы строго ни контролировались коммерческие секреты, понятно, что широкое распространение продукции рано или поздно приводит к утечкам информации. В GSM они стали появляться уже в начале 90-х годов. К 1994 году основные детали алгоритма A5 уже были известны. Во-первых, British Telecom передала всю техническую документацию Брэдфордскому университету, забыв заключить соглашение о неразглашении информации. Во-вторых, описание A5 появилось в материалах одной из конференций в Китае. Короче говоря, детали о конструкции алгоритма понемногу стали просачиваться в печать, и в конце концов кембриджские ученые М. Роу и Р. Андерсон опубликовали восстановленную по этим деталям примерную криптосхему в Интернете.

Представляет схема собой следующее. A5 реализует поточный шифр на основе трех линейных регистров сдвига с неравномерным движением. Такого рода схемы на языке специалистов именуются «криптографией военного уровня» и при верном выборе параметров способны обеспечивать очень высокую стойкость шифра. Однако, в A5 длины регистров выбраны очень короткими – 19, 22 и 23 бита. Начальное заполнение этих регистров в сумме и дает 64-битный сеансовый ключ шифрования в GSM. Уже одни эти укороченные длины регистров дают теоретическую возможность для хорошо известной криптографам лобовой атаки, когда перебирают заполнение двух первых регистров, восстанавливая содержимое третьего регистра по выходной шифрующей последовательности.

Регистры сдвига в схеме A5 имеют не только короткую длину, но и слабые прореженные полиномы обратной связи. Это дает шансы на успех еще одной атаке – корреляционному анализу, позволяющему вскрывать ключ по просачивающейся в выход информации о заполнении регистров. В июне 1994 года д-р Саймон Шеферд из Брэдфордского университета должен был представить на коллоквиуме IEEE в Лондоне свой корреляционный способ вскрытия A5. Однако, в последний момент его выступление было запрещено спецслужбой GCHQ, Штаб-квартирой правительственной связи. Доклад был сделан лишь на закрытой секции и опубликован в засекреченном сборнике [SS94].

Прошла еще пара лет, и до анализа A5 дошли руки у сербского криптографа д-ра Иована Голича, наиболее, вероятно, авторитетного в академических кругах специалиста по поточным шифрам [JG97]. С чисто теоретических позиций он описал атаку, позволяющую легко вскрывать начальные заполнения регистров всего по 64 битам шифрпоследовательности. (Справедливости ради надо, правда, отметить, что в реальности данная атака оказалась значительно более трудоемкой. Проведенный в стенах Microsoft эксперимент [PL98] действительно привел к вскрытию ключа, но понадобилось для этого около двух недель работы 32-узлового кластера машин РП-300. Практичной такую атаку никак не

назовешь. Правда, и репутация у криптоэкспертов Microsoft, мягко говоря, не блестящая.) Но в той же работе Голича был описан и еще один метод, известный в криптоанализе под общим названием «балансировка время-память», позволяющий существенно сокращать время вскрытия за счет интенсивных предвычислений и хранения предварительных данных в памяти. Так, к примеру, можно было сократить количество опробований вариантов ключа всего до смешных 222 (вскрытие просто «влет»), но для этого требовались 64 терабайта дисковой памяти (что, понятное дело, тоже трудно назвать приемлемыми цифрами для практичной атаки). Но сама идея четко продемонстрировала метод постепенного выхода на реальное соотношение параметров.

А вскоре пошли и сигналы уже о действительном вскрытии защиты системы GSM.

Клонирование и перехват

В апреле 1998 г. группа компьютерных экспертов и криптографов из Калифорнии широко объявила и продемонстрировала, что ей удалось клонировать мобильный телефон стандарта GSM. Ранее всеми по умолчанию предполагалось, что цифровые сети GSM гораздо надежнее защищены от этой напасти, приносящей миллионные убытки сетям аналоговой сотовой телефонии [SC98].

Возглавлял группу Марк Брисено (в Сети более известный как Лаки Грин), глава ассоциации SDA (Smartcard Developer Association), представляющей интересы разработчиков программного обеспечения для смарт-карт. Избрав своей целью определить степень стойкости GSM к попыткам клонирования, исследователи занялись обратной разработкой модуля SIM – той самой смарт-карты, что вставляется в сотовый телефон, содержит алгоритмы A3-A8 и однозначно идентифицирует абонента. В процессе подготовки к работам по вскрытию содержимого чипа, в руки к исследователям неисповедимыми путями попало описание «алгоритма COMF128» – наиболее широко распространенной практической реализации A3-A8 в SIM-модулях. Эта документация помогла быстрее и полностью восстановить всю необходимую информацию о схеме. После этого Брисено пригласил для ее анализа двух молодых, но уже известных криптоаналитиков, аспирантов Калифорнийского университета в Беркли Дэвида Вагнера и Иэна Голдберга. Тем понадобилось всего несколько часов, чтобы отыскать в схеме фатальные прорехи и разработать метод извлечения из смарт-карты секретного содержимого с помощью 219 опросов чипа (примерно 8 часов).

Представители консорциума GSM, как это принято, сразу же объявили полученные результаты «лабораторными» и не несущими реальной угрозы пользователям сотовой связи. По сути, угроза была представлена «нереальной» лишь на том основании, что в США обладание оборудованием для клонирования и публичная практическая демонстрация разработанной атаки являются противозаконными. Но уже очень скоро стали появляться сообщения о демонстрации клонирования телефонов GSM в странах с иным законодательством, в частности, в Германии [CC98].

Затем, вместе с освоением новых способов атак – через анализ

побочных каналов утечки информации – появились и намного более эффективные методы клонирования. Так, в 2002 г. группа криптографов исследовательского центра IBM продемонстрировала, что взламывать алгоритм COMP128 и клонировать SIM-карту можно меньше чем за минуту [RR02].

Об имеющихся на рынке средствах перехвата и мониторинга GSM (сама возможность чего до неприличия долго отрицалась официальными представителями MoU) наиболее красноречиво рассказывают реальные объявления в Интернете. Чтобы не ходить далеко, достаточно процитировать текст веб-страницы одного из виртуальных магазинов, развернутых в России в конце 1990-х годов (вскоре, правда, сайт упрятали из общего доступа поглубже – по той же, в сущности, схеме, как это делают все солидные-официальные торговцы подобной аппаратурой):

Система профессионального тестирования и мониторинга GSM

Используя наше уникальное аппаратное и программное обеспечение, «Система…» будет отслеживать звонки в границах выделенной области, оставаясь подключенной к соединению. Она будет выводить на дисплей управляющие команды, идущие на телефон и от телефона, отслеживать речевой канал (голос) и резервный канал (где проходят: SIM –номер модуля идентификации абонента, IMSI – международный идентификатор абонента мобильной связи, TMSI – временный идентификатор абонента, SAK – ключ аутентификации абонента, PIN – номер персональной идентификации и другая информация). Процесс декодирования и выполнения всех калькуляций занимает около 2,5 минут, так что длительность телефонного соединения, которое вы отслеживаете, должна быть по крайней мере такого же порядка, чтобы устройство мониторинга могло обработать и проверить всю информацию, включая соответствующие значения для программирования нового SIM [т.е. для клонирования GSM-телефона]. *Программное и аппаратное обеспечение позволяют отслеживать конкретные номера телефонов. Можно создавать «файлы регистрации данных» (data log flies) для последующего анализа, а аудиоинформацию можно записывать для контроля с помощью звукозаписывающего оборудования (в поставку не входит). В комплект поставки входит подробное Руководство и программное обеспечение для Windows или DOS . Данная система разработана для 900 Мгц GSM – сетеu . Цена – 4500 долларов. Все заказы оплачиваются через Western Union или трансфером банк-банк.*

Тотально ослабленная защита

В начале 1999 года в ассоциации SDA были полностью восстановлены и проверены на реальных тестовых векторах криптосхемы алгоритмов A5/1 и A5/2. Обратное восстановление A5/2 подтвердило уже имевшуюся информацию, что в этой схеме добавлен еще один короткий регистр длиной 17 бит, управляющий движением бит в остальных трех регистрах. Вагнеру и Голдбергу очень быстро удалось продемонстрировать, что в этих условиях для вскрытия системы достаточно лобовым перебором (сложность

216) отыскать заполнение управляющего регистра. Делается это всего по двум фреймам сеанса связи длиной по 114 бит (в системе GSM первые два фрейма шифрпоследовательности известны, поскольку шифруются одни нули). Другими словами, вскрытие такого шифра осуществляется буквально «на лету», за 15 миллисекунд работы рядового персонального компьютера [DW 99].

Подводя своего рода итог проделанному в Smartcard Developer Association исследованию, Лаки Грин следующим образом выразился о соотношении декларируемой и истинной безопасности проанализированной системы: «Мой опыт работы с GSM показывает, что разведывательные службы, стоящие как известно, за всеми криптоалгоритмами GSM, используют в своей работе весьма специфический подход. Разведслужбы компрометируют любой и каждый компонент криптосистемы, какой только можно скомпрометировать. Разведслужбы, имея такую возможность, ослабляют компонент просто потому, что могут это сделать, а не потому, что им это нужно. Это как бы извращенное воплощение в целом правильного принципа многократной избыточности» [LG 99].

Это весьма сильное, прямо скажем, заявление Лаки Грин затем подтверждает на конкретных примерах выявленных в GSM слабостей, серьезным образом компрометирующих систему.

- Скомпрометирована эффективная длина сеансового ключа. В 64-битном ключе, который A8 генерирует для A5, последние 10 бит принудительно обнулены. Это совершенно умышленное ослабление системы примерно в 1000 раз.
- Скомпрометирована система аутентификации и алгоритм генерации секретного ключа. Известно, что о слабостях в COMP128, обнаруженных SDA в 1998 году, участники GSM MoU были официально уведомлены еще в 1989 году. То есть задолго до широкого распространения GSM. Имеющаяся в MoU «группа экспертов по алгоритмам безопасности» (SAGE), состоящая из никому неведомых людей, сохранила в тайне это открытие и не стала информировать о нем даже собственно членов MoU. В результате чего разведслужбы имеют возможность клонировать телефоны и вычислять секретные ключи абонентов непосредственно в ходе сеанса связи.
- Скомпрометирован сильный алгоритм шифрования A5/1. В этом шифре с 64-битным ключом имеются многочисленные конструктивные дефекты, приводящие к стойкости, не превышающей стойкость шифра с 40-битным ключом (другими словами, стойкость понижена на 6 порядков или в миллион раз). Непостижимо, каким образом столь очевидный дефект мог быть упущен французскими военными разработчиками.
- Скомпрометирован более слабый алгоритм шифрования A5/2. Хотя в MoU признают, что вскрываемость шифра и была целью разработки A5/2, тем не менее в официальных результатах анализа SAGE сказано, что им неизвестно ни о каких криптографических дефектах в A5/2.

Чтобы обеспечить перехват и дешифрование GSM-трафика, отмечает Лаки Грин, было бы достаточно скомпрометировать эффективную длину ключа. Было бы достаточно скомпрометировать алгоритм генерации ключа. Было бы достаточно скомпрометировать алгоритм шифрования. Но спецслужбы сделали все три эти вещи. Такое можно назвать лишь «хорошо

продуманной гарантированно избыточной компрометацией».

И, наконец, еще один очень существенный нюанс. Все шифрование разговоров в системе GSM осуществляется только на канале между мобильным телефоном и базовой станцией, то есть в «эфирной» части передачи. При наличии санкции суда на прослушивание звонков правоохранительные органы всегда имеют возможность подключиться непосредственно к базовым станциям, где уже нет никакого шифрования. Так что единственной причиной для тотального ослабления криптозащиты оказывается «нелегальный» доступ без каких бы то ни было ордеров и санкций.

Вскрытие A5/1

Вскоре, в декабре 1999 г., под натиском университетских криптографов пал, можно считать, и самый сильный элемент в защите GSM – алгоритм шифрования A5/1. Израильские математики Ади Шамир и Алекс Бирюков (чуть позже к ним присоединился американец Дэвид Вагнер) опубликовали работу, в которой описан созданный ими весьма нетривиальный, но по теоретическим расчетам весьма эффективный метод вскрытия A5/1.

Ади Шамира вполне заслуженно называют «патриархом израильской академической криптографии». Еще в 1977 году, работая в США совместно с Рональдом Райвестом и Леонардом Адлеманом, Шамир участвовал в создании знаменитой криптосхемы с открытым ключом RSA (здесь «S» – это Shamir). В 80-е годы им разработано несколько криптографических протоколов и криптосхем. На рубеже 1980-1990-х, работая совместно с Эли Бихамом, Шамир создал метод дифференциального криптоанализа, в открытом академическом сообществе ставший основой практически всех современных методов исследования и вскрытия блочных шифров (подобные работы спецслужб ведутся в строжайшем секрете). Совместный же с Бирюковым криптоанализ A5/1 стал, похоже, первым обращением Шамира к исследованию поточных шифров на основе регистров сдвига – класса схем, более характерных для военной, а не коммерческой криптографии.

Характеризуя изобретенный метод вскрытия A5, Шамир выразился так: «Это весьма сложная идея, реализуя которую мы наступаем на многих фронтах, чтобы накопить несколько небольших преимуществ, но сложенные все вместе они дают большой выигрыш». Если чуть более подробно, то новый метод атаки использует тонкие слабости в структуре регистров сдвига, необратимый механизм их движения, а также частые перезагрузки регистров, применяемые в GSM. Развивая потенциал балансировки «время-память», ученые создали два родственных вида атак, реализуемых на персональном компьютере с увеличенным объемом внешней памяти. Для успеха первой атаки требуется выходная последовательность алгоритма A5/1 в течение первых двух минут разговора – тогда ключ вычисляется всего за секунду (но в реальных условиях получить для анализа эти две минуты крайне проблематично). Вторая атака требует выход A5/1 всего за две секунды, но на вычисление ключа тогда затрачивается несколько больше времени – несколько минут.

Все расчеты были подтверждены реальными вычислительными экспериментами. Попутно следует отметить, что факт реальной длины ключа не в 64, а лишь в 54 бита криптографами не использовался.

Теперь будем делать по-другому?

К началу 2000-х годов уже почти все эксперты в области защиты информации (спецслужбы, как обычно, воздерживаются от комментариев) сошлись во мнении, что разработка мер безопасности для широко используемых систем в тайне от общественности – это в корне порочный путь. Единственный способ гарантировать надежную безопасность – это честно дать возможность проанализировать систему защиты всему сообществу специалистов.

Поначалу создалось впечатление, что данную истину (хотя бы отчасти) признали и в консорциуме GSM. Процитированный в самом начале главы Джеймс Моран, ведающий безопасностью GSM, прокомментировал вскрытие всех криптоалгоритмов системы так: «Когда эти шифры разрабатывались в 1989 году, широкая публикация алгоритмов не была распространенным подходом. Однако, создаваемые ныне алгоритмы будут опубликованы для предварительного их изучения» [DM99].

Летом 2002 года, когда появилось широко анонсированное известие о введении в систему GSM нового криптоалгоритма A5/3, могло показаться, что обещания открытого процесса обсуждения действительно выполняются [NR02]. Про этот реально качественный алгоритм сообществу криптографов академии и индустрии было известно практически все – фактически, это алгоритм Kasumi, созданный рабочей группой 3GPP (3rd Generation Partnership Project) для сетей мобильной связи следующего, третьего поколения. Шифр Kasumi, в свою очередь, построен на основе сильного, еще в 1990-е годы всесторонне исследованного криптоалгоритма MISTY известного японского криптографа Мицуро Мацуи…

Но на этом вся открытость, похоже, и закончилась. Новая спецификация в GSM, именуемая GPRS и обеспечивающая длительное подключение мобильного телефона к Интернету, имеет в своем арсенале новое семейство криптоалгоритмов под общим названием GEA. Про конструкцию этих шифров, по сути дела, известно лишь то, что они не имеют никакого отношения к алгоритмам A5/1 и A5/2. Да еще изменен порядок классификации: GEAO – никакого шифрования (одни нули), GEA1 – экспортный (ослабленный) вариант, GEA2 – обычная стойкость, GEA3 – фактически, тот же вариант, что A5/3. Про стойкость GEA1 и GEA2 неизвестно ничего, поскольку по состоянию на конец 2003 года никто их в открытом сообществе криптографов не видел [GR03].

Тот же принцип сокрытия информации консорциум GSM сохранил и в отношении новых версий алгоритма COMF128 (практической реализации A3-A8 в SIM-модулях). Известно лишь то, что имеются две версии секретного алгоритма под названиями COMF128-2 и COMF128-3, призванные решить проблемы, выявленные в первой, вскрытой версии. В частности, COMF128-3 уже не делает принудительное обнуление 10 битов в сеансовом ключе [FQ03].

Так что в целом, как можно видеть, ситуация с «безопасностью

по-страусиному» практически не изменилась.

Тяжелое наследие

В период с 2000 по середину 2003 года сколь-нибудь серьезных происшествий в области дальнейшей компрометации GSM более не происходило. Точнее, кое-что, конечно, случалось – вспомним, например, «моментальное» клонирование SIM-карты в IBM – но в прессу и широкое публичное обсуждение эти новости уже не просачивались, оставаясь в материалах и кулуарах научных конференций. Однако к лету 2003 года группа израильских криптографов из института Technion – Элад Баркан, Эли Бихам и Натан Келлер – отыскала серьезнейшую, неведомую прежде слабость в системе защиты GSM. В подготовленной авторами работе, «Мгновенное вскрытие защищенных коммуникаций GSM только по шифртексту» [BBO3], было показано, что эту брешь можно весьма эффективно эксплуатировать для проведения реальных атак самого разного рода – от прослушивания открытых и шифрованных разговоров до подделки SMS (коротких текстовых сообщений) или динамического клонирования телефонов жертв, т.е. звонков якобы с номера жертвы.

В соответствии с традицией, публичное представление этой работы научному сообществу было сделано на одном из форумов – в рамках августовской международной конференции CRYPTO-2003 в Санта-Барбаре. Профессионалы-криптографы прореагировали на доклад с огромным интересом (по словам ветерана Бихама, «были удивление, шок, потом поздравления» в связи с получением неожиданного результата). А в прессе при этом – абсолютно ничего, ни единого упоминания о столь значительной работе. На подобных примерах наиболее отчетливо видно, сколь эффективно и мощно власти способны контролировать «свободную» прессу, если хотят удержать какую-либо информацию в сокрытии. Но тот же пример одновременно наглядно демонстрирует, что «всех обманывать можно лишь какое-то время».

Спустя примерно две недели известие все же прошло в локальной израильской прессе, оттуда попало в Интернет, после чего его донесли миру агентство Reuters и все остальные СМИ. В самом кратком изложении суть результатов Баркана, Бихама и Келлера сводится к следующему.

1. Алгоритм A5/2 очень легко вскрывается еще до начала собственно телефонных разговоров – на этапе звонка вызова. Причем делается это на основе лишь пассивного прослушивания линии. Это возможно по той причине, что в GSM код исправления ошибок применяется к сигналу до шифрования. Но этот код, защищающий сигнал от возможных ошибок и искажений, вносит в сигнал очень большую избыточность, благодаря чему нужные для вскрытия ключа данные становятся известны подслушивающей стороне уже на стадии вызова.

2. Все другие шифрованные звонки по GSM (включая применение более сильных алгоритмов A5/1 или A5/3) можно вскрывать, применяя активную атаку. Здесь используется дефект в протоколе: процесс генерации сеансового ключа не зависит от того, какой выбран алгоритм засекречивания, сильный или слабый. Поэтому становится возможным сначала организовать атаку с вынуждением жертвы применить слабый

шифр A5/2, узнать благодаря этому внутренний секретный ключ телефона, а впоследствии этот же самый ключ будет применяться в шифрованных звонках с сильным криптоалгоритмом A5/1 или A5/3. Злоумышленник может записать эти разговоры, а затем их расшифровать, используя вскрытый через A5/2 ключ.

Израильские криптографы, надо подчеркнуть, прекрасно понимая всю серьезность полученных ими результатов, задолго до публикации известили консорциум GSM о выявленной слабости. Но деланно равнодушная и демонстративно незаинтересованная реакция со стороны «Ассоциации GSM», судя по всему, оказалась для Бихама и его коллег полной неожиданностью. В официальном заявлении консорциума очень сдержанно признали, что новый метод взлома действительно «идет дальше предыдущих академических статей, однако не содержит в себе ничего нового или удивительного для сообщества GSM; Ассоциация GSM полагает, что практические следствия данной статьи ограничены, а недавний апгрейд криптоалгоритма A5/2, доступный с июля 2002 года, направлен на то, чтобы закрыть брешь в безопасности, выявленную израильскими учеными» [JW03].

Сами израильские ученые, в частности Бихам категорически не согласны с выводами Ассоциации. Слова же про то, что апгрейд A5/2 закроет выявленную брешь, вообще расцениваются как ввод общественности в заблуждение (поскольку при апгрейде старый алгоритм тоже приходится оставлять в телефоне в целях обеспечения совместимости, а значит он продолжает играть роль «черного хода»).

Но почему же новость об этом взломе все-таки прорвалась в центральные средства массовой информации после двух недель дружного и полного замалчивания? Этого, естественно, не объяснил никто, но кое-какие разумные соображения на данный счет все же выдвинуты. С подачи агентства Reuters, первым запустившим шар, практически всякое новостное сообщение об исследовательской работе израильтян заканчивалось примерно такими словами: «И Эли Бихам, и Ассоциация GSM говорят, что выявленная проблема никак не касается мобильных телефонов третьего поколения, поскольку в системе 3G разработчики радикально сменили алгоритм шифрования и протоколы безопасности». Следовательно – появился замечательный стимул к переходу на новую, более продвинутую (и дорогую) систему. Денег-то уже вбуханы миллиарды, а публика окупать их что-то совсем не торопится.

Бизнес, конечно, дело хорошее. Да и новые технологии – вещь замечательная. Вот если б врали народу еще поменьше…

Глава 6. Охота за людьми и машинами

Страницы жизни героя, 1942. Звериные клетки и электрический стул

Летом 1942 года на долю Эдгара Гувера выпала редкостная удача. Получилось родить одну из тех наиболее героических и насквозь фальшивых историй, что заложены в основу мифа о всеведении и

несокрушимости гуверовского ФБР. Начиналось же все достаточно серьезно и тревожно, когда у берегов острова Лонг-Айленд немецкая субмарина высадила диверсионную группу из четырех человек, снабженных деньгами, оружием, взрывчаткой и планами террористических актов на заводах, производивших важную военную продукцию. Патрульный службы Береговой охраны, наткнувшийся на четырех подозрительных мужчин с плотом, не стал поднимать тревогу, поскольку те представились заплутавшими рыбаками, да еще дали ему денег, чтоб не было неприятностей. Отпустив «рыбаков», патрульный все же решил подстраховаться и доложил-таки о своих подозрениях начальству.

Когда о происшествии на следующий день узнало ФБР, Береговая охрана уже нашла у места высадки довольно небрежно устроенный тайник со взрывчаткой и другим снаряжением. Однако сами диверсанты бесследно исчезли. Гувера происшествие чрезвычайно возбудило и встревожило, поскольку дело пахло угрозой диверсионных актов, а быть может и подготовкой военного вторжения. Он приказал сохранить инцидент в полнейшей тайне от прессы и объявил самую крупномасштабную облаву за всю историю ФБР.

Чем бы закончилась эта большая охота, сказать трудно, поскольку четверо диверсантов уже рассредоточились и поселились в разных отелях огромного Нью-Йорка. Однако дальнейшие действия группы пошли совсем не по плану, поскольку ее руководитель, тридцатидевятилетний Георг Даш, до войны много лет проживший в США, был абсолютно не расположен к выполнению диверсионных задач. Об этом он рассказал своему ближайшему партнеру-приятелю по группе Эрнсту Бергеру, который тоже был не прочь тихо рассосаться в большой стране, поделив 84 тысячи долларов, полученные от германского военного командования.

Но Даш выбрал иной путь, позвонив в местное нью-йоркское отделение ФБР и сообщив, что только что прибыл из Германии и хотел бы передать господину Гуверу чрезвычайно ценную информацию. Когда Вашингтон уведомили о звонке, Даш сам отправился в столицу и сдался вместе со всей кассой. Помимо большой суммы денег ФБР получило в лице Даша ценный источник информации о составе и местах проживания остальных членов группы (Даш предупредил, что действовал с ведома Бергера), о составе и месте высадки другой диверсионной группы у берегов Флориды, о главных целях диверсионных актов и вообще о подготовке диверсантов в Германии. На основе полученных данных ФБР быстро арестовало всех семерых коллег Даша, а ему самому настоятельно порекомендовали признать себя на суде виновным и помалкивать о добровольной сдаче американским властям. В обмен же за молчание было обещано, что уже через несколько месяцев добрый президент Рузвельт его амнистирует и выпустит на свободу. Даш все сделал так, как ему велели, за что едва не поплатился головой.

На самом деле президент Рузвельт вовсе не был добрым, а уж после Перл-Харбора так вообще начал лютовать, особенно в отношении японцев и немцев. Во всех предоставленных ему докладах от разведывательно-аналитических служб был сделан вывод, что живущие на Западном побережье США японские американцы не представляют никакой угрозы государству. Тем не менее, Рузвельт настоял на интернировании в

концлагеря 114 тысяч мужчин, женщин и детей японского происхождения – этого хотела жаждущая мести публика. Когда же пришло известие о поимке доблестным ФБР восьми немецких шпионов-диверсантов, то поначалу Рузвельт хотел посадить их в звериные клетки и, провезя в таком виде по всей стране, затем казнить. Тогдашний министр юстиции Фрэнсис Биддл в своих возражениях указывал, что никаких актов шпионажа или диверсий в действительности не было, однако Рузвельт настаивал на смертной казни. Биддл предупредил, что в подобных обстоятельствах ни один гражданский суд не сможет вынести столь суровый приговор. Тогда президент отправил шпионов под военный трибунал [JP01].

Для Гувера было чрезвычайно важно, чтобы в глазах американского общества вся заслуга в поимке шпионов принадлежала ФБР, а Германия ничего не узнала о предательстве Даша. Поэтому самые существенные подробности данной истории были тщательно сокрыты даже от военного суда. Лично сопровождая ход дела, Эдгар Гувер регулярно присутствовал на заседаниях трибунала, тщательно следя, чтобы не просочилось никакой лишней информации. Как вспоминал впоследствии член военного трибунала Ллойд Катлер, в 1970-е годы советник президента Картера, они получили к разбирательству дело, «целиком подготовленное в ФБР, причем Гувер держал нас на расстоянии от своих агентов».

В итоге все 8 диверсантов были приговорены к смертной казни, причем Гувер потребовал, чтобы казнили их как можно быстрее, лично организовав исполнение приговора. Вскоре шестерых посадили на электрический стул. Георга Даша и Эрнста Бергера все же оставили в живых, заменив смертную казнь на длительные сроки тюремного заключения. Вместо обещанной амнистии Даша продержали в тюрьме пять лет, но и после этого не выпустили на свободу, а принудительно депортировали из США.

А Эдгар Гувер и три десятка лет спустя все еще любил вспоминать об этом деле, как об одном из «самых важных своих достижений». Эта фабрикация настолько глубоко впечаталась в историю ФБР, что уже после смерти Гувера, в 1979 году в холле Министерства юстиции установили мемориальную бронзовую доску в честь столь выдающегося события. На долгую, как говорится, память.

Действительно, есть что вспомнить.

Ловля рыбы в волнах бури

Выявление мыслепреступлений

Если основную часть американской нации трагические события 11 сентября 2001 года повергли в состояние шока, то отдельные персонажи, напротив, пришли в состояние повышенного возбуждения, поскольку усмотрели в атаках террористов невероятно удачный шанс для раскрутки своего бизнеса. Так, коммерсант-нейрофизиолог Лоуренс Фаруэл из г. Айова, владеющий небольшой фирмой Brain Wave Science [http://www.brainwavescience.com], тут же, не мешкая, ринулся трубить на всех перекрестках, что разработанное им оборудование для измерения

мозговой активности – это именно то, что нужно ФБР и всем правоохранительным органам для отлова злоумышленников.

Нынешний бизнес Фаруэла родился из научной статьи «Отпечатки мозга», в начале 1990-х опубликованной им в журнале «Психофизиология» в соавторстве с учителем, профессором Имануилом Дончином [FD91]. Но если Дончин по сию пору продолжает настаивать, что полученные в работе результаты являлись лишь демонстрацией концепции и требовали обширных дополнительных исследований для применения в реальных приложениях, то Фаруэлл решил иначе – «куй железо пока горячо».

На основе исходных экспериментов ученый разработал своего рода «детектор лжи» – специальный криминалистический тест с целью установления, известна подозреваемому интересующая следствие информация или нет. Для этого испытуемому надевается на голову повязка с электродами, регистрирующими волны электромагнитной активности мозга. На компьютерном экране, установленном перед «пациентом», начинают демонстрировать разного рода специально подобранные картинки, и когда мозг «узнает» тот или иной образ, то генерируется определенного рода волна, именуемая у специалистов «реакция РЗОО». Разработанный Фаруэлом алгоритм для анализа формы РЗОО позволяет с высокой вероятностью делать заключение, опознал мозг испытуемого улики или нет. Например, для отыскания действительных сообщников терактов 9/11 среди более чем 700 подозреваемых Фаруэл предложил протестировать их на своем приборе, который будет демонстрировать, скажем, название организации «Аль-Каида» на арабском языке или приборную панель «Боинга-757» [JS01].

Аппаратура Фаруэла для снятия «отпечатков мозга» уже несколько лет испытывается ФБР и полицией ряда штатов в реальных расследованиях, однако, как настаивают критически относящиеся к технологии ученые, всецело полагаться на показания прибора было бы слишком опрометчиво. Например, хорошо известно, что люди с психопатическими наклонностями часто дают неадекватную реакцию РЗОО, массу нюансов в реакцию вносят раса, пол и возраст испытуемых, а человек эрудированный и образованный всегда распознает намного больше предметов и слов, чем невежественный. В интерпретации формы волны важнейшим остается субъективный фактор личности конкретного эксперта, да и многолетняя практика использования «детекторов лжи» свидетельствует, что при соответствующей подготовке подобные приборы вполне можно обманывать. Но Фаруэл напрочь отметает все эти аргументы, настаивая, что его аппаратура абсолютно надежна и «ради национальных интересов чрезвычайно важно внедрить ее как можно быстрее».

Неудивительно, что в поддержку напористого ученого-бизнесмена уже выступили и другие «патриотично настроенные» компании, усмотревшие в технологии перспективы и для себя. Так, целую программу [KI01] по общенациональному снятию «отпечатков мозга» выдвинул Стив Кирш, в прошлом основатель поискового сервиса InfoSeek, а ныне глава Propel Software – фирмы, разрабатывающей программное обеспечение для управления большими массивами данных. По мнению Кирша, нет более надежной защиты от террористов, чем регулярное (раз в два-три года)

сканирование мозга всех граждан с хранением отпечатков в общенациональной базе данных. Тогда при покупке билета на самолет, посещении массовых зрелищ или еще каких мероприятий, потенциально таящих опасность, каждого человека можно будет быстренько проверить на «склонность к преступлению» и на основании формы электромагнитного импульса-отклика допустить или же отказать… [TC01].

Звучат, конечно, столь странные идеи, как полнейшая антиутопия в духе Оруэлла, однако предлагаются эти меры абсолютно всерьез, причем вполне адекватными в других отношениях людьми. Более того, журнал Time [TM01] настолько проникся идеями и перспективами «отпечатков мозга», что назвал доктора Лоуренса Фаруэла одним из 100 самых ярких новаторов на этой планете, обещающих стать «Эйнштейнами и Пикассо XXI века». Светлую надежду на фоне столь тоскливых перспектив человечества вселяет лишь то, что все сообщения СМИ о блестящем творчестве Фаруэла, любовно собранные на сайте его компании, датируются 2001 годом. Похоже, перевозбужденные мозги журналистов с той поры несколько поостыли.

В спецслужбах, где обычно работают люди с более холодной (и циничной) головой, к новой технологии детектора лжи относятся сугубо прагматично. Работы Brain Wave Science отчасти финансирует ЦРУ, в дирекцию фирмы вошел один из бывших руководящих чинов ФБР, и, судя по публикациям после сентября 2001 года, власти США действительно рассматривали возможности приобретения этой аппаратуры [FW03]. Главной же причиной отказа от технологии снятия отпечатков мозга стала невозможность автоматизации процесса тестирования, а значит – необходимость наличия всякий раз опытного эксперта, от субъективных оценок которого напрямую зависит исход любой «проверки на лживость». Для повсеместного применения такой подход явно не годится.

Мужчины с ошеломительным оснащением

В безбрежном море научно-исследовательских публикаций, посвященных технологиям связи и компьютерной обработки информации, время от времени появляются любопытные статьи, существенно раздвигающие представления общества о шпионских возможностях современной техники. Нельзя сказать, что происходит это часто, но вот в начале 2002 г., к примеру, в Интернете были опубликованы сразу две новые работы, в которых эффектно продемонстрированы неизвестные прежде методы дистанционного съема информации с экранов мониторов и другого компьютерного оборудования.

В первой из этих работ германский ученый Маркус Кун, работающий в Кембриджском университете, показал, что имеется принципиальная возможность с расстояния в несколько сотен метров восстанавливать картинку экрана просто по мерцанию света в окне комнаты, где установлен монитор или телевизор. Все, что для этого требуется, – это качественный светочувствительный датчик, хорошая оптика и знание тонкостей работы электронно-лучевых трубок [MK02].

Другой ученый-исследователь, американец Джо Лоухри, продемонстрировал, что с помощью той же примерно техники – подзорной

трубы и хорошего светового сенсора – на расстоянии до полутора километров можно снимать данные с постоянно мигающих индикационных лампочек компьютерного оборудования. Выяснилось, что в модемах, к примеру, подключающих компьютер к Сети, мигание индикатора-светодиода в точности соответствует битам проходящей через аппарат информации [LU02].

«Новаторскими» упомянутые выше статьи можно считать лишь по той причине, что подготовлены они исследователями открытого академического сообщества, которое прежде не было знакомо с подобного рода «оптическими» атаками. Что же касается закрытых работ, ведущихся в данной области государственными структурами, то все публикации здесь являются строжайше засекреченными как «представляющие угрозу национальной безопасности страны».

Несмотря на это, к настоящему времени уже прекрасно известно, что США и их ближайшие союзники еще в 1950-е годы всерьез озаботились проблемой компрометирующих излучений, обеспечивающих утечку информации по электромагнитным и акустическим волнам, сопровождающим работу связного оборудования и компьютеров. Секретная американская программа по защите техники от подобных утечек получила кодовое наименование Tempest (Буря), а со временем этим же «бурным» словом стали обозначать и все исследования как по экранированию собственной аппаратуры, так и по методам доступа к чужой компрометирующей информации. (Впрочем, относительно двойного оборонительно-наступательного смысла термина среди экспертов имеются значительные расхождения. Также как и о том, является ли Tempest просто кодовым словом или же краткой аббревиатурой более длинного названия. Одна из наиболее вдохновенных расшифровок аббревиатуры TEMPEST, кстати говоря, выглядит так: Tremendously Endowed Men Performing Exciting Sexual Techniques, т.е. «Мужчины с ошеломительным оснащением, демонстрирующие захватывающую сексуальную технику». Этот перл позаимствован с сайта [JM96] Джоэла Макнамары «Информационная страница о TEMPEST», слывущего наиболее содержательным в Интернете собранием открытой информации по данной тематике. Удачным дополнением к нему служит компилятивная веб-страница [TL02] «Хронология Tempest» на сайте Cryptome.org).

О темпест-разработках, ведущихся за высокими стенами спецслужб, известно крайне мало. Но и получившие огласку факты выглядят весьма впечатляюще. В 1987 году, несмотря на яростное сопротивление британского правительства, в Австралии вышла книга «Ловец шпионов» с мемуарами Питера Райта, высокопоставленного сотрудника английской контрразведки MI5.

Райт среди прочего описал в своих воспоминаниях и несколько весьма успешных темпест-атак, проведенных MI5 в 1950-1960-е годы. В 1956 г., в ходе одной из операций (Engulf) чувствительные микрофоны, тайно установленные в посольстве Египта в Лондоне, позволили англичанам по звукам механического шифратора Hagelin получить доступ к секретной дипломатической переписке арабов в период суэцкого кризиса. В ходе другой, еще более изощренной операции Stockade, ученые MI5 проанализировали записи шифрованной телеграфной переписки между

французским посольством в Лондоне и МИДом в Париже, обнаружив в сильном основном сигнале еще один, вторичный. Когда сконструировали оборудование для выделения слабого вторичного сигнала, то выяснилось, что это был открытый текст телеграмм, который каким-то образом просачивался через шифратор в линию… [PW87].

Интересно, что академическое сообщество ученых впервые близко познакомилось с проблемой компрометирующих электромагнитных утечек буквально накануне публикации книги Райта. Это произошло в 1985 году, когда голландский инженер-компьютерщик Вим ван Экк, занимавшийся медицинской техникой, самостоятельно переоткрыл, что с помощью телевизора, антенны и вручную настраиваемого генератора синхроимпульсов можно дистанционно восстанавливать изображение другого видеодисплея [WE85].

Несмотря на большой резонанс, произведенный работой ван Экка в научном мире, последующих темпест-исследований в академической среде было очень мало. Причин тому множество: затраты средств требуются весьма существенные; специальная литература и справочники если и имеются, то засекречены; государств, заинтересованных в поддержке публичных работ подобного рода, практически нет.

При этом следует отметить, что на бытовом, так сказать, уровне темпест-аппаратура властей, напротив, начинает все больше входить в повседневную жизнь. Например, в Великобритании и других странах с обязательным лицензированием телевизионных приемников по улицам ездят автофургоны с «ТВ-детектором», позволяющим дистанционно определить, пользуются ли в доме телевизором на законном основании и какие конкретно каналы с его помощью смотрят [КА98].

В США полиция прибегает к другой идейно родственной технике – тепловизорам, позволяющим без проникновения в дом поинтересоваться, чем там за стенами занимаются жильцы. Например, таким методом по мощному инфракрасному излучению ламп обогрева выявляют «ботаников-надомников», питающих слабость к марихуане и выращивающих запрещенную американскими законами коноплю в домашних мини-оранжереях [TG01].

Что же касается мощнейших технологических возможностей разведывательных служб США, то с некоторых пор они вызывают серьезные опасения даже в традиционно союзных Америке странах Западной Европы. Причины тому разобраны в предыдущем разделе книги – существует масса свидетельств, что военно-политическая разведка США регулярно занимается откровенным экономическим шпионажем в пользу компаний американской индустрии. Дело дошло даже до того, что в 1998 году начальник шведской контрразведки SEPO Андрее Эриксон публично предупредил граждан страны, чтобы они не брали мобильные телефоны на те деловые встречи, где обсуждается конфиденциальная информация. По свидетельству Эриксона, все сотовые телефоны можно использовать для подслушивания даже тогда, когда они находятся в нерабочем состоянии. Глава SEPO тут же подчеркнул, что не будет вдаваться в подробности, как именно это делается [RS98].

Фрагменты официальных американских документов по Tempest-тематике, добытые правозащитниками через закон FOIA (о праве

граждан на доступ к информации) и опубликованные в Интернете, дают представление о том, сколь тщательно охраняются секреты подобных технологий. В одной из инструкций, затрагивающей «методы Nonstop/Hijack» (кодовые слова для обозначения техники подслушивания с помощью работающего по соседству аналогового/цифрового электронного оборудования вроде приемника, магнитолы или сотового телефона), сказано буквально следующее: «Следует отметить, что даже НЕСЕКРЕТНАЯ информация, касающаяся NONSTOP, не должна обсуждаться или предоставляться людям без служебной необходимости. Никакая информация, касающаяся NONSTOP, не должна становиться доступной публике через прессу, рекламу, радио, ТВ и другие средства массовой информации» [EM75].

Если принять во внимание, что методами NONSTOP спецслужбы занимаются по меньшей мере с 1960 годов, а об их подробностях публике ничего не известно и поныне, то можно быть уверенным: прогресс технологий сулит нам еще немало интереснейших открытий. Как впереди, так и позади.

Тотальный локатор

Все ходы записаны

В сентябре 2003 года вступила в силу директива Европейского Союза, именуемая E112 и требующая, чтобы сети мобильной связи обеспечивали службы спасения любой имеющейся у них информацией о географическом местоположении телефона, с которого делается вызов [DG03]. Понятно, что точное знание спасателями места, откуда сделан вызов, во многих случаях ускоряет прибытие помощи и помогает сохранить людям здоровье или даже жизнь. Характерно, что несколько раньше директивы E112 в Германии, Британии и других европейских странах начали появляться коммерческие сервисы, предлагающие клиентам разнообразные услуги вокруг отыскания местоположения интересующего объекта – человека с известным номером мобильного телефона, адрес ближайшего банкомата, китайского ресторана или кинотеатра.

На этом основании у публики могло появиться ощущение, что в технологиях мобильной сотовой связи сделано очередное важное достижение, благодаря которому телефонные операторы теперь могут предложить новые интересные услуги. В действительности дела обстоят существенно иначе, ибо возможности географической локализации абонента изначально заложены в саму архитектуру мобильной сотовой связи. Просто потому, что для эффективной организации соединения сеть должна знать, в какой из ее ячеек находится всякий конкретный телефон. Делается это известными в навигации методами триангуляции – по времени отклика аппарата на сигналы трех-четырех ближайших мачт базовых станций. Более того, информация о перемещениях каждого абонента из одной ячейки в другую не только регулярно фиксируется, но и довольно долго хранится в базах данных телефонных операторов. Однако, многие годы все это было большим секретом, поскольку технология

предоставляла спецслужбам и правоохранительным органам удобнейший инструмент для совершенно незаметного наблюдения за интересующими их объектами.

Наиболее громкий скандал в связи с негласной слежкой за гражданами с помощью системы GSM разразился в 1997 году, когда цюрихская газета Sonntags Zeitung рассказала о том, как швейцарская полиция тайно следит за перемещениями пользователей мобильных телефонов с помощью компьютера национальной телекоммуникационной компании Swisscom. Естественно, в разоблачительном угаре журналисты слегка приврали, когда выстраивали сильные фразы примерно такого рода: «В Swisscom хранят данные о передвижениях более миллиона пользователей мобильной связи и могут восстановить местоположение всех абонентов с точностью до сотни метров на протяжении по крайней мере последнего полугода… И если понадобится, они могут в точности воссоздать, вплоть до минуты, кто, где, когда и с кем созванивался для конфиденциальных переговоров».

Несмотря на очевидные преувеличения прессы, представители Swisscom официально признали, что практикуют сбор и хранение информации о перемещениях абонентов, но выдают ее властям лишь по соответствующему ордеру суда. А один из цюрихских следователей, специализирующийся на борьбе с организованной преступностью, подтвердил, что данная компьютерная система – «это очень эффективный инструмент при расследованиях».

Но, с другой стороны, нет (да и не должно быть) в демократических странах «законов, которые допускали бы превентивный сбор данных в целях будущих расследований». Именно в таком виде сформулировал обозначившуюся проблему Одило фон Гунтерн, глава швейцарской Федеральной комиссии по защите данных, который был вынужден начать специальное расследование в связи со скандальной публикацией цюрихской газеты. Результаты его расследования, частично опубликованные летом 1998 года, с одной стороны подтвердили суть утверждений «Зонntагс Цайтунг», а с другой – сняли вину с компании Swisscom в покушении на приватность граждан. Как сказано в сухом докладе Гунтерна, «компания собирает лишь те данные, что требуются ей для организации телефонных соединений или же для составления счетов к оплате». Критике компания подверглась лишь за то, что «слишком долго хранит данные и ограничивает для клиентов доступ к информацию об этих данных». Но при этом в прессе опубликованы были лишь три страницы выдержек из доклада Гунтерна, а в целом данный 30-страничный документ получил статус «конфиденциального» и широкая общественность его не увидела [RB98].

Был, правда, в Швейцарии другой, менее официальный источник информации о широком использовании мобильной телефонии для слежки за людьми. Весьма обширный веб-сайт «Interception» («Перехват»), посвященный шпионским аспектам мобильной связи, вел живший в Лозанне французский правозащитник Кристиан Массой. В мае 1999 г. при крайне загадочных обстоятельствах Массой погиб, упав с моста [Ш99]. Полиция квалифицировала произошедшее как самоубийство, хотя у родственников и близких на этот счет остались очень сильные сомнения. В

память о Массоне его веб-сайт сохранили друзья по адресу www.seriot.ch/interception/.

Среди материалов, собранных Массовом, имеется свидетельство дублинской штаб-квартиры GSM, согласно которому постоянное отслеживание перемещений всех мобильных телефонов осуществляется ради обеспечения наиболее эффективных соединений. Причем даже если человек выключает свой телефон, не желая постоянно фигурировать в базах данных, которые ему абсолютно неподконтрольны, практически никакого эффекта это не возымеет. Потому что и в выключенном состоянии мобильный телефон регулярно подает о себе сигнал базовой станции. Так что если абонент категорически не желает постоянно находиться под наблюдением, ему придется вынуть из аппарата батарейку или засунуть телефон в пакет/контейнер, экранирующий электромагнитные излучения. На сайте Массона составлена обширная таблица об особенностях работы фирм-провайдеров мобильной связи и о том, как долго каждая из компаний хранит данные о перемещениях своих абонентов. Сроки эти для различных компаний могут быть очень разными – от нескольких дней до нескольких месяцев [CM99]. Но суть накапливаемых данных одна: на их основе для любого конкретного номера и его владельца имеется возможность выстроить «профиль» с точными датами и временем всех перемещений на местности.

То же самое, но за деньги

К началу 2000-х годов мощные локационные способности сетей мобильной связи перестали быть секретом, а значит компаниям-провайдерам стало можно делать на этом реальные деньги. Естественно, без конфузов новое и довольно щекотливое в вопросах приватности дело обойтись не могло. Вот, к примеру, недавние истории из биографии небольшой софтверной фирмы GateS (www.gateS.de) в Берлине, специализирующейся на разработке программного обеспечения для онлайновых сервисов с определением местоположения абонентов мобильной связи. В конце 2001 года GateS, дабы привлечь побольше внимания со стороны клиентов, разместила на своем веб-сайте приложение, позволяющее всем желающим узнать, включен или выключен в данное время интересующий их телефон. Причем делалось это без какого-либо уведомления владельца «прощупываемого» мобильника [RP01].

Этот невинный, на первый взгляд, демонстрационный сервис, реализующий на базе кратких текстовых посланий (SMS) функцию известной сетевой программы PING, не только очень быстро набрал популярность среди пользователей (поскольку срабатывал от Англии до Австралии), но и навлек на GateS целую волну крайне неприятной критики со стороны специалистов по безопасности и защитников приватности. Больше всего их встревожило то, что совсем молодая и никому неизвестная крошечная фирма имеет доступ к сугубо внутренним, неафишируемым возможностям программного обеспечения сетей мобильной связи. Другими словами, в базах данных операторов сотовой связи содержится масса информации весьма деликатного свойства об их

абонентах, а история с GateS показала, что по крайней мере к части этих данных вполне может получать доступ чуть ли не любой желающий. Руководство GateS, обеспокоенное таким поворотом событий, наотрез отказалось раскрывать, от кого именно из операторов связи была получена внутренняя документация по SMS, а заодно, как говорится «во избежание», с веб-сайта компании убрали и вызвавший раздражение сервис SMS Gateway Ping [EB01].

Вскоре после этих событий GateS, уже получившая известность, начала продавать операторам мобильной связи полноценный программный продукт People Finder, что на русский язык можно перевести как «Человекоискатель». Суть программы ясна из названия – за приемлемую плату предоставлять абонентам сервис, позволяющий определять текущее географическое местоположение других владельцев сотовых телефонов. Естественно, подразумевается, что и эти другие абоненты не возражают против оказания заказчику подобной услуги. Впрочем, тут все зависит от того, как поставлено дело.

Китайская фирма Pinpoint, внедрившая на рынке Гонконга аналогичную систему, ориентировалась в первую очередь не на индивидуальных клиентов, а на компании, желающие точно знать местоположение своих сотрудников. Согласно грубым оценкам, использование системы локализации на основе сотовых телефонов, получившей в Pinpoint название Workplace («рабочее место»), позволяет компаниям повысить свою продуктивность на 10-15 процентов. При этом расходы на сервис оказываются совсем небольшими – порядка 20 долларов в месяц, поскольку GSM-телефоны есть практически у всех, кто работает ныне в Гонконге. Аккуратность позиционирования Pinpoint Workplace не так высока, как при использовании значительно более дорогой спутниковой системы GPS, но обычно особая точность и не нужна. Локализации с точностью до 100 метров оказывается вполне достаточно, чтобы диспетчеру определить на электронной карте города работников, ближе всего находящихся к очередному клиенту, сделавшему запрос на обслуживание. Сами сотрудники компаний, посаженные на «короткий поводок», особого восторга по поводу нововведения не выражают, но и организованных акций протеста не отмечается – работа есть работа.

Фирма Pinpoint же, обнадеженная удачным стартом, тут же подготовила новую систему Safety Walker, на этот раз для индивидуального отслеживания местоположения тех, кто может потеряться – детей, престарелых родственников и т.д., насколько хватит фантазии. В отличие от Workplace этот сервис уже нельзя отключить простым нажатием кнопки [AB02].

Несколько иначе, нежели в густонаселенных Европе или Гонконге (плотно накрытых сетью базовых станций GSM), обстоят дела с технологией точной локализации абонентов в США. Здесь федеральные власти еще в 1996 году обязали всех операторов мобильной связи внедрить в свои сети такие возможности, которые тоже позволяли бы отыскивать владельца телефона с точностью до 50-100 метров. Поскольку в первую очередь эта директива привязывалась к потребностям службы спасения «911», технология получила условное название E911 (от Enhanced, т.е. «продвинутая»), но не секрет, что сильную

заинтересованность в расширении возможностей связи проявляют полиция и прочие силовые структуры.

Главная же проблема заключается в значительных территориальных пространствах Америки. «Требование о 100 м» без проблем удовлетворяется в городах, но в сельской местности, где плотность мачт намного меньше, такая точность локализации все еще недостижима. Как правило, абонента с телефоном здесь «видят» не три-четыре, а в лучшем случае лишь две мачты, расположенные в нескольких милях друг от друга. В подобных условиях – пока не развернуто в достатке базовых станций – особую актуальность обретают удешевление и миниатюризация технологии GPS [ВС02].

Движущиеся мишени

Устройства GPS нередко называют суперсовременной версией обычного компаса – хайтек-прибор не просто показывает направление на север, а с высокой точностью определяет географические координаты своего местоположения. В основе системы лежит прием аппаратом GPS синхросигналов от спутников, оснащенных точнейшими атомными часами. Орбиты двух дюжин спутников построены так, что GPS-приемник в любой точке Земли способен одновременно «видеть» сигналы по меньшей мере от четырех аппаратов. Сравнивая расхождения в сигналах времени от каждого из атомных хронометров, GPS-устройство вычисляет расстояние до каждого из спутников. Используя эти данные, аппарат одновременно может определять не только свое местоположение, но и точное время замера. Чувствительные GPS устройства способны определять координаты на местности с точностью до 15-20 метров, а при определенных условиях – и до 3-5 метров.

Понятно, что эта технология в сочетании с аппаратурой беспроводной мобильной связи несет в себе чрезвычайно заманчивый потенциал для организации постоянного слежения, скажем, за перемещением автомобилей или других транспортных средств. Потенциал этот быстро оценили не только спецслужбы, но и коммерческие фирмы, тоже желающие внедрять GPS «для контроля за ситуацией». Как и со всякой шпионской технологией, вскоре пошли известия о перегибах и судебных разбирательствах.

Наиболее громкое разбирательство, создавшее в США прецедент со злоупотреблением GPS в бизнесе, происходило летом 2001 года в штате Коннектикут. Когда Джеймс Тернер, один из постоянных клиентов местной компании Acme Rent-A-Car, г. Нью-Хейвен, в очередной раз пришел брать напрокат автофургон, администрация фирмы сообщила ему, что теперь все машины оборудованы системой GPS, а в контракте появилась новая строка, согласно которой за каждое превышение скорости 80 миль/час будет дополнительно взиматься 150 долларов. Тернер, естественно, не обратил никакого внимания на нововведение, поскольку брал машину здесь постоянно, а в навигационной системе GPS не нуждался. Но на самом деле Acme оборудовала свои автомобили куда более хитроумной технологией OnBoard компании AMQ (www.airiq.com), которая с помощью GPS позволяет не только следить из центра за всеми перемещениями

машины, но и постоянно отслеживать скорость, а также может заглушить мотор и даже запереть все замки… Так что Джеймс Тернер не успел еще и автофургон вернуть, когда обнаружил, что со счета его кредитной карточки уже снято 450 долларов, поскольку он «трижды превысил допустимую скорость». Компания с готовностью предложила ему даже показать на карте, где именно скорость превышалась [RS01].

Разгневанный Тернер нанял адвоката и решил через суд наказать компанию, столь беззастенчиво вторгающуюся в его личную жизнь. Компания, естественно, стала напирать на то, что все ее действия заблаговременно оговорены в условиях контракта. Дело получило резонанс, к нему подключились не только правозащитные организации, но и высокие судебные инстанции, однако в какую сторону качнется чаша правосудия было совершенно неясно. Ибо масштабы вторжения бизнеса в частную жизнь граждан с помощью глобальных спутниковых систем – дело пока что неурегулированное. Конкретно в коннектикутском деле суд в итоге встал на сторону Тернера, запретив компании Acme Rent-A-Car взимать самовольно установленные штрафы за превышение скорости и обязав ее выплатить обратно деньги всем, кто уже был оштрафован. В применении системы GPS ничего предосудительного не усмотрено, ибо машины – собственность фирмы проката [CB02].

Вызванные техническим прогрессом перемены в «автодорожном» гражданском законодательстве и в работе полиции – это, вообще говоря, отдельная очень большая тема, сильно выходящая за рамки книги. Здесь же имеется возможность упомянуть лишь несколько ярких примеров. Так, с сентября 2002 г. в американском штате Мэриленд вступил в силу новый закон, согласно которому людям, дважды за пять лет уличенным в вождении автомобиля в нетрезвом состоянии, принудительно устанавливают в машину блокиратор зажигания с тестовой трубкой. Это электронное устройство размером с сотовый телефон крепится к приборной панели и дозволяет запуск двигателя лишь в том случае, если водитель проходит тест на безалкогольное дыхание.

При вступлении закона в силу в Мэриленде насчитывалось около 5200 такого рода водителей, склонных к нетрезвой езде, которых обязали выплачивать по 65 долларов в месяц за блокиратор и сопутствующее «обслуживание». Для этого им ежемесячно надлежит являться в один из 26 сервис-центров штата, где из микрокомпьютера-блокиратора выгружается для анализа информация о датах, времени и дальности каждой из поездок за отчетный период. Таким образом выявляются люди, решившие обмануть систему, к примеру, пересев на другую машину. В принципе, любители выпить за рулем имеют право отказаться от столь навязчивого присмотра, но тогда они лишаются водительской лицензии. Мэриленд стал уже 41-м штатом, вводящим за последние годы закон о принудительном блокираторе зажигания, поскольку от этого напрямую зависит дальнейшее поступление денег из федеральной казны на поддержание автострад [DO02].

В том же 2002 году стало известно о новом способе борьбы с угоном автомобилей, который все шире начинает применять американская полиция. Впервые опробованный в Миннеаполисе, шт. Миннесота, этот метод за первый же год понизил количество украденных машин примерно на 30%, а потому берется сейчас на вооружение стражами порядка как в

других штатах, так и в столичном округе Колумбия.

Суть способа предельно проста – не искать уже угнанный автомобиль, а оставлять в привлекательных для воров местах машину-«наживку», на которую преступник непременно клюнет. Марка наживки специально выбирается среди наиболее популярных у профессиональных угонщиков моделей. В 2002 году на территории США это были машины Toyota Camry, Honda Accord и Oldsmobile Cutlass [NI02]. Внутри такой «наживки» монтируется специальное электронное оборудование на сумму около 3 тысяч долларов: аппаратура GPS для постоянного отслеживания местоположения машины, автоматический блокиратор для дистанционного выключения мотора и система беспроводной связи, с помощью которой автомобиль делает звонок в полицию с единственным сообщением «меня опять украли». Техника отлова угонщиков уже отточена. Машины полиции никогда не преследуют вора, чтобы не спровоцировать его на увеличение скорости и аварию с возможными жертвами. Вместо этого мотор машины-«наживки» просто вдруг глохнет где-нибудь в удобном месте и возле нее тут же оказываются несколько полицейских [PD02].

Ушлые адвокаты, защищающие угонщиков в суде, уже неоднократно пытались обвинить полицию в «entrapment», т.е. провоцировании их подопечных на уголовно наказуемое деяние. Однако суд не усматривает в подобных действиях провоцирования, поскольку считает, что чужие машины, стоящие на улице, не угоняются людьми «нечаянно».

Зато в отношениях других действий полиции с применением аппаратуры GPS судебные инстанции США выдают, бывает, значительно более строгие вердикты. Так, в сентябре 2003 г. Верховный суд штата Вашингтон постановил, что полиция не имеет права без получения надлежащей санкции устанавливать следящее устройство GPS в транспортное средство подозреваемого. Практика тайной установки в машину GPS-устройства для постоянного отслеживания перемещений подозреваемых ныне все шире используется полицией и спецслужбами развитых стран, особенно в США и Канаде. Причем делается это, как правило, без получения соответствующего ордера в судебных органах, поскольку полиции удобнее расценивать GPS-закладку в машине как некий хайтек-аналог традиционного сотрудника наружного наблюдения, не обязанного иметь никаких санкций. Однако вашингтонский суд постановил, что полиция никогда не имела возможностей круглосуточно на протяжении недель или месяцев непрерывно следить за перемещениями людей. Поскольку вина этих людей еще не доказана, новые методы слежки представляют слишком серьезное посягательство на тайну личной жизни. По свидетельству правозащитников ACLU, Американского союза за гражданские свободы, подобное решение судебных властей штата стало в этой стране первым, а значит прецедент может иметь серьезные последствия для перемен в законодательстве других регионов США [APO3].

Вполне очевидно, что подобное решение крайне актуально и для всех остальных стран, считающих себя свободными и уважающими принцип презумпции невиновности. Особенно в условиях, когда размеры GPS-аппаратуры становятся совсем миниатюрными и уже в принципе позволяют незаметно встраивать приемопередатчики, фиксирующие свое местоположение, даже в одежду, обувь, сумку или другие личные вещи.

Например, компания Motorola в середине сентября 2003 г. объявила о создания крошечного, размером с 10-центовую монетку GPS-модуля FS Опсоге, способного работать как автономно, так и в комплексе с поддерживающей аппаратурой [DS03]. В принципе, предполагается, что такого рода миниатюрная аппаратура в первую очередь найдет свое место в носимой карманной электронике бытового назначения, вроде сотовых телефонов или КПК. Но также здесь вполне проглядываются богатые возможности для незаметных шпионских закладок или модификации уже существующих устройств несколько иного, тюремно-полицейского рода.

Министерство внутренних дел Великобритании решило перенять богатый опыт своих американских коллег и объявило осенью 2003 г., что скоро отбывшие тюремный срок педофилы по выходе на свободу будут оснащаться электронными метками-маяками. Специальное оборудование на основе GPS разработано английской фирмой Sky Guardian, взявшей за основу аналогичное оборудование фирм США. Там его применяют для тотального отслеживания перемещений условно освобожденных лиц, согласившихся на подобный «поводок».

По свидетельству Sky Guardian, ее GPS-устройство позволяет полиции определять местоположение «клиента» в любой точке на территории Великобритании с точностью до 3 метров. В конце каждого дня устройство может предоставить подробнейший отчет о том, где побывал его носитель. Этот электронный дневник эксперты-наблюдатели могут изучать дистанционно, чтобы выстраивать профили и прогнозы возможных будущих действий поднадзорного. Собственно электронная метка крепится неснимаемым образом в коленной области ноги человека. Эта метка соединена близкодействующим радиоканалом со специальным мобильным телефоном, который поднадзорный должен все время носить при себе. Если телефон, автоматически подсоединяющийся к центру полицейских-надзирателей, оказывается вдруг на удалении от метки, то в центр тут же поступает сигнал тревоги [JD03].

Британские правозащитные организации всерьез обеспокоены новым прожектом властей, намеренных применять электронные метки к людям, уже полностью отбывшим наказание. Потому что, по словам одного из правозащитников, если человека освободили, то он должен жить как свободные люди, а подобные меры мутят воду и стирают грань между виной и невиновностью. Достаточно очевидно, что педофилов в данном случае выбрали в качестве «пробного шара» вполне умышленно, как людей с поведением, наиболее широко осуждаемым в обществе. Если же эксперимент удастся, то впоследствии его легко можно развить и на другие категории граждан, переступивших черту закона. В какую сторону постепенно смещается эта черта, наглядно видно из следующего примера.

От школы до тюрьмы

Небольшая начальная школа в г. Буффало, штат Нью-Йорк, в сентябре 2003 г. стала, похоже, первым учебным заведением в США (да и в мире, наверное), где всех детей пометили чипами радиочастотной идентификации, или кратко RFID. Дирекция школы решила, что именно таким путем учебу можно сделать более эффективной и безопасной. Для

начала, с первых сентябрьских дней компьютерная система стала автоматически фиксировать время появления каждого ребенка в школе. С ноября использование RFID постепенно расширяется для отслеживания взятых книг в библиотеке, автоматического ведения дисциплинарных журналов, регистрации покупок в кафетерии и посещений медицинского кабинета. Ну а еще через несколько месяцев уже видится полный контроль за перемещениями каждого школьника – от времени посещения конкретных аудиторий до времени входа и выхода из школьного автобуса.

Все 422 ученика этой школы теперь носят на шее небольшую пластиковую карту с фотографией, именем, классом и встроенным пассивным RFID-чипом. Пассивный чип намного дешевле активного, имеющего элемент питания, и излучает идентифицирующую информацию не постоянно, а лишь при попадании в поле действия прибора-считывателя. На всю систему идентификации школа потратила 25 000 долларов, а одна карточка с RFID стоит около 3 долларов. Любопытно, что в карточке используется тот же самый чип (smart label) фирмы Texas Instruments, что и в браслетах, надеваемых всем заключенным техасской тюрьмы Pima County Jail [JS03].

Более наглядной параллели для новой жизни школы, пожалуй, и придумать-то невозможно.

Глава 7. Тайны выборов

Страницы жизни героя, 1952. Тонкая, однако, работа

Президентские выборы 1952 года как никакие другие оказались заполнены всевозможными скандалами, грязными слухами и обвинениями на сексуальной почве. Кандидата от демократической партии Эдлая Стивенсона повсюду преследовали кривотолки о его, якобы, аресте полицией за гомосексуализм. Одновременно о соратнике Стивенсона по президентской кампании, кандидате демократов в вице-президенты Джоне Спаркмене, упорно распространялись слухи, что он закоренелый бабник, не пропускающий мимо себя ни одной юбки. Ныне общеизвестно, что основную часть этих слухов тайно распускал шеф ФБР Эдгар Гувер, всерьез вознамерившийся помешать демократической партии опять занять Белый дом. С предыдущим президентом-демократом Гарри Трумэном хороших отношений у Гувера явно не сложилось – Трумэн был весьма жесткий политик (достаточно вспомнить принятое им решение об атомной бомбардировке Хиросимы и Нагасаки) и решительно препятствовал росту влияния и полномочий ФБР. Существенных перемен в партийной линии демократов с приходом нового президента не ожидалось, поэтому кандидат от республиканцев – прославленный боевой генерал Дуайт Эйзенхауэр – по целому ряду причин устраивал Гувера куда больше.

Вокруг бравого военачальника, правда, тоже разгорелся предвыборный «сексуальный» скандал, поскольку сторонники демократов где-то раздобыли копию письма генерала Маршалла к Эйзенхауэру, с предостережениями от развода с женой и запланированной женитьбы на

фронтовой подруге Кей Саммерсби, водительнице автомашины главнокомандующего в годы Второй мировой войны. К этой интриге, правда, Гувер не имел никакого отношения, поскольку информация утекла из Пентагона.

Внешне же, как и вообще на протяжении почти всей своей карьеры, Эдгар Гувер упорно старался поддерживать имидж человека, находящегося вне политики и острой межпартийной борьбы. Лишь так, не выказывая явных предпочтений какой-либо из соперничающих сторон, можно было стабильно удерживаться в кресле директора ФБР при смене администраций. Гувер весьма рано, еще в 1920 году на собственном опыте убедился, сколь опасно в открытую делать ставку на какого-либо конкретного политика. Летом того года министр юстиции Митчел Палмер решил выдвинуться кандидатом в президенты на съезде демократической партии в Сан-Франциско, а молодой Гувер в ту пору лишь в Палмере видел залог своего успешного продвижения по службе. Поэтому он приложил все силы для выполнения предвыборных поручений министра, часто превышая служебные полномочия. За что вскоре серьезно поплатился, поскольку на съезде удача Палмеру не сопутствовала, последующие выборы демократы проиграли, а «партийными» разъездами Гувера и ряда других сотрудников Бюро за счет налогоплательщиков всерьез заинтересовалась комиссия сенатского расследования. Дело, правда, удалось замять, хотя угроза увольнения тогда наметилась вполне всерьез. С той поры Эдгар Гувер зарекся от вступления в политические партии и не принимал участия в выборах.

В доверительных беседах с близким друзьями, впрочем, шеф ФБР вполне определенно признавался в своих политических предпочтениях. Историкам известны личные письма Гувера, из которых очевидно, что начиная с 1921 года он считал себя последовательным сторонником правого крыла республиканской партии.

Но делались такие признания очень осмотрительно и лишь в ближнем кругу. Потому что столь милая его сердцу администрация однофамильца-республиканца Герберта Гувера за 1929-32 гг. довела экономику США до окончательного краха, и к власти опять решительно устремились демократы. Причем один из влиятельных политиков этой партии, Митчел Палмер, теперь был уверен, что его бывший протеже Эдгар Гувер оказался низким и недостойным человеком, которого давно пора вышвырнуть вон из Министерства юстиции. Если, конечно, удастся прийти к власти.

Угрозы эти стали совсем реальны, когда демократы и «новый курс» их лидера Франклина Рузвельта победили на выборах, а министром юстиции решили назначить сенатора Томаса Уолша, имевшего к Гуверу длинный список годами копившихся претензий за беззаконные «красные рейды» и прочие злоупотребления. Уолш, по его словам, намеревался провести в Министерстве юстиции радикальную реорганизацию с заменой «практически всех кадров». Вполне возможно, что именно по такой траектории и пошел бы новый курс нового министра, но по дороге в столицу, уже непосредственно в вашингтонском поезде Томас Уолш скоропостижно скончался – от инфаркта.

Будущее Гувера оставалось все еще мрачным и неопределенным.

Новым министром юстиции стал Гомер Каммингс, на которого очень серьезно давили некоторые сенаторы и конгрессмены-демократы, настаивая на увольнении Гувера. Сам Каммингс тоже был не прочь поставить на важный пост своего человека, и новым директором Бюро расследований уже прочили Уоллеса Фостера, бывшего чиновника Министерства юстиции. Но тут и Фостер скоропостижно скончался.

В итоге Каммингс все же решил, что лучше оставить опытного Гувера. Президент Рузвельт с этим решением согласился, и в июле 1933 года Эдгар Гувер был вновь утвержден на посту директора. А Гомер Каммингс впоследствии очень сожалел о своем решении, назвав его «одной из самых больших ошибок, которые я когда-либо сделал»…

За годы правления Рузвельта шеф ФБР чрезвычайно усилил свое могущество, но все же его явно пока не хватало, чтобы реально влиять на выбор нацией президентов. Это убедительно продемонстрировала предвыборная кампания 1948 года, когда Гувер изо всех сил давил на доступные тайные рычаги, пытаясь добиться смещения неудобного Гарри Трумэна, однако ничего путного из этого все равно не вышло. Зато тогда же, в конце 1940-х годов директора ФБР начали усиленно обхаживать техасские нефтяные магнаты Клинт Мерчисон и Сид Ричардсон, признавшие в Гувере влиятельного деятеля национального масштаба и очень полезную фигуру в своих политических играх. Поэтому Гувера стали регулярно приглашать на красивый отдых в Техас, на богатую охоту, в роскошные курортные отели Калифорнии и Флориды, принадлежавшие миллионерам. Гуверу очень понравилась новая компания, не скупившаяся на щедрые подарки, а Клинта Мерчисона он стал называть «одним из своих ближайших друзей». В устах шефа ФБР подобное звучало весьма двусмысленно, поскольку в окружении этого человека в достатке было людей, весьма авторитетных в мире организованной преступности.

Мерчисону и Ричардсону, мультимиллионерам и богатейшим людям планеты, как и Гуверу, очень не нравился курс президента Трумэна, правда, по собственным резонам. Нефтяным королям Трумэн был ненавистен тем, что публично заявлял о необходимости лишить их налоговых льгот, а также наложил вето на те законопроекты, что сулили принести им еще большую прибыль. Техасцам, по большому счету, было абсолютно без разницы, какую партию поддерживать, главное – поставить в президенты «своего» человека. Выбор их пал на пятизвездного генерала Эйзенхауэра, в ту пору главнокомандующего вооруженными силами НАТО. Сид Ричардсон лично слетал в Париж, в штаб-квартиру главкома, где передал ему программный пятистраничный документ, обосновывающий массу причин, по которым именно Эйзенхауэр должен стать новым лидером нации. Вдобавок была обещана щедрая финансовая помощь на предвыборную кампанию. Как только от генерала было получено принципиальное согласие, мощно завертелась предвыборная машина, подключившая к финансированию и других богатейших людей.

Попутно другие «нефтяные» приятели Мерчисона, Ричардсона и Гувера начали тайно финансировать принадлежавшие Эйзенхауэру и его близким родственникам хозяйства, от которых не слишком обильным, но вполне ощутимым ручейком потекли финансовые прибыли. Когда Эйзенхауэр и его команда пришли к президентской власти, было сделано

множество ощутимых шагов в пользу магнатов из «группы поддержки», в первую очередь нефтяного бизнеса. Например, только за первые 4 года правления администрация Эйзенхауэра выдала шестьдесят лицензий на добычу нефти из правительственных запасов. Для сравнения можно сказать, что за предыдущие 55 лет было выдано лишь 16 таких лицензий. Кроме того, большое количество ключевых постов в федеральных органах власти было отдано нефтепромышленникам и «дружественным» им индустриальным группам.

Чудесные времена настали не только для Мерчисона и Ричардсона, но и для их верного союзника. Люди из близкого окружения Гувера сообщали, что шеф ФБР называл восемь лет правления Дуайта Эйзенхауэра «самыми лучшими и счастливыми» за всю свою карьеру. Вспоминая эти годы, Гувер говорил так: «Я был в близких отношениях с генералом Эйзенхауэром. Он был великим человеком и великим президентом».

Генерал действительно сумел оставить о себе память как о великом человеке. Именно им был запущен в оборот столь расхожий впоследствии термин «военно-промышленный комплекс». Именно Эйзенхауэр предупредил страну и мир об угрозах этого чудовищного монстра в своей прощальной речи, когда в январе 1961 года передавал высокий пост новому президенту Джону Кеннеди. Вот наиболее важный фрагмент этой речи:

[За годы Второй мировой, Корейской и Холодной войны] Мы были вынуждены создать постоянную индустрию вооружений гигантских масштабов. Вдобавок к этому три с половиной миллиона мужчин и женщин непосредственно вовлечены в деятельность вооруженных сил. Сумма ежегодных расходов на военную безопасность превышает чистый доход всех корпораций США вместе взятых. Эта связка гигантских вооруженных сил и огромной индустрии вооружений представляет собой нечто новое в опыте Америки. Суммарное воздействие этого – экономическое, политическое, даже духовное – ощущается в каждом городе, в каждом доме Штатов, в каждом ведомстве федерального правительства. Мы признаем, что так было нужно. Однако, мы не должны упускать из виду и серьезнейшие последствия этого […] для самих основ нашего общества. В правительстве мы должны препятствовать обретению того недопустимого влияния, которого вольно или невольно добивается военно-промышленный комплекс. Потому что потенциал для погибельного роста этой неприемлемой силы существует и будет сохраняться в дальнейшем. Мы никогда не должны позволить, чтобы давление этого союза стало угрожать нашим свободам или демократическим процессам. Нам ничего не следует брать на веру. Только бдительное и хорошо осведомленное гражданское общество может обеспечить […], чтобы безопасность и свобода могли процветать совместно [DE60].

Как известно, никто из последующих американских президентов не внял предупреждению Эйзенхауэра.

Голосование с черным ящиком

В декабре 2003 года главный государственный орган стандартизации США – Национальный институт стандартов и технологий (НИСТ) – устроил

довольно необычный «Первый симпозиум по формированию доверия к системам голосования». Необычным было даже не то, что Америка использует на выборах разной конструкции машины голосования уже 115 лет, а симпозиум «о доверии технике» собрали только первый раз [NI03]. Куда более удивительным выглядел на форуме специфический расклад сил. Чиновники избирательных комиссий штатов, ответственные представители федерального правительства и руководство фирм-изготовителей техники для голосования – почти все дружно выступали за скорейшее и повсеместное внедрение нового компьютерного оборудования, облегчающего как саму процедуру выборов, так и итоговый подсчет голосов. Оппозиционной же группой, настойчиво и всерьез выступавшей против этих намерений, оказались компьютерные специалисты и эксперты в сфере защиты информации. То есть единственные, по сути дела, участники форума, реально представляющие суть обсуждаемого предмета – риски и ненадежность применения компьютеров в выборах [LL03b].

Узнать это вы не можете никак

Насколько серьезную угрозу самим основам демократии представляют поспешно внедряемые ныне компьютерные системы голосования, общество всерьез начало осознавать лишь с лета 2003 года, когда в печать все больше и больше начали просачиваться сведения о чрезвычайно странных «глюках» аппаратуры и плохо объяснимых несоответствиях в итогах выборов.

Вот наглядный тому пример. На выборах в штате Джорджия в ноябре 2002 г. итоги голосования заставили густо покраснеть все службы опроса общественного мнения. В самый канун выборов находившийся у власти губернатор-демократ Рой Варне опережал по опросам своего соперника-республиканца примерно на 9-11% голосов избирателей. На параллельных выборах в Сенат кандидату-демократу опросы отдавали несколько меньший перевес в 3-5 пунктов. Поскольку штат Джорджия имеет давнюю традицию предпочитать демократов, прогнозы аналитиков и опросы избирателей вполне согласовывались друг с другом. Однако реальные итоги голосования поразили всех совершенно неожиданным результатом. Кандидат в губернаторы от республиканцев Сонни Пэдью набрал 51%, а Рой Варне – лишь 46%, т.е. итоги последнего опроса и выборов разошлись на 16 пунктов. В выборах сенатора от штата – та же картина: республиканец Чемблис (53%) обошел демократа Клеланда (46%), «обманув» результаты всех опросов на 9-12 пунктов.

В политике, конечно, случается всякое, и смена партии у власти – даже неожиданная – вещь вполне обычная. Но конкретно в данном случае столь гигантская ошибка служб изучения общественного мнения не получила никаких объяснений даже при последующих разбирательствах и повторных опросах. А дополнительным фактором, сильно усиливающим подозрения в манипуляции итогами выборов, стало следующее обстоятельство. Именно в ноябре 2002 года, как раз накануне выборов, Джорджия стала первым в стране штатом, где все голосования были полностью проведены с помощью новейших компьютерных систем,

обошедшихся в 54 миллиона долларов и обещавших «самые надежные, самые современные и самые дружелюбные к избирателю выборы за всю историю» самой великой из демократий на планете [AG03].

Причем Джорджия оказалась далеко не единственным штатом, где выборы последнего времени, проводимые с помощью новой компьютерной техники, приносят удивительные, а порой и просто потрясающие результаты. Наиболее комичный, пожалуй, случай произошел в ноябре 2003 года на местных выборах в штате Индиана, где компьютеры для голосования выдали итог о подсчете 144 000 поданных голосов – при общем количестве избирателей менее 19 тысяч человек [IR03]. Запаниковавшие организаторы голосования, уверенные, что подобный «глюк» может быть лишь следствием ошибок в программном обеспечении, срочно провели исследование программы, что смогли исправили, и выдали новый, правдоподобный результат– 5352 проголосовавших. Насколько результат соответствует истине – никому неведомо, а проверить невозможно, потому что в новых машинах для голосования не предусмотрены альтернативные, т.е. распечатанные на бумагу, данные голосования для проверки и пересчета.

Интересно, что количество проблем с избирательными технологиями резко возросло в США после гранд-конфуза с мутными по сию пору итогами президентских выборов 2000 года. Учтя множество нареканий к качеству регистрации и учета голосов, американский Конгресс в 2002 году принял специальный закон с громким названием HAVA (Help America Vote Act – «Поможем Америке голосовать») и выделил властям штатов 3,9 миллиарда долларов на полную модернизацию избирательной техники. Уже более века на избирательных участках США применяются разного рода рычажные и перфокарточные машины для голосования. Теперь же в качестве наиболее вероятной замены для устаревшей техники выступает, как правило, электронный «черный ящик», т.е. компьютер со строго засекреченной изготовителем начинкой. Внешне же это устройство чаще всего представляет собой сенсорную жидкокристаллическую панель-экран с регистрационной смарт-картой избирателя, инициализирующей процедуру голосования. Изготовляют эти весьма недешевые устройства по цене 4-5 тысяч долларов за штуку, главным образом, три частные американские компании – Diebold, ESS (Election Systems Software) и Sequoia, контролирующие свыше 90% данного сектора рынка (причем все три фирмы контролируются республиканской партией, о чем чуть позже).

Предельно доступно суть проблемы с новой техникой излагает в своих выступлениях конгрессмен-демократ Раш Холт от штата Нью-Джерси [RH03]: «Представьте себе день выборов 2004 года. Вы приходите на избирательный участок и отдаете свой голос при помощи сенсорного экрана новейшей машины для голосования. Экран говорит, что ваш голос учтен. Но покидая избирательную кабинку вы, однако, задаете себе вопрос – а как я, собственно, узнаю, действительно ли машина верно зафиксировала мой голос? Факты таковы, что узнать это вы не можете никак». При реализованных ныне электронных технологиях у избирателя в США нет абсолютно никакой возможности удостовериться, что голос, отданный через сенсорный экран за кандидата А не приписан машиной кандидату Б.

Естественно, подобная ситуация не может не вызывать серьезного беспокойства у тех американцев, которые понимают, что голосование – это процедура, лежащая в фундаменте всей демократической политической системы. И если возникают хоть какие-то сомнения в честности и законности данной процедуры, то в конечном итоге это ударяет по легитимности всей власти в целом. Поскольку дело касается электроники, то громче всех бьют тревогу компьютерные специалисты, озабоченные тем, что сотни тысяч новых избирательных машин, обобщенно именуемых DRE (от direct-recording electronic – электроника прямой записи) и все шире используемых на выборах, не обеспечивают поддающегося контролю и пересчету «бумажного следа», регистрирующего каждый индивидуальный голос. Коалицию компьютерных ученых, а теперь уже целое общественное движение «Проверяемое голосование» [http://www.verifiedvoting.org] организовал Дэвид Дилл, профессор информатики Стэнфордского университета. Другим активным противником нынешних систем и авторитетным экспертом в данной области слывет Ребекка Меркюри, профессор информатики Гарвардского университета и основатель консалтинговой компании Notable Software, защитившая в 2000 году докторскую диссертацию по методам надежного контроля электронных систем голосования [http://www.notablesoftware.com/evote.html].

Но по каким-то нераскрываемым причинам уже много лет (постепенное внедрение сенсорных экранов началось в середине 1990-х) официальные государственные структуры США, ведающие организацией выборов, фактически игнорируют настойчивые предупреждения ученых. Как говорит Дэвид Дилл, «все, что мы слышим во множестве разных мест – это то, что не следует волноваться по поводу данных машин, поскольку они сертифицированы на федеральном уровне и уровне штатов; однако чрезвычайно сложно получить непосредственную информацию о том, что именно происходит в ходе сертификационного процесса». Причем одновременно под предлогом коммерческой тайны в строжайшем секрете удерживаются и все подробности о внутреннем устройстве техники. Согласно принятой в США практике, машины для голосования выпускаются частными фирмами и выведены из-под проверки независимых экспертов. Оборудование продается властям штатов на условиях строгой охраны коммерческих секретов, делающих уголовным преступлением самостоятельные попытки изучения внутреннего устройства машины. Легальный анализ схемы дозволен только при наличии соответствующего ордера суда, получить который, как свидетельствует Меркюри, оказывается очень и очень непросто даже при наличии множества нареканий к работе машины.

Не желая мириться с плотной завесой секретности вокруг машин для голосования, журналистка и общественная активистка Бев Харрис уже не первый год ведет с помощью друзей частное расследование всей этой темной истории. Итогом работы стала книга [BHO3] Харрис «Выборы с черным ящиком: подделка голосования в 21 веке». В этой книге на основе документов и бесед с конкретными участниками событий показано, в частности, что так называемая «сертификация» электронных машин – это чистый фарс вперемежку с откровенной ложью. (Подробности см. [SM03])

Здесь же собрано свыше ста официально зафиксированных случаев на

региональных выборах в разных округах США, демонстрирующих множество удивительных результатов, порожденных электронными машинами голосования. Например в трех округах штата Техас победившие в ноябре 2002 года кандидаты-республиканцы набрали в точности одинаковое количество голосов – 18181 (кто-то остроумно заметил, что если цифры этого результата перекодировать в соответствующие по порядку буквы латинского алфавита, то получится совсем весело – АНАНА).

А выборы губернатора штата Алабама в том же ноябре закончились еще интереснее. Предварительный подсчет голосов вечером по окончании выборов показал, что победителем стал демократ Дон Сиджлмен. С этим результатом все наблюдатели разошлись по домам спать, однако на следующее утро выяснилось, что 6300 голосов за Сиджлмена необъяснимым образом куда-то из накопителя пропали, так что победу пришлось присудить республиканцу Бобу Райли. Возмущенные демократы пытались, естественно, судиться, однако выяснилось, что законы штата в подобных случаях не предусматривают повторных выборов…

Но самая важная, пожалуй, часть расследования Харрис – это анализ обнаруженных на служебном интернет-сайте фирмы Diebold архивов с файлами исходных кодов программного обеспечения машин для голосования AccuVote-TS (т.е. touch-screen – с сенсорным экраном). Подробности этой истории см. [DJ03]

И грянул гром

В начале июля 2003 г. друзья Харрис выложили материалы Diebold в Интернет для всеобщего ознакомления, благодаря чему файлы с кодом программ попали в поле зрения весьма авторитетного эксперта Ави Рубина, директора Института информационной безопасности при университете Джонса Хопкинса. Вместе с группой из еще трех коллег Рубин провел предварительный анализ текстов программного обеспечения машин Diebold, что стало фактически первым независимым исследованием реальной безопасности электронных систем голосования в США. Публикация статьи [AR03] с результатами этого анализа без преувеличения произвела эффект разорвавшейся бомбы.

Уже поверхностное исследование ПО показало, что уровень системы AccuVote-TS находится намного ниже даже самых минимальных стандартов безопасности, применяемых в других контекстах, подразумевающих защиту информации. Отмечены несколько серьезнейших слабостей, включая неавторизованное расширение полномочий, неправильное использование криптографии, уязвимость в отношении сетевых угроз. Продемонстрировано, что даже не зная исходного кода программ, злоумышленник может бесконтрольно манипулировать результатами выборов. А уж при знании кода вся система предоставляет просто бескрайний простор для злоупотреблений…

Поскольку имя Рубина достаточно хорошо известно, исследование быстро получило резонанс в СМИ – об экспертизе прошли сообщения практически во всех центральных новостных службах (однако, что характерно, в американской прессе старательно избегают упоминать давно

бьющую тревогу Бев Харрис или ее книгу, хотя Рубин с коллегами честно ссылаются на источник подвергнутой анализу информации).

На поднявшееся в обществе волнение сочли нужным, наконец, прореагировать и официальные представители избирательных органов власти. Национальная ассоциация секретарей штатов, большинство членов которой отвечает за организацию выборов на местах, под впечатлением от публикации решила рассмотреть вопрос о введении стандартов на машины для голосования, что должно воспрепятствовать подделке результатов выборов. Разработку соответствующих критериев для оценки машин нового поколения решено поручить Национальному институту стандартов и технологий США. Прежде подобная мысль никому из чиновников почему-то в голову не приходила.

В целом же столь долгую и мутную историю вокруг «секретной» избирательной техники (единственная задача которой состоит в аккуратном учете голосов) стали трактовать как результат обычного разгильдяйства и недосмотра бюрократов. А то, что в США имеются очень серьезные структуры, знающие толк в защите информации и компьютерной безопасности, предпочли вообще не вспоминать. Но если на государственном уровне полдесятка лет вокруг машин для голосования сохранялся полный бардак, тщательно огражденный от вмешательств извне, значит просто кому-то это было очень выгодно.

Поскольку фирма Diebold уже успела охватить своей техникой для голосования AccuVote почти 40 американских штатов, проблема обрела общенациональный размах. Первым решил на деле продемонстрировать заботу властей о честных результатах выборов Роберт Эрлих, губернатор-республиканец штата Мэриленд, где именно в это время вовсю шла закупка машин AccuVote-TS на сумму 55,6 миллионов долларов и где, кроме того, расположена штаб-квартира Агентства национальной безопасности США. Роберт Эрлих заказал еще одно независимое экспресс-исследование электронных машин третьей стороне – калифорнийской фирме Science Application International Corps (SAIC), имеющей очень тесные связи с АНБ. Одновременно губернатор Эрлих пообещал, что результаты этого исследования будут честно опубликованы в Интернете для всеобщего ознакомления [СВОЗ].

Вскоре, уже в начале сентября 2003 г. властям Мэриленда был представлен большой 200-страничный отчет с результатами анализа экспертов SAIC, в целом подтвердивший, что система Diebold AccuVote-TS, «реализованная в нынешних процедурах и технологиях, с высокой степенью риска подвержена компрометации». В отчете даны внятные рекомендации по улучшению защиты оборудования, однако последующая интерпретация выводов документа руководством SAIC, губернатором Эрлихом и компанией Diebold породили у специалистов и публики недоумение, массу новых вопросов и лишь обострили споры вокруг махинаций с электронным голосованием.

Для примера, вот выдержка из официального пресс-релиза властей штата Мэриленд, где цитируется вывод губернатора Эрлиха: «В августе я приказал моей администрации подвергнуть машину Diebold и исходные коды ее программ строжайшей проверке для уверенности в том, что она отвечает моим высоким стандартам. В этом месяце (сентябре) аналитики

третьей стороны представили мне положительный независимый обзор, свидетельствующий, что машина Diebold и ее исходный код, если работать с ними правильно, могут быть одной из самых надежных и наиболее безопасной из доступных систем голосования. Благодаря этому отчету избиратели Мэриленда будут иметь лучшее среди всей нации оборудование для выборов» [GO03].

Достоверно известно [WP03], что в аналитическом обзоре SAIC выявлено 328 слабостей в безопасности машин Diebold, из которых 26 расцениваются как «критические». Газета New York Times процитировала слова профессора Ави Рубина, возглавлявшего июльское исследование в университете Джонса Хопкинса и крайне озадаченного реакцией властей Мэриленда на отчет SAIC: «Создается сильнейшее впечатление, что люди, планирующие дела в штате, или не читали, или не поняли документ SAIC… Потому что им явно следовало сказать: мы намерены приостановить разворачивание этих систем до тех пор, пока нам не подтвердят, что эти вещи безопасны в использовании». Та же газета одновременно цитирует слова исполнительного директора Diebold Марка Радке, который в комментариях к исследованию SAIC заявил, что этот документ «действительно подтвердил позицию компании, согласно которой наше оборудование столь же безопасно, если не более безопасно, чем любая другая электронная система на рынке»… [SZ03].

Отчет SAIC, как и было обещано, администрация Мэриленда действительно опубликовала в Интернете [RR03], но реально его оценить невозможно, поскольку от исходных 200 страниц в документе оставлено лишь неполных 40. Прочие 160 страниц и многие строки-абзацы из оставленных фрагментов изъяты по рекомендации SAIC, поскольку «могут быть использованы хакерами-злоумышленниками». Власти же Мэриленда, вполне довольные проделанной работой, объявили о продолжении закупок электронных машин Diebold, поскольку фирма-поставщик пообещала внести нужные поправки. А если Ави Рубин и другие независимые эксперты заявляют, будто всю систему надо переделывать с нуля и поправлять что-либо в подобных условиях «наивно и нереалистично», то это их личные трудности. Для чиновников и изготовителей оборудования подобных проблем не существует.

Чужие здесь не ходят

Хотя статье Рубина и коллег безусловно удалось сыграть важную роль в привлечении внимания общества к угрозе «украденных выборов», центральные СМИ предпочитают фокусировать внимание публики на «позитивных сдвигах», якобы происходящих в данной сфере. На глубинных причинах создавшейся неприятной ситуации аналитики больших и важных изданий почему-то фиксировать свое внимание не желают. Поэтому все наиболее интересные материалы с исследованиями и расследованиями, а также текущие любопытные наблюдения, как и прежде появляются лишь в Интернете и малотиражной региональной прессе США (плюс немного в британской).

Так, например, тотально была проигнорирована совершенно позорная история о недопущении на отраслевой международный форум наиболее

авторитетных специалистов в области электронного голосования Ребекки Меркюри и Дэвида Чома. Дело происходило в августе 2003 года, в городе Денвере, шт. Колорадо, где собиралась ежегодная выставка-конференция IACREOT, Международной ассоциации избирательной и архивной госадминистрации.

В рамках этого мероприятия проходила демонстрация делегатам новейших электронных машин для голосования, и президент ассоциации IACREOT Мэриэн Рикенбах сделала все, чтобы не допустить выступления на конференции специалистов, весьма критически оценивающих данную аппаратуру. Рикенбах лично вывела из зала заседаний Ребекку Меркюри и объявила ей об аннулировании мандата участника. Поскольку столь крутые действия требовалось чем-то аргументировать, было заявлено, что Меркюри неправильно заполнила регистрационные бланки. Точно так же аннулировали мандат и Дэвиду Чому, криптографу с мировым именем, разработавшему надежно защищенный протокол анонимного проверяемого голосования и входящему в «группу поддержки» Меркюри [LM03].

Здесь уместно вспомнить, что машины для голосования продаются в США по той же схеме, что издавна действует для всех правительственных закупок– т.е. путем интенсивного лоббирования, «смазывания и смачивания» заказчиков из структур власти. На упомянутой денверской конференции IACREOT, к примеру, фирмы-изготовители избирательного оборудования обильно кормили-поили делегатов на банкетах и щедро одаривали всякими нескромными «сувенирами», вроде дорогих чемоданчиков-кейсов, украшенных логотипом компании Sequoia.

Делегаты-чиновники совершенно спокойно принимают подобные подарки, и никого, похоже, не тревожит, что лишь в 1999 году Министерство юстиции США возбуждало против Sequoia дело с обвинением компании расходовании свыше 8 миллионов долларов на взятки. В 2001 г. администрация одного из округов Флориды (Pinellas County) была вынуждена аннулировать контракт на закупку избирательного оборудования Sequoia на сумму 15,5 млн долларов, когда вскрылось, что против Фила Фостера, регионального директора фирмы, возбуждено уголовное дело в Луизиане по обвинению в отмывании денег и коррупции. Обвинения затем были сняты в обмен на показания против чиновников Луизианы из комиссии по организации выборов. Совершенно аналогичная история происходила в 2002 году с компанией ESS, вице-президент которой также был освобожден от уголовного преследования за дачу взяток в обмен на показания против секретаря штата Арканзас Билла Маккьюэна, обвиненного в коррупции и взяточничестве при покупке машин для голосования [AG03].

Компания ESS, крупнейший в стране изготовитель избирательной аппаратуры DRE, прежде называвшаяся American Information Systems (AIS), принадлежит финансово-промышленной группе McCarthy Group. Основатель этой группы Майкл Маккарти в 1996 и 2002 гг. возглавлял избирательные кампании Чака Хейгла, сенатора-республиканца от штата Небраска. Установлено, что Хейгл с 1992 по 1995 год был президентом ESS (тогда под названием AIS) и по сию пору является совладельцем фирмы, поскольку в капитале McCarthy Group ему принадлежит доля размером около 5 млн долларов. Почти все новое избирательное оборудование в

штате Небраска изготовлено фирмой ESS. Сенатор Чак Хейгл стал первым за 24 года республиканцем в Сенате от Небраски, причем 80% отданных за него в 1996 и 2002 гг. голосов были подсчитаны на машинах принадлежащей ему компании [ML03].

Но больше всех любовью к республиканской партии прославилась компания Diebold, второй по величине изготовитель DRE. Исполнительный директор Diebold Уолден О'Делл известен как один из наиболее преданных и энергичных активистов по сбору денег на избирательные президентские кампании Джорджа Буша. В письмах, разосланных потенциальным спонсорам, О'Делл всячески заверяет о намерениях «помочь штату Огайо в отдаче своих избирательных голосов за президента на выборах следующего года».

Короче говоря, имеется масса свидетельств о ярко выраженной «республиканской ориентации» всех трех основных фирм, производящих в США электронное оборудование для голосования. И не только этих фирм. Вот, к примеру, еще одна компания – VoteHere, создающая специальное криптографическое обеспечение, планируемое к установке во все машины голосования для более надежной защиты информации. В совете директоров VoteHere обнаруживается Роберт Гейтс, бывший директор ЦРУ, ныне работающий в Школе бизнеса Джорджа Буша. Председателем же дирекции VoteHere является адмирал Билл Оуэнс, он же недавний глава корпорации SAIC, он же член Консультативного политического совета Пентагона [Defense Policy Board, еще об этом прибыльном органе – см. раздел «Служба гибкой морали»] и близкий соратник вице-президента Дика Чейни.

При более глубоком проникновении за кулисы всей кухни, изготовляющей DRE-машины для «прямого голосования», неожиданно обнаруживаются глубокие корни, уходящие в недра корпораций-гигантов военно-промышленного комплекса США. Издателю книги Бев Харрис «Голосование с черным ящиком» Дэвиду Аллену удалось однажды незримо поприсутствовать на телефонной конференции-совещании руководителей всех основных DRE-компаний (поприсутствовать не по приглашению, ясное дело, а благодаря паролю доступа от одного из «сочувствующих инсайдеров»). Из записанных на магнитофонную ленту переговоров становится известно, что некая лоббирующая «Рабочая группа по системам голосования», сыгравшая ключевую роль в принятии Конгрессом закона HAVA (3,9 миллиардов на избирательную электронику), состояла из головных контракторов Министерства обороны – компаний Lockheed-Martin и Northrop-Grumman, а также ИТ-фирм Accenture и EDS, активно подвизающихся на заказах Пентагона и спецслужб [KF03].

Еще одна торгово-промышленная группа, активно лоббировавшая принятие закона HAVA, а ныне проталкивающая внедрение DRE-машин, – это ITAA, Информационно-технологическая ассоциация Америки, где за электронику для голосования отвечает Рональд Кнехт, старший вице-президент корпорации Science Applications International Corp. Той самой «шпионско-военной корпорации» SAIC, что делала «независимую экспертизу» машин Diebold для штата Мэриленд [DA03][ES03].

Как видим, круг замкнулся. На этой кухне интерес у всех один, и чужих сюда не принимают.

Оптимальное решение

Понятно, что электронные машины голосования на избирательных участках – это, вообще говоря, вынужденная полумера. В условиях, когда почти в каждом доме граждан развитых стран уже стоит компьютер (один или несколько), а вскоре чуть ли не до каждого из них дотянется Интернет, намного более заманчивой выглядит идея непосредственного голосования населения через Сеть прямо из дома.

Увы, большинство независимых экспертов вполне единодушно в том, что голосование через Интернет – с помощью компьютеров, находящегося вне избирательных участков – это особо рискованное и ненадежное дело из-за очень сложного сочетания социальных и технологических проблем. Всякое голосование с помощью открепительных талонов несет в себе угрозу свободе и тайне выбора из-за возможностей принуждения и скупки голосов избирателей. А интернет-голосование добавляет к этим проблемам целый букет собственных сложностей. Здесь чрезвычайно трудно гарантировать, что сервис-провайдеры обеспечат надежную защиту от вирусов, сетевых подмен и атак на серверы, что все голоса будут аккуратно и анонимно зарегистрированы, что конкретный голос будет отдан именно тем, кто выдает себя за легитимного избирателя, что, наконец, за плечом у голосующего через компьютер просто не стоит его начальник или покупатель голосов.

Если онлайновые системы выборов оказываются крайне уязвимы для злоупотреблений со стороны внешних сил, то уж для манипуляций со стороны тех, кто управляет системой изнутри, открываются просто фантастические возможности. Особенно, если создавать систему под покровом секретности.

Мутный шлейф за Accenture

Одним из наиболее активных сторонников скорейшего внедрения интернет-голосования является Министерство обороны США, напирающее на необходимость обеспечить равные гражданские права для сотен тысяч своих солдат и офицеров, разбросанных по всему земному шару, а также вообще для миллионов американцев, работающих за рубежом (примерно 5% электората). Первая серьезная попытка устроить выборы через Сеть была предпринята военными в 2000 году, когда в конечном счете было затрачено 6,2 миллиона долларов на то, чтобы свои виртуальные бюллетени бросили через Интернет в виртуальную урну 84 человека. Этот опыт очень сложно назвать удачным, поскольку каждый голос таких избирателей обошелся американским налогоплательщикам в 73 809 долларов [JB01].

Вероятно, несколько человек очень неплохо заработали на столь интересном хайтек-проекте (контракторами были консалтинговая фирма Booz-Allen Hamilton и крупная ИТ-компания Computer Sciences Corp), но на будущее государственные заказчики стали подыскивать менее расточительное решение. К лету 2003 года Министерство обороны окончательно выбрало под эту задачу, конкретно – для обеспечения

интернет-голосования на президентских выборах 2004 года, нового контрактора – консалтинговую фирму Accenture. Подобный выбор трудно назвать очевидным для страны, остро озабоченной национальной безопасностью, поскольку Accenture не является американской компанией. Но зато имеет богатую историю тесных связей с высокими эшелонами нынешней власти США.

Еще совсем недавно эта компания носила другое имя – Andersen Consulting, – под которым громче всего прославилась в ходе скандала вокруг финансовых злоупотреблений и банкротства фирмы Enron. Именно бухгалтеры Andersen Consulting должны были считать и проверять доллары Enron, однако ничего подозрительного в липовой отчетности не увидели. После обретения самостоятельности и процедуры акционирования, сопровождавшихся появлением нового имени Accenture и перемещением интернациональной штаб-квартиры на Бермудские острова, компания за свою короткую историю уже успела создать себе весьма сомнительную репутацию.

Согласно данным канадского исследовательского института Polaris, фирма Accenture мощно вовлечена в крупные проекты по приватизации коммунальных служб, особенно программ социального обеспечения, в США, Канаде и Евросоюзе. Хорошо известно, сколь пышно цветет на этой почве коррупция госчиновников, так что за Accenture потянулся дымный шлейф скандалов, замешанных на взятках и крупных перерасходах государственных средств [DA03].

Accenture сейчас – это очень крупная фирма, по состоянию на конец 2003 года насчитывающая свыше 83 000 сотрудников в 48 странах мира, и с чистым годовым доходом 11,8 миллиарда долларов. В совете директоров фирмы входит много известных людей. Например, глава корпорации Microsoft Стив Баллмер. Отсюда становится вполне естественным, что программное обеспечение, создаваемое в Accenture для интернет-голосования, работает под самой небезопасной из всех популярных операционных систем – ОС Windows. Более того, между Accenture (тогда еще Andersen Consulting) и Microsoft подписан 1-миллиардный «Пакт о создании совместного предприятия и расширении глобального альянса». Другой важный стратегический партнер Accenture – техасская строительно-нефтяная компания Halliburton, которую прежде возглавлял нынешний вице-президент США Дик Чейни (сейчас эта фирма заправляет разделом нефтедобычи в Ираке). Интересно, что теперешний глава Halliburton Дэвид Лесар, пришедший на смену Дику Чейни, до этого работал в Arthur Andersen, родительской компании Accenture. В октябре 2001 года компании Halliburton и Accenture объявили совместным пресс-релизом о «большом расширении» своего долгосрочного сотрудничества [LL03a].

Несмотря на свой зарубежный статус и финансовых инвесторов с Ближнего Востока, компания Accenture является крупным контрактором правительства США с заказами на сумму порядка 1 млрд. долларов, из которых около 300 миллионов приходится на Министерство обороны. Хотя точная сумма военных контрактов Accenture, как правило, объявляется в пресс-релизах, стоимость проекта по созданию системы интернет-голосования (или SERVE, от Secure Electronic Registration and

Voting Experiment) по необъявленной причине сохранена в тайне [АСОЗ][ММОЗ].

Обычно это свойственно разработкам секретного оружия или тайным операциям спецслужб.

Мавр сделал свое дело

В конце сентября 2003 года стало известно, что ключевым партнером Accenture, взявшимся обеспечить важнейшие компоненты системы SERVE для Министерства обороны, стала фирма VeriSign [RL03]. На VeriSign возложены задачи хостинга серверов голосования и разработки такой системы аутентификации, которая одновременно обеспечила бы надежность справедливых выборов и анонимность избирателей. Поскольку и здесь даже сумма контракта сохранена в тайне, крайне маловероятно, что будут опубликованы технические подробности того, каким образом VeriSign решит мудреную задачу соотнесения подробнейших лог-файлов с отчетом о каждом доступе к системе (чего требуют нормы компьютерной безопасности) и строгой анонимности голосования на основе фундаментального принципа справедливых выборов «один человек – один голос».

Связаны эти события или нет, неизвестно, но интересно, что практически одновременно с получением контракта на SERVE – спустя всего пару недель – VeriSign объявила о продаже стороннему покупателю своего важного подразделения Network Solutions [AJ03]. Эту историю необходимо рассмотреть подробнее, поскольку на самом излете памятного многим интернет-бума, весной 2000 года, корпорация VeriSign купила Network Solutions за беспрецедентную для сетевого бизнеса сумму в 21 миллиард долларов. А кроме того, в 1990-е годы деятельность компании Network Solutions Inc. можно рассматривать как пример одной из наиболее успешных акций американских спецслужб по контролю за Интернетом. Поскольку долгое время главным регистратором доменных имен и сборщиком податей со всех пользователей Сети, заводящих в Интернете собственный адрес, была единственная частная компания, тесно связанная с военными и разведывательными ведомствами США.

Компания Network Solutions Inc. (NSI) из г. Херндон, штат Вирджиния, получила гарантированную государством монополию на регистрацию доменных имен в 1993 году. Впоследствии вспышки скандалов вокруг монополизма NSI неоднократно обостряли дискуссии о том, кто контролирует Сеть и управляет Интернетом в целом. Хотя физически Сеть децентрализована и распределена по миллионам соединенных компьютеров планеты, фактически она имеет единую иерархическую организацию. Изначально было положено так, что любой пользователь любой страны, желающий получить собственный интернет-адрес, оканчивающийся на один из наиболее популярных суффиксов (доменнных имен высшего уровня) «.com», «.edu», «.org», «.net» или «.gov», должен зарегистрировать это имя в InterNIC (Internet Network Information Center), созданном по заказу правительства США центральном реестре. Когда-то администрированием InterNIC занималось правительство, эта служба оплачивалась из кармана американских налогоплательщиков и была

бесплатной для всех пользователей, которые просто регистрировали незанятые имена. Но в мае 1993 года Национальный научный фонд приватизировал реестр имен и передал права на его администрирование компании NSI, платя ей за это еще и 5,9 млн. долларов в год. Так что вплоть до середины 1999 года администрированием этого реестра единолично распоряжалась NSI.

Самое интересное началось в 1995 году, когда компанию NSI на корню скупила фирма SAIC, и с сентября 1995 года за регистрацию нового имени стали брать 100 долларов плюс 50 долларов в год за обновление имени старого. Более того, очень скоро NSI начала отбирать адреса у тех тысяч строптивых владельцев, кто, памятуя прежние времена, отказался оплачивать нововведения. Благодаря астрономическим темпам роста Интернета торговля доменными именами оказалась весьма прибыльным бизнесом, и на компанию-монополиста множество раз подавали в суд, однако американское правосудие неизменно занимало сторону NSI [JD97].

Одна из самых последних историй такого рода имела место в конце января 2000 г., когда апелляционный суд США повторно отверг антимонопольный иск компании Name.Space против NSI. Поскольку NSI, пользуясь своим исключительным положением, всячески препятствовала заведению новых доменных имен верхнего уровня, то многие усматривали здесь посягательство на поправку к Конституции США, гарантирующую свободу слова – потому что, например, среди дополнительных имен предлагались и такие, как, например, «microsoft.free.zone», то есть «зона, свободная от Microsoft». Истцы явно надеялись, что суд, чтущий Конституцию, примет во внимание факт ущемления основных свобод граждан. Однако апелляционный суд еще раз подтвердил первоначальное решение окружного суда, согласно которому деятельность Network Solutions «ограждена от антимонопольного законодательства, а доменные имена Интернета не составляют речь, защищенную первой поправкой». Так что апелляция Name.Space и ряда других лиц была полностью отвергнута судом, причем без каких бы то ни было комментариев [NSOO].

Для многих членов интернет-сообщества непробиваемая позиция американского правосудия представлялась довольно странной, хотя люди более сведущие были склонны считать, что все дело тут в многолетнем хозяине компании Network Solutions, поскольку хозяин очень уж необычный – калифорнийская компания SAIC, или Science Applications International Corp. Фирмы такого рода по-русски называются ЗАО или «закрытое акционерное общество», а по-английски «employee-owned company». Хотя абсолютно все акции SAIC находятся в частном владении ее сотрудников, вся история фирмы с самого ее начала связана с государственными заказами. Причем заказами не обычными, а повышенной секретности. И за тридцать с лишним лет своего существования эта «частная лавочка на господряде» выросла в огромную фирму с ежегодным доходом свыше 6 миллиардов долларов долларов и с 40 тысячами сотрудников. Сегодня SAIC называют одной из наиболее крупных в мире и наиболее успешной из компаний типа ЗАО [AN03].

Примерно треть нынешнего бизнеса SAIC приходится на системную интеграцию для других компаний, таких как Pfizer или British Petroleum, однако суть и сердцевина корпорации – это шпионские и специальные

военные технологии. В секретных спецслужбах не принято публиковать списки фирм-контракторов, работающих по их заказам. Но при этом в разведывательном сообществе не считают нужным делать секрет из того, что в последние годы SAIC является главным поставщиком Агентства национальной безопасности США и входит в пятерку ведущих бизнес-партнеров ЦРУ [РКОЗ]. Столь интересной фирме имеет смысл посвятить отдельный (следующий) подраздел, здесь же закончим историю о «владельцах» Интернета.

К середине 90-х годов в связи с окончанием Холодной войны поток военных госзаказов SAIC стал ощутимо сокращаться. Обладая мощным научно-технологическим потенциалом, компания стала искать новые области приложения средств и получения прибыли. Один из ее выборов пал на Network Solutions, лишь недавно выигравшую контракт на распоряжение реестром доменных имен Интернета. Есть, правда, и несколько иное мнение – что NSI, одну из немногих успешных технологических компаний, возглавляемых афроамериканцами, власти выбрали заранее, поскольку в США черные лица боссов – это с некоторых пор весьма выгодный фон для прикрытия разных многоходовых комбинаций.

Так что в 1995 году SAIC целиком купила NSI, превратив ее в свое дочернее предприятие. Вскоре после этого изменились и порядки регистрации доменных имен. Имея большой опыт общения с правительством и зная нужные рычаги, SAIC пробила разрешение взимать 100-долларовую плату за каждое новое имя, а в обмен стала отчислять с этой сотни 30 долларов в правительственный Фонд поддержки инфраструктуры Интернета. Практически полностью автоматизировав в NSI процесс регистрации имен, SAIC успешно обеспечила себе и здесь если не миллиардный, то все равно вполне ощутимый непрерывный приток доходов. Ну а попутно спецслужбы США на много лет получили полный контроль за адресной системой Сети, поскольку среди прочих своих функций Network Solutions хранила и поддерживала так называемый «корневой сервер А» – компьютер, который содержит официальный список Интернет-имен и адресов. Тысячи остальных серверов Сети получают этот список из «корня А».

В течение примерно семи лет Network Solutions наслаждалась полнейшей монополией на регистрацию доменных имен благодаря эксклюзивному соглашению с федеральным правительством США. В таких условиях о продаже NSI и речи быть не могло. Но в конце концов силы, недовольные столь откровенным монополизмом, все-таки дожали администрацию президента Клинтона, и весной 1999 года Министерство торговли открыло рынок доменных имен для конкуренции, позволив регистрировать Web-адреса и другим компаниям. Конечно, Network Solutions продолжала оставаться крупнейшим регистратором (продавая имена, правда, уже по рыночной цене 35 долларов), и еще на четыре года под контролем NSI был оставлен «реестр сетевых имен» – главная база данных обо всех Интернет-адресах. Но в новых условиях с NSI стали соперничать сразу около 25 других компаний, нередко предлагающих более выгодные условия регистрации, да к тому же не имеющие сомнительного шлейфа тесного сотрудничества со спецслужбами. В таких

условиях «крыша» SAIC уже становилась для бизнеса скорее бременем, чем подмогой… Вот тут-то и последовал элегантный увод NSI под крыло «не замазанной» и сугубо коммерческой VeriSign, контролирующей к тому же львиную долю рынка цифровых сертификатов.

Ошеломившая многих новость пришла первых числах 2000 года: компанию NSI за 21 миллиард долларов купила интернет-фирма VeriSign Inc., специализирующаяся в области защиты информации [MFOO]. К тому времени калифорнийская компания VeriSign (г. Маунтин-Вью) уже была хорошо известна как один из главных в мире поставщиков цифровых сертификатов, или «услуг доверия» (куда входят аутентификация, подтверждение достоверности и обеспечение заверенных платежей), используемых для организации безопасного бизнеса и коммуникаций в IP-сетях. Компания установила стратегические отношения чуть ли не со всеми ключевыми для Интернета фигурами – ATT, British Telecom, Checkpoint Technologies, Cisco, Microsoft, Netscape, Network Associates, Network Solutions, RSA Security, VISA и т.д. – что обеспечило широкое применение цифровых сертификатов VeriSign как непосредственно в сетевом оборудовании, так и во множестве программных приложений. Уже к концу 1990-х годов цифровыми сертификатами VeriSign пользовались практически все компании из Fortune 500, сотни тысяч бизнес-сайтов и миллионы индивидуальных пользователей. Компанией созданы несколько десятков филиалов на всех (кроме Антарктиды) континентах, оказывающие трастовые услуги во всех регионах планеты. Характерно, что региональные филиалы нередко создавались путем скупки местных конкурентов.

С приобретением NSI VeriSign получила доступ к ценнейшей базе данных ее клиентов, уже тогда насчитывавшей свыше 10 миллионов владельцев доменных имен (к середине 2003 года это число выросло до 27,5 млн), а также непосредственный доступ к тем тысячам компаний, что ежедневно заводят себе Web-адреса. Когда под одной крышей объединяются ведущий регистратор доменных имен и провайдер цифровых сертификатов, подтверждающих идентичность владельца, то услуги получившейся в итоге фирмы – это, по выражению одного из экспертов, «как одновременная выдача свидетельства о рождении, водительских прав, паспорта и кредитной карточки в одном и том же месте».

Но при этом многие выражали и недоумение от столь тяжеловесной покупки, поскольку обе компании вполне могли бы обеспечить тот же самый сервис через простое партнерское соглашение и с гораздо меньшими финансовыми затратами. На проходившей в тот же месяц встрече членов организации ICANN, с 1999 года надзирающей за новой системой присвоения доменных имен, многие были, мягко говоря, шокированы, не очень понимая, что вообще происходит. Как сказал один из участников, «это очень странная вещь, когда компанию, являющуюся центральной для стабильности и цельности Интернета, можно вот так запросто купить или продать».

Происходило же это примерно так. Компании уже давно приглядели друг друга и несколько лет работали над рядом совместных проектов. Связи их укреплялись, и вот главу VeriSign Стрэттона Склейвоса пригласили занять место в совете директоров Network Solutions. А еще

через некоторое время у того как бы сама родилась идея полностью слить компании. Он отправился с этим предложением к руководству NSI и к ее крупнейшему акционеру – SAIC (несколькими годами раньше SAIC акционировала дочернюю компанию, оставив за собой основную долю). Там же Склейвоса просто как будто ждали, и вопрос о приобретении был решен практически моментально, за пару дней. Если принять во внимание, что сделка стоимостью более 20 миллиардов долларов – это крупнейшая покупка сервисной интернет-компании за всю историю Сети, а покупатель напоминал питона, заглатывающего буйвола (поскольку ежегодные доходы VeriSign составляли менее половины доходов Network Solutions), то быстрота сделки уже тогда порождала сильнейшее подозрение о заранее продуманном и заблаговременно подготовленном ходе.

Впоследствии руководству VeriSign, вероятно, довольно быстро стало ясно, что с торопливой гранд-покупкой NSI они, мягко говоря, несколько погорячились. Бизнес с регистрацией доменных имен в условиях острой конкуренции оказался намного менее прибыльным, чем в сладкие времена монополизма 1990-х. Все последующие годы Network Solutions лишь постоянно теряла свою рыночную долю, снизив цену за имя уже до 27 долларов. При этом средняя цена на рынке составляет около 15 долларов – из которых, правда, любой регистратор отчисляет 6 долларов фирме VeriSign как держателю главного реестра имен. Впрочем, и реестр уже стал не такой уж и главный, поскольку, после настойчивых «наездов» органов, регулирующих Интернет, VeriSign сумела оставить за собой головные базы данных лишь на самые популярные имена «.com» и «.net».

Короче говоря, к осени 2003 года в VeriSign вполне дозрели до того, чтобы признать покупку фирмы NSI ненужной и продали ее за 100 миллионов долларов аризонской венчурной фирме Pivotal Private Equity. Продали, правда, не полностью «с потрохами», а лишь вялый бизнес регистрации имен и хостинга, оставив за собой наиболее существенное – базы данных доменных имен.

Одновременно вся эта история продемонстрировала, насколько дальновидным оказалось в своих расчетах и действиях руководство SAIC, вовремя купив Network Solutions за 4,5 миллиона, а спустя несколько лет продав компанию почти в тысячу раз дороже – уже за 3,1 миллиарда долларов. Причем продажа была организована всего лишь за несколько месяцев до того, как на глазах изумленной публики начал лопаться пузырь перегретой интернет-экономики [AN03].

Закрытое акционерное общество власти

«Мы – компания-невидимка», – доверительно поведал в интервью один из топ-менеджеров SAIC Кит Найтингейл, в прошлом полковник подразделения спецопераций американской армии. – «Мы повсюду, но почти никто этого не видит» [PKO3].

Калифорнийская штаб-квартира SAIC находится на северной окраине г. Сан-Диего, и внешне ее ухоженный кампус ничем не отличается от всех остальных сооружений подобного рода. Однако внутри повсюду бдит вооруженная охрана, двери запираются на сейфовые замки, а многие комнаты экранированы от компрометирующих электромагнитных

излучений. На протяжении многих лет миллиардные доходы компании почти полностью обеспечивались контрактами федерального правительства США. В значительной части – это задания разведки: разработка мощных компьютерных систем анализа данных (data mining), программное обеспечение для спутников видовой разведки, спецтехника для систем наблюдения.

Помимо выполнения контрактов разведслужб, корпорация SAIC разрабатывает компьютерное обеспечение для подводных лодок и реактивных истребителей, участвует в создании систем противоракетной обороны и подземных ядерных бункеров в Неваде, обеспечивает работу общенациональной системы учета преступлений ФБР, а также имеет контракт с федеральной налоговой службой США на администрирование финансовой информации. Еще одна бурно развивающаяся в последнее время сфера бизнеса – разного рода системы для нового Департамента безопасности отечества, вроде сканирующих приборов на базе гамма-излучения, прощупывающих содержимое опломбированных контейнеров и грузовиков.

Аура секретности постоянно окружает SAIC, в кадрах которой работает огромное количество бывших сотрудников спецслужб, руководящих кадров из военных структур и правоохранительных органов. Допуск к государственной тайне имеют свыше 5000 сотрудников SAIC, а основатель и свыше 30 лет бессменный руководитель компании Дж. Роберт Бейстер, говорят, имеет один из самых высоких уровней допуска, когда-либо выдававшихся штатским гражданам страны.

Самая же, наверное, выдающаяся достопримечательность SAIC – это ее совет директоров. Точный состав этого коллектива никогда не известен, поскольку (как сообщается на сайте компании) численность данного органа все время варьируется в пределах 12-22 человек. Кроме того, имеется и специальный механизм непременной ротации – ежегодно состав обновляется на треть с приглашением новых директоров на примерно трехлетний период. Прежние директоры нередко отходят от бизнеса, чтобы «всплыть» на каком-нибудь из очередных высоких государственных постов.

В целом же состав участников этой «карусели» очень впечатляет: адмирал Бобби Инман, бывший директор Агентства национальной безопасности и зам. директора ЦРУ; Мелвин Лейрд, министр обороны при президенте Никсоне; генерал Макс Турман, командовавший вторжением в Панаму; Дональд Хикс, в прошлом возглавлявший исследования и разработки в Пентагоне; Роберт Гейтс, бывший директор ЦРУ; Уильям Перри, министр обороны в клинтоновской администрации; Джон Дойч, еще один недавний директор ЦРУ… И так далее.

Из самых последних директоров можно упомянуть отставного генерала Уэйна Даунинга, члена совета «Комитета по освобождению Ирака», а перед началом войны – главного лоббиста американского детища под названием «Иракский национальный конгресс» и его главы Ахмеда Чалаби. Ранее уже упоминался и другой высокопоставленный военный, адмирал Уильям Оуэнс, главный операционный директор и вице-председатель совета директоров SAIC, одновременно заседающий в советах пяти компаний, активно прокачивающих через себя миллиарды «помощи

Ираку», а также член Консультативного политсовета Пентагона, вырабатывающего стратегию для министра обороны Рамсфелда [SP03].

Суть весьма доходного частного предприятия SAIC, сытно подсосавшегося к изобильной государственной кормушке, видимо, уже ясна в общих чертах. Со времен Ричарда Никсона, с тех пор, как физик-ядерщик Роберт Бейстер создал свое «закрытое акционерное общество» в 1969 году, в ближайшем окружении каждого из президентов США непременно находится кто-то из совета директоров корпорации SAIC. Благодаря несомненным организаторским талантам Бейстера и столь выгодному положению фирмы при власти, абсолютно все годы существования корпорации были для нее прибыльными – несмотря на экономические спады, политические кризисы и прочие неурядицы жизни. Доход фирмы, владельцами которой являются исключительно ее сотрудники, вырос с 243 тысяч долларов в 1970 г. до 6 с лишним миллиардов долларов в 2003 году [РКОЗ].

В ноябре 2003 г. Роберт Бейстер, которому уже 78 лет, принял решение оставить ключевые посты президента и исполнительного директора корпорации, пригласив себе на смену Кеннета Далберга, вице-президента по инфотехнологиям корпорации General Dynamics. За собой Бейстер оставил кресло председателя совета директоров SAIC.

Считается, что лишь при нынешней госадминистрации Буша-сына бурная приватизация выгодных госзаказов обрела в США столь откровенно неэтичные – на взгляд многих, просто уродливые – формы, свидетельствующие о неуемной алчности высокопоставленных госчиновников. Ярчайшим примером тому обычно приводят компанию Halliburton (нефть, строительство, военные заказы), «вне конкурса» получившую многомиллиардный контракт на восстановление иракской нефтяной индустрии фактически лишь по той причине, что недавним ее директором был нынешний вице-президент Дик Чейни.

Но в действительности весь этот механизм раздачи контрактов «среди своих» отработан уже очень давно и при самом непосредственном участии SAIC. Поэтому совершенно не случайно, конечно, что корпорация SAIC оказалась среди первых, получивших выгодные контракты в Ираке, причем еще за несколько месяцев до начала войны. Сколь жирный кусок здесь ожидается отхватить, можно понять уже по тому, что издание Wall Street Journal назвало иракский проект «крупнейшими восстановительными работами правительства США со времен помощи Германии и Японии после Второй мировой войны». Точные суммы денег американских налогоплательщиков, которые уйдут в проект, пока неизвестны. Но уже ясно, что госадминистрация Буша дополнительно запросила в сентябре 2003 года 87 миллиардов долларов, помимо тех 3,7 млрд, что выделяются на Ирак ежемесячно. Согласно приблизительным оценкам, за ближайшие годы эта сумма в общей сложности может вырасти до 200-500 миллиардов долларов [SP03].

На сегодняшний день SAIC, вероятно, является самой влиятельной в американской госадминистрации компанией, о которой большинство людей никогда не слышало. Федеральное правительство – как главный заказчик – обычно совершенно не желает, чтобы публика хоть что-то знала о том, чем занимается SAIC. А благодаря своему статусу ЗАО, весьма необычному

для крупного господрядчика, SAIC удается также постоянно пребывать вне досягаемости обременительных проверок финансовых органов и обеспокоенных инвесторов. Еще одна из важных особенностей в деятельности SAIC – мощная диверсификация бизнеса и огромное количество сравнительно небольших заказов. В 2003 году корпорация одновременно работала над выполнением 8 с лишним тысяч контрактов, из которых более 5300 – это заказы правительства США, главным образом спецслужб и Пентагона [ВАОЗ].

Когда Пентагон решил собрать и подготовить команду иракских эмигрантов, чтобы она помогла США в восстановлении послевоенного Ирака, контракт на эту работу был заключен с SAIC. Когда губернатор Мэриленда Роберт Эрлих решил организовать экспертизу безопасности закупаемых штатом электронных машин голосования, он поручил это SAIC. Когда Армия США решила приступить к решению весьма деликатной задачи по уничтожению старого химического оружия на полигоне Aberdeen Proving Ground, контракт был заключен с SAIC. Национальный онкологический институт США (National Cancer Institute) обратился за помощью к SAIC при организации работ в исследовательском центре Frederick, шт. Мэриленд (здесь в рамках 1,25-миллиардного контракта около 1500 сотрудников корпорации занимаются, среди прочего, разными аспектами применения биологического оружия).

Бывают у SAIC и весьма необычные контракты. Например, национальное Управление безопасности транспортных перевозок (TSA) решило, что нуждается в серьезной помощи при утилизации гигантского количества всевозможных вещей, после 11 сентября 2001 г. интенсивно конфискуемых при досмотре авиапассажиров – маникюрных ножниц, газовых баллончиков, праздничных хлопушек, перочинных ножичков и т.д. Кому-то может показаться, что для разгребания всего этого хлама намного дешевле было бы нанять какие-нибудь небольшие фирмы при аэропортах. Но в государственных структурах США считают в корне иначе, и многомиллионный контракт на эти работы был доверен, ясное дело, надежной компании SAIC [SS03].

Одна из важнейших областей работы корпорации – это, конечно же, инфотехнологические спецпроекты. В лаборатории SAIC в г. Аннаполисе, штат Мэриленд, неподалеку от Форт-Мида, штаб-квартиры Агентства национальной безопасности США, команда из 150 человек разрабатывает для АНБ новое ПО проходки данных – эффективный инструментарий для анализа гигантских объемов материалов радиоперехвата, собираемых от коммуникационных сетей по всей планете. Объявленная стоимость данного суперсекретного проекта, получившего кодовое название Trailblazer, – 282 миллиона долларов.

Вот еще один, совсем свежий пример. В ноябре 2003 г. под сильнейшим нажимом Федеральной комиссии по связи (FCC) в США вступили в действие новые правила, согласно которым все пользователи сотовых телефонов теперь могут сохранять за собой привычный телефонный номер, переходя от одного провайдера мобильной связи к другому. FCC провела эти правила в жизнь к великому удовольствию публики, несмотря на сильнейшие протесты и сопротивление со стороны телекоммуникационных компаний, терявших надежный инструмент

привязки абонентов, а взамен получавших лишь новые технические проблемы.

На фоне множества весьма непопулярных решений [FA03], принятых FCC за то время, что ее возглавляет Майкл Пауэлл (сын госсекретаря бушевской администрации, генерала Колина Пауэлла), подобная забота о нуждах простых граждан выглядела, прямо скажем, необычно. Но вскоре все стало намного понятнее, когда выяснилось, что в этом проекте была активно замешана корпорация SAIC. Вероятно, прослушивающие сотовые телефоны спецслужбы слишком утомила ситуация, при которой абоненты мобильной связи все время меняют номер при смене провайдера. Интересы абонентов и тех, кто за ними приглядывает, здесь полностью совпали – и вот на государственном уровне принято твердое решение о постоянном закреплении номера за владельцем. Ну, а техническое обеспечение деликатного дела, как обычно, поручили SAIC. Корпорация наняла 90 человек, которые примерно за три месяца создали систему обмена телефонными номерами между провайдерами [OR03].

При подобном состоянии дел вряд ли кого уже может удивить, что сопровождение важнейшей для власти задачи по внедрению в жизнь электронных систем голосования поручили самой надежной фирме – Science Applications International Corp.

Глава 8. Обратная сторона луны

Страницы жизни героя, 1956. Бюро подготовки общественных беспорядков

Непримиримая борьба с угрозой мирового коммунизма всегда была для Гувера одной из главных целей жизни. А уж в 1950-е годы – рост мощи СССР, укрепление социализма в Восточной Европе и в Китае – более страшной опасности, чем большевизм, для шефа ФБР, наверное, не существовало. На словах, по крайней мере. Но вскоре после бесславного заката звезды Джозефа Маккарти, вконец спившегося и спятившего сенатора от штата Висконсин, при непосредственной помощи Гувера разжигавшего пламя антикоммунистической «охоты на ведьм», в методах борьбы с политическими противниками образовался определенный вакуум.

В 1956 году Гувером был запущен существенно иной тайный проект, получивший название COINTELPRO, или Counter Intelligence Program – «контрразведывательная программа». Под этим малозначащим наименованием в действительности скрывались принципиально новые формы работы, изначально по своим целям направленные на подрыв компартии США. Секретная программа COINTELPRO выходила очень далеко за рамки обычной деятельности ФБР по сбору информации и отлову нарушителей закона или иностранных шпионов. В методы COINTELPRO входил целый арсенал грязных трюков, служивших разрушению изнутри компартии и других «антиамериканских» организаций: стравливание лидеров запуском в прессу ложных слухов, подбивание партийных активистов на акты экстремизма с помощью внедренных провокаторов, подстраивание прочих всевозможных провокаций и множество

нечистоплотных операций на основе заранее пущенной дезинформации. По сути дела, COINTELPRO превращала ФБР из правоохранительного органа в свою собственную противоположность– в ведомство по подготовке общественных беспорядков.

Поскольку в умелых гуверовских руках инструменты COINTELPRO оказались весьма эффективными, в начале 1960-х годов их начали применять против других радикальных организаций, в первую очередь – против Ку-Клукс-Клана в южных штатах страны. Успешная борьба нелегальными методами с расистами-экстремистами принесла свои плоды, но вместе с подрывом деятельности ККК сфера применения COINTELPRO стала распространяться на другие политические движения, порой весьма далекие от экстремизма, но активно не нравившиеся Гуверу или его начальству.

Во времена президента Линдона Джонсона, когда общественность и особенно молодежь активно протестовали против войны США во Вьетнаме, мишенью тайных мероприятий COINTELPRO стал уже весьма обширный ряд организаций – Студенческий ненасильственный оргкомитет (SNCC), партия чернокожих радикалов «Черная пантера», группы «новых левых», такие как Студенты за демократическое общество (SDS). В конечном же счете под пристальное внимание агентов ФБР стала попадать любая мало-мальски активная пацифистская группа, организовывавшая акции протеста против вьетнамской войны. Борьба федеральной полиции с этими организациями имела уже чисто идеологическую подоплеку, поскольку абсолютно никак не была связана с преследованием преступников или предотвращением насилия.

В конце концов Америка все же узнала, что за грязными делами втихаря занимается доблестное ФБР. В ночь на 8 марта 1971 года кто-то вломился в небольшой офис отделения Бюро в городе Медиа, штат Пенсильвания, и похитил хранившиеся там сотни документов. Вскоре выяснилось, что сделала это группа общественных активистов, называющих себя «Гражданская комиссия по расследованию деятельности ФБР». Похищенные документы давали наглядное представление о грандиозных масштабах слежки и прослушивания, которые федеральная полиция вела не только в отношении Черных пантер, левацких организаций, Еврейской лиги обороны или Ку-Клукс-Клана, но также против множества обычных граждан либеральных взглядов, участвовавших в антивоенных демонстрациях или собиравших в своем доме молодежь.

Копии документации ФБР были разосланы некоторым членам Конгресса, а также в ряд печатных изданий. И хотя генеральный прокурор Джон Митчел настоятельно попросил прессу не публиковать ничего из этих бумаг, фрагменты все же появились в печати. Главной причиной возмущения журналистов было то, что под наблюдением полиции находилось множество людей, не совершивших абсолютно никаких преступлений. На одном из похищенных документов стоял штамп COINTELPRO – кодовое название наиболее секретных и грязных операций ФБР. Этим названием заинтересовались некоторые репортеры, начавшие собственное расследование – и Гуверу пришлось не мешкая, уже в апреле, свернуть все операции по этой программе. Что интересно, членов Гражданской комиссии по расследованию деятельности ФБР так и не

смогли поймать.

Широкая публика наконец узнала, насколько глубоко ФБР вторгается в частную жизнь граждан, ни в чем не преступающих закон. Один из высоких руководителей Бюро впоследствии признал, что взлом офиса в Медиа стал своего рода событием-водоразделом, радикально «изменившим образ ФБР, возможно навсегда, в умах многих американцев».

Далее последовало множество новых критических и разоблачительных публикаций, а также несколько гневных выступлений и протестов политиков в Конгрессе. Самой выдающейся в этом ряду стала речь конгрессмена Хейла Боггса, обличавшего ФБР за беззаконные подслушивания телефонных разговоров своих коллег и засылку провокаторов в студенческие городки: «Если ФБР берет на вооружение тактику советского КГБ и гитлеровского гестапо, значит, давно уже пора сделать так, чтобы нынешний директор оставил свой пост. Министру юстиции уже давно пора предложить мистеру Гуверу подать в отставку».

Очень показательной была реакция на эти обвинения со стороны первых лиц государства. Президент Ричард Никсон заявил, что подобные нападки на Гувера несправедливы, а министр юстиции Митчелл вообще потребовал, чтобы Боггс «немедленно взял свои слова назад и извинился перед великим человеком и преданным родине американцем».

Жажда биометрии

В эпоху Холодной войны и острого идеологического противостояния двух систем советская практика поголовной паспортизации-регистрации населения, помнится, трактовалась в «свободном западном мире» как один из порочных атрибутов тоталитарного общества. Теперь же, когда от лагеря социализма, считай, ничего не осталось, вдруг выясняется, что расхождения в этом вопросе носили чисто косметический характер. А постоянная и надежная идентификация собственных граждан – причем, желательно, высокотехнологичными методами – это, как заверяют ныне почти все правительства, очень удобная и полезная вещь для любого государства, как на Востоке, так и на Западе. Более того, теперь паспорт с биометрической информацией владельца преподносится обществу не иначе, как гарант безопасности и гражданских свобод.

Война – это мир, паспорт – это свобода или Как приходит биометрия

Вряд ли удивительно, что главной движущей силой здесь стали США, где после 11 сентября 2001 года госадминистрация всерьез вознамерились защитить страну от террористических угроз с помощью биометрических систем идентификации личности. На высоких этажах власти кто-то очень крепко вбил себе в голову, что опознание людей с помощью биометрии – цифрового снимка лица, отпечатков пальцев, рисунка радужки или сетчатки глаза – резко повышает уровень безопасности. Процесс внедрения этих технологий идентификации начался уже давно, однако после событий 11 сентября в государственных структурах США и других стран спрос на биометрические системы опознания подскочил чрезвычайно

резко. И хотя эксперты упорно и постоянно твердят о незрелости технологии и высокой степени ошибок в реальной эксплуатации, в США уже полным ходом запущена машина закупок и установки соответствующего оборудования. Ибо Конгресс категорически установил весьма сжатые сроки, в течение которых паспорта либо визы всех граждан, пересекающих границу страны, должны содержать биометрическую информацию.

Власти постановили, что снятие отпечатков пальцев и цифровых снимков с иностранцев, прибывающих в США, необходимо срочно начать в воздушных и морских портах уже с января 2004 года. Отныне эти биометрические идентификаторы подлежат добавлению в соответствующие записи правительственной базы данных. Биометрическое сканирование на сухопутных границах с Мексикой и Канадой, на которые приходится около 80% из 440 миллионов ежегодных иммиграционных проверок, должно начаться в 2005 году. Но самый крутой, наверное, срок положен Конгрессом на 26 октября 2004 года, поскольку после этой даты все иностранцы, желающие попасть в США, обязаны иметь в своих визах либо паспортах биометрическую информацию идентификации. Очевидно, что это весьма усложняет жизнь сотрудникам 210 посольств и консульств США по всему миру, поскольку в большинстве случаев именно им придется заниматься снятием биометрии и последующей вклейкой чипов или полосок с идентификатором в паспорта/визы. Прежде, как известно, около 37% обращающихся за американской визой (граждане «дружественных» стран), получали ее без долгих формальностей по почте, если их личные данные удовлетворяли определенным критериям на благонадежность. По новым же порядкам биометрического сканирования не избежать никому [ВРОЗ].

Если оценивать ситуацию глобально, то в деле внедрения хайтек-паспортов на основе смарт-карт пока что явно лидирует Восток. Так, осенью 2003 г. правительством Тайваня объявлено, что в стране завершена начатая годом раньше выдача гражданам 22 миллионов идентификационных карточек на основе технологии Java. На Тайване данная инициатива была запущена с подачи Национального бюро страхования здоровья для борьбы с участившимися случаями «кражи личности». Другими словами, компетентные органы сочли, что слишком часто одни люди стали выдавать себя за других для получения оплаченной государством медицинской помощи. Поскольку в тайваньской смарт-карте имеется 32 килобайта памяти, туда же, помимо идентифицирующих личность данных, стали записывать медицинскую информацию, контактные адреса и телефоны, номера социального страхования. Плюс, по мере появления новых приложений, обещано добавлять и другие данные. Еще дальше по этому пути намерен идти Таиланд, где идентификационные смарт-карты планируется выдать поголовно всему 61 миллиону граждан, причем эти карточки уже содержат биометрический идентификатор личности (отпечаток пальца), а также информацию для налоговых служб и социального обеспечения. В континентальном же Китае в 2004 году начинается самый грандиозный в масштабах планеты эксперимент – замена бумажных паспортов на смарт-карты с персональным кодом ДНК для всех 960 миллионов взрослых граждан

[CAO3][WB03].

В Западной Европе главным поборником идентификационных смарт-карт обычно выступают министерства внутренних дел. Например, в Великобритании – это лично глава Home Office Дэвид Бланкег. Однако, на сентябрьской, 2003 г., конференции правящей лейбористской партии в поддержку ввода хаитек-паспортов вдруг активно выступил и премьер-министр Тони Блэр, прежде критиковавший подобные идеи. Кто сумел Блэра переубедить – неизвестно, но теперь он всячески пытается доказать публике, что карточки-идентификаторы – это вовсе не ущемление гражданских свобод, а совсем даже наоборот – эффективный способ их защиты. Каким образом? Очень просто: в нынешнем мире массовой миграции населения и участившихся проблем с подделкой личности именно паспорта, по мнению Блэра, обеспечат гражданам подлинную социальную справедливость [JL03].

Во Франции в первых числах октября 2003 г. Министерство внутренних дел объявило, что «совершенно безопасная» электронная карточка идентификации граждан будет использоваться в этой стране к 2006 году. В чипе карты будут содержаться «персональные данные, стандартные для такого типа документов, и система криптографической аутентификации», гарантирующая подлинность паспорта. На прямой вопрос, будет ли там записана и биометрическая информация, министерство дает уклончивый ответ, ссылаясь на раннюю стадию разработки Ш-карточки. В то же время хорошо известно, что администрация Европейского Союза в целом предпринимает весьма энергичные шаги для выработки «согласованного и единого подхода в том, какая биометрическая информация должна храниться в (визовых) документах граждан третьих стран, паспортах граждан Евросоюза и в компьютерных информационных системах». Наблюдая за происходящим, европейские правозащитники из организации Statewatch констатируют, что «ныне Евросоюз, как и США, столь же увлечен идеей ввода системы массового надзора, которая гораздо больше похожа на политический и социальный контроль, нежели на борьбу с терроризмом» [ED03][TR03].

На эти обвинения защитников гражданских свобод власти неизменно отвечают примерно так: «Все делается во имя человека, все для блага человека». Для всякого бывшего гражданина СССР чем-то очень знакомым веет от этих слов…

Лицо как удостоверение или Почему биометрия так нравится властям и бизнесу

В Minority Report, мрачном фантастическом фильме Стивена Спилберга, главным «удостоверением личности» людей будущего являются их глаза – все операции идентификации и определения полномочий на доступ осуществляются компьютерами по рисунку сетчатки. Поэтому, чтобы уйти от вездесущих стражей порядка, подставленному главному герою приходится сделать нелегальную операцию по замене глаз. В жизни же реальной в качестве аналогичного эквивалента «универсального идентификатора», похоже, все чаще пытаются использовать лицо. Одна из главных тому причин – для опознания человека по лицу требуется

значительно меньшее его участие и сотрудничество, нежели для опознания по другим биометрическим характеристикам. Более того, идентификацию по лицу можно делать практически незаметно. Причем тут для смены личности и пластическая операция не слишком поможет – во всяком случае, так заверяют некоторые специалисты, совмещающие науку и бизнес по продаже подобных систем опознания.

Один из наиболее заметных, т.е. чаще других упоминаемых в прессе, экспертов подобного рода – д-р Джозеф Атик, основатель, президент и исполнительный директор биометрической корпорации Visionics, а после сравнительно недавнего слияния/укрупнения – теперь и глава более мощной фирмы Identix. Атик и его коллеги разработали известную систему FaceIt – специализированное программное обеспечение для распознавания лиц, автоматически выделяемых в кадрах видеосъемки телекамер слежения, и для последующего поиска этих лиц в базах данных о людях, находящихся в розыске. Вообще-то говоря, база данных может быть, конечно, какая угодно – знаменитых людей, важных гостей, жильцов дома – просто наибольшим коммерческим спросом пользуются именно системы полицейского применения.

Следящая система сканирования лиц, излагая в нескольких фразах, работает следующим образом. Видеосигнал от камеры постоянного наблюдения преобразуется в последовательность цифровых фотографий. Программа сканирования выделяет на фотографии лица и проводит измерения лицевых параметров, используя в качестве базы отсчета глаза «объекта». Сделанные замеры сравниваются с соответствующими параметрами фотографий, предварительно накопленных в базе данных. Когда обнаруживается «близкое» соответствие, оператору системы подается сигнал тревоги. В программе Visionics FaceIT, в частности, процедура сравнения фотографий выглядит так. Два фото соотносятся друг с другом по шкале от 0 до 10. Здесь «0» означает отсутствие совпадений параметров, а «10» – идеальное совпадение. В FaceIT по умолчанию в качестве порогового значения для «близкого сходства» выбрано 8,5. Вообще же говоря, порог подстраивается оператором, и последствия неправильного выбора решающим образом влияют на эффективность программы. Если задать порог слишком высоким, то «плохих ребят» отловить просто не удается. Если задать слишком низким, наоборот – система начинает бить тревогу непрерывно, считая «плохими» всех подряд.

Но даже если порог выставлен очень аккуратно, система, как показывает практика, все равно ошибается довольно часто, давая обычно неверное положительное опознание. Происходит это, главным образом, из-за далекого от идеала качества анализируемой фотографии. На ошибки влияет множество сопутствующих факторов: изменения в освещении объекта, что за предметы оказываются на заднем фоне, конкретное положение лица и его выражение, наличие очков, расположение снимающей камеры и качество даваемой ею картинки. Все это способно решающим образом влиять на исход опознания и относится не только к фотографиям от видеокамеры, но и к «эталонам» из базы данных [RS02].

Несмотря на это, по убеждению Атика, система FaceIT намного эффективнее других средств в деле поимки преступников и террористов,

поскольку те обычно не предоставляют заранее свои отпечатки пальцев или снимки радужки глаза, а вот фотографии намного легче раздобыть при скрытой оперативной съемке «объекта». Технология FaceIt не исследует «текущий» вид лица. Здесь работа ведется над аналитическими замерами характерных лицевых элементов и их взаимными соответствиями. Поэтому, говорит Атик, если добавить усы, очки и даже сделать стандартную пластическую операцию, это не изменяет фундаментальных лицевых параметров. Более того, исследования показывают, что расположение характерных особенностей на лице человека является сверхизбыточным. Важных черт гораздо больше, чем нужно для положительной идентификации в FaceIt. Специалисты выделяют таких особенностей около 80, в то время как для опознания программе требуется всего лишь 14. Некоторые из особенностей можно «заблокировать лицевой растительностью» или изменить с помощью силиконовых инъекций, тем не менее, заверяют в Visionics, первоначальное лицо все еще можно выявить и «восстановить исходную личность» [JA01].

Но на самом деле все эти декларации по преимуществу одна лишь теория да шумная маркетинговая трескотня. Систему FaceIt продают в разные страны не первый год, в рекламных релизах не гнушаясь фразами типа: «Благодаря данной технологии еженедельно в мире задерживается несколько известных террористов», однако на самом деле конкретного примера отлова хотя бы одного «известного террориста» общественности не представили ни разу.

С другой же стороны, имеется множество свидетельств, что технологии распознавания лиц вообще (и FaceIt в частности) пока еще весьма незрелы для реального применения в системах безопасности. Так, на проходившей в феврале 2002 года в США конференции Биометрического консорциума выступал с докладом один из руководящих чинов Пентагона д-р Стивен Кинг, представивший результаты трехмесячного тестирования в одной из военных лабораторий системы FaceIt (как одной из лучших в своем классе). Результаты экспериментов на сотрудниках-добровольцах показали, что реальные рабочие характеристики продукта Visionics и близко не соответствуют тем, что декларируются изготовителем. Верная идентификация человека из массива численностью около 3 сотен происходила лишь в 51% случаев. В условиях реального применения для контроля доступа на объект, понятное дело, такие характеристики оказываются мало подходящими. В течение 2002-2003 гг. к такому же выводу пришли и в администрации нескольких американских аэропортов (флоридского «Палм Бич», бостонского «Логан»), где аналогичное оборудование тестировалось на сотрудниках. Аппаратура и здесь верно срабатывала лишь в половине случаев, давая очень много ложных опознаний, поэтому в конечном итоге от ее применения в аэропортах было решено отказаться [MZ02][HB02].

В августе 2003 г. полицейское управление города Тампа, штат Флорида, после двух лет эксплуатации демонтировало за бесполезностью ПО опознания лиц FaceIt, работавшее совместно с камерами наружного наблюдения. Сеть таких камер обеспечивает надзор за публикой в городском парке развлечений Айбор-сити. Предполагалось, что в комплекте с базой данных, содержащей 30 000 фотографий известных

бандитов, преступников и сбежавших из дома детей, техника повысит эффективность работы полиции. Однако, два года работы системы не принесли ни одного успешного результата, будь то автоматическое опознание разыскиваемых или арест подозреваемых лиц [BR03].

Повсеместные попытки внедрения программ автоматического распознавания лиц чрезвычайно тревожат правозащитные организации. Что именно беспокоит правозащитников, и как конкретно системы дистанционного опознания угрожают праву человека на тайну частной жизни? Одна из наиболее очевидных угроз заключается в том, что с течением времени эта технология в сочетании с постоянно растущим количеством телекамер слежения становится все более всепроникающей и навязчивой. Практика показывает, что однажды установленная, аппаратура подобного рода редко сохраняет за собой те функции, которые предназначались ей первоначально. Новые способы применения оборудования слежения возникают, по сути дела, сами собой, давая операторам систем и властям захватывающее ощущение всеведения, при этом люди постоянно утрачивают элементы тайны личной жизни, даже того не замечая. Типичнейший пример – использование телекамер на американских пляжах. В середине 1990-х их начали устанавливать для наблюдения за морем и для прочих нужд метеослужбы. Затем, благо аппаратура уже на месте, камеры стали снабжать поворотным механизмом и приспособили для помощи службе правопорядка и Береговой охране. Наконец, в 2002 году на пляжах Флориды и Вирджинии к телекамерам решили добавить и системы распознавания лиц [PBO3] [QA03].

Другая важнейшая проблема – угрозы злоупотреблений системой. Недавнее расследование, проведенное журналистами в Детройте, показало, что сотрудники полиции, имеющие доступ к базам данных правоохранительных органов в штате Мичиган, регулярно используют их для сбора информации об интересных (для них или их друзей) женщинах, для угроз автовладельцам, для слежки за неверными супругами и даже для запугивания политических оппонентов. И реальность такова, что чем больше людей получает доступ к подобным базам данных, тем больше становится вероятность злоупотреблений [ME01].

Адепты системы FaceIT и ей подобных любят подчеркивать, что база данных ведется лишь на преступников и находящихся в розыске лиц, а отсканированные снимки «честных людей» в ней не сохраняются. Однако опыт использования этой же системы для распознавания автомобильных номеров в аэропортах свидетельствует об обратном – на постоянной основе запоминаются ВСЕ зафиксированные номера машин, заезжавших на территорию объекта. Аналогичную процедуру, кстати, рассматривают лондонские власти в отношении ВСЕХ машин, направляющихся в центр города (благо, телекамеры слежения уже установлены на всех подъездных дорогах) [JR01].

Распознавание же лиц по самой своей природе является особо выдающейся технологией для злоупотреблений, поскольку применение здесь возможно в пассивной форме, без оповещения наблюдаемых или получения их согласия на участие в процедуре опознания. Современные камеры с хорошей оптикой без труда могут схватывать лица с расстояния более 100 метров, поэтому устанавливать подобную аппаратуру можно

практически незаметно в любых местах. А значит, как только появятся для этого технические возможности, появится искушение и сохранять снимки всех попавших в поле зрения камеры.

И раз уж речь зашла о камерах наблюдения, то имеет смысл отметить любопытную интернет-публикацию на эту тему – большую аналитической статью немецкого исследователя Марка Весслера «Как отыскивать скрытые камеры». Обстоятельный разговор о всевозможных системах слежки за ближним предстоит в следующей главе, здесь же имеет смысл привести итоговое заключение автора, глубоко занимавшегося изучением ситуации: «Имейте в виду, что, вопреки широко распространенному в обществе мнению, скрытые камеры – это НЕ редкость» [MR02].

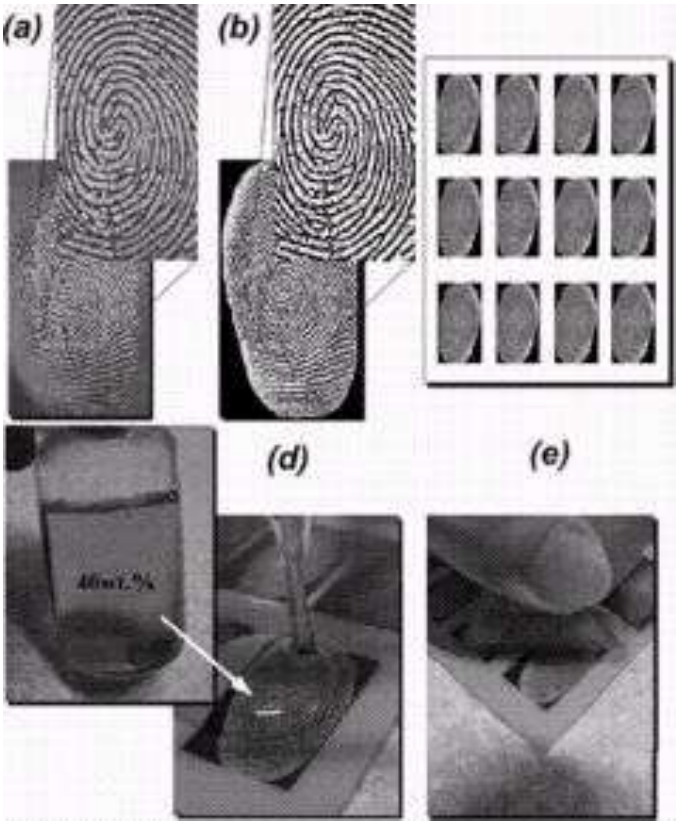
Забавные игрушки или Почему надежность биометрических систем – это сплошной обман

Государственные структуры, радеющие за повсеместное применение биометрических систем опознания, и компании, продающие на рынке такого рода аппаратуру, всячески заверяют общество, что это – высшее достижение современных технологий безопасности, очень надежное и практически не поддающееся обманам и злоупотреблениям. Реальное же положение дел в этой области, мягко говоря, выглядит абсолютно иначе.

В начале 2002 года японский криптограф Цутомо Мацумото в высшей степени наглядно продемонстрировал, что с помощью подручного инвентаря и недорогих материалов из магазина «Умелые руки» можно обмануть практически любую из биометрических систем контроля доступа, идентифицирующих людей по отпечатку пальца. Мацумото и группа его студентов в Университете Иокогамы не являются профессионалами в области тестирования биометрических систем, а занимаются математическими аспектами защиты информации. Однако, даже чисто любительского энтузиазма исследователей хватило на то, чтобы создать две крайне эффективные технологии для изготовления фальшивых дактилоскопических отпечатков [TM02].

Изготовление фальшивого пальца по методу Мацумото:

(а)



улучшение качества снятого отпечатка;
(b) создание цифрового отпечатка-образа сканированием;
(c) создание из нескольких образов маски для отливочной формы;
(d) заполнение формы жидким желатином;
(e) остудить форму в холодильнике и осторожно вынуть «палец».

При первом (тривиальном) способе японцы делали непосредственный слепок с пальца «жертвы», для чего использовался обычный пищевой желатин и формовочный пластик, применяемый авиа– и судомоделистами. Полупрозрачную желатиновую полоску-отпечаток можно незаметно прилеплять к собственному пальцу и обманывать компьютерную систему доступа даже в присутствии поблизости охранника. Эта нехитрая технология сработала в 80% случаев при тестировании более десятка коммерческих приборов биометрической защиты.

Но еще более эффективен оказался «высокотехнологичный» способ, разработанный группой Мацумото в воодушевлении от первого успеха. При этом методе уже не требуется сам палец, а просто аккуратно обрабатывается один из оставленных им отпечатков (согласно исследованиям экспертов, человек ежедневно оставляет на различных предметах в среднем около 25 отчетливых «пальчиков»). Взяв отпечаток «жертвы» на стекле, исследователи улучшили его качество с помощью циан-акрилатного адгезива (паров супер-клея) и сфотографировали результат цифровой камерой.

Затем с помощью стандартной программы PhotoShop на компьютере была повышена контрастность снимка, после чего его распечатали принтером на прозрачный лист-транспарант. Для изготовления же объемного отпечатка Мацумото воспользовался методом фотолитографии:

в магазине для радиолюбителей студенты купили светочувствительную печатную плату-заготовку, спроецировали на нее «пальчик» с транспаранта и вытравили отпечаток на меди. Эта плата стала новой формой для изготовления желатинового «фальшивого пальца», который оказался настолько хорош, что обманывал практически все из опробованных биометрических систем, как с оптическими, так и емкостными сенсорами.

Более того, после некоторой тренировки желатиновый слепок позволил исследователям-любителям преодолевать и более продвинутые системы, оборудованные «детекторами живого пальца», реагирующими на влажность или электрическое сопротивление. И нет никакого сомнения, что профессионалам в этой области удается проделывать много больше. Короче говоря, пользуясь комментарием известного крипто-гуру Брюса Шнайера, можно говорить, что полученных результатов вполне достаточно для полной компрометации подобных систем и для того, чтобы отправить многочисленные компании дактилоскопической биометрии «паковать вещички» [BS02].

Самое же неприятное, что настоящим специалистам в области биометрии все эти факты известны давным давно. Широкая публикация в Интернете результатов группы Мацумото позволила привлечь внимание к значительно более раннему исследованию голландцев Тона ван дер Путте и Иероэна Койнинга, уже давно разработавших собственную технологию, обманывающую 100% из доступных на рынке биометрических систем распознавания отпечатка пальца. Все попытки этих ученых достучаться до компаний, изготовляющих оборудование, закончились ничем, а полученные ими результаты просто всяческими способами замалчивались [PKOO].

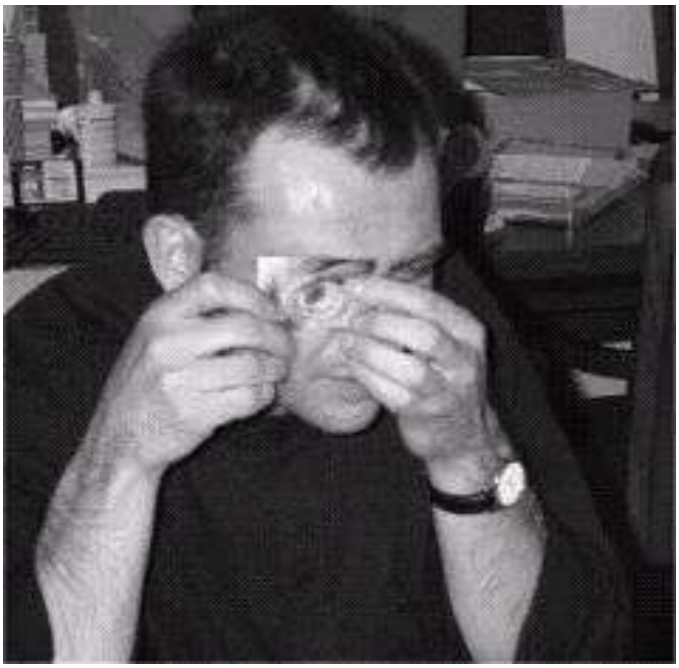
Вслед за эффектной работой японских исследователей из Иокогамы, на страницах средств массовой информации стали появляться сообщения и о других исследовательских проектах, очень серьезно компрометирующих биометрические системы. Так, летом того же 2002 года немецкий компьютерный журнал «c't» опубликовал результаты собственного обширного исследования, посвященного изучению 11 систем биометрической верификации на основе распознавания лиц, пальцев и радужной оболочки глаз пользователей [TZ02].

Выводы экспертов журнала вполне однозначны: биометрические системы для потребительского рынка пока что не достигли того уровня, когда в системах доступа их можно рассматривать в качестве реальной альтернативы традиционным паролям и персональным идентификационным номерам. Все из изучавшихся систем приходится рассматривать скорее как забавные игрушки, а не «серьезные средства защиты» (как заявляют их изготовители), поскольку преодоление каждого из устройств не вызвало у исследователей существенных проблем. Важно подчеркнуть, что эксперты «c't» ориентировались в первую очередь на самые тривиальные методы обмана систем, не требующие сколь-нибудь серьезных профессиональных навыков. Так, систему опознания лиц FaceVACS-Logon немецкой фирмы Cognitec удается обмануть даже с помощью подсовывания фотографии зарегистрированного пользователя, снятого предварительно цифровой камерой. Если же в системе работает

более чувствительное (и менее дружелюбное к пользователю) программное обеспечение, анализирующее характерные признаки движения живого человека, то для обмана успешно применен экран мобильного компьютера-ноутбука, демонстрирующий видеоклип с лицом «жертвы».

Обман системы опознания лица

Несколько более сложно было преодолеть систему Authenticam BM-ET100 фирмы Panasonic для опознания радужной оболочки глаза, поскольку здесь инфракрасные датчики реагировали не только на характерный узор изображения, но и на иную глубину расположения зрачка. Тогда в снимке глаза, распечатанном на матовой бумаге принтером высокого разрешения, исследователи проделали небольшое отверстие на месте зрачка, куда и подставляли собственный глаз при опознании. Этого ухищрения для обмана системы оказалось вполне достаточно.



Обман системы опознания по радужной оболочке глаза

Что же касается систем аутентификации пользователя по отпечатку

пальца с помощью емкостного сенсора на «мышке» или клавиатуре, то здесь самым тривиальным способом обмана является повторное «оживление» уже имеющегося отпечатка, оставленного зарегистрированным пользователем. Для «реанимации» остаточного отпечатка иногда бывает достаточно просто подышать на сенсор, либо приложить к нему тонкостенный полиэтиленовый пакет, наполненный водой. Подобные трюки, в частности, весьма удачно опробованы на мышках ID Mouse фирмы Siemens, оснащенных емкостным сенсором FingerTIP производства Infineon. Еще эффективнее срабатывает более тонкая технология, когда оставленный «жертвой» отпечаток на стекле или CD посыпается тонкой графитовой пудрой, лишний порошок сдувается, а сверху накладывается липкая лента, фиксирующая характерный узор папиллярных линий. Прикладывание этой ленты обманывает не только емкостные, но и некоторые более строгие оптические сенсоры. Наконец, «искусственный палец», отлитый в парафиновой форме из силикона, позволил исследователям преодолеть все из шести протестированных систем на основе дактилоскопии.

Обман дактилоскопических систем опознания

Любопытства ради эксперты «c't» немного поиграли не только с лобовыми атаками на основе «фальшивых» частей тела, но и с более тонкой технологией «повторного воспроизведения». В этом случае подлинная биометрическая информация незаметно перехватывается на канале между сенсором и проверяющей программой, а затем вновь воспроизводится в нужный момент для получения нелегального доступа. Как показали эксперименты, коммуникационный порт USB, через который обычно подсоединяются к ПК биометрические датчики, легко допускает подобные манипуляции, поскольку информация здесь никак не шифруется.

Справедливости ради следует признать, что все из опробованных систем относятся к сравнительно недорогому рынку потребительских товаров, т.е., грубо говоря, не предназначены для защиты секретных объектов. С другой стороны, у экспертов журнала просто не было доступа к исследованию дорогих «настоящих» систем, а, кроме того, все выявленные слабости оборудования относятся не столько к собственно сенсорам, сколько к алгоритмам программного обеспечения. И если более

мощное ПО уже существует, то почему не применяется? Как известно, производители биометрических систем всячески уклоняются от внятных ответов на подобные вопросы, предпочитая напирать на то, что лабораторные эксперименты весьма далеки от условий реальной эксплуатации.

В августе 2003 г. пришло известие, что и этот аргумент производителей пытливые исследователи демонстративно раздолбали. В Германии, на проходившем под открытым небом близ Берлина слете хакеров Chaos Computer Camp, свою исследовательскую работу продемонстрировали два местных умельца, именующие себя Starbug и Lisa. Новой компрометации вновь подверглись сканеры, идентифицирующие людей по отпечатку пальца, поскольку именно такое оборудование все чаще начинают использовать в торговых точках для электронной регистрации покупок. Методика преодоления системы разработана для реальных условий и позволяет обманывать сканер даже в присутствии надзирающего ока продавца или охраны.

Метод весьма дешев и при наличии навыка позволяет подделывать отпечаток, по характеристике авторов, «на лету» с помощью тонкой прозрачной полоски из латекса. Технология подделки с некоторыми модификациями повторяет способ группы Мацумото: отпечаток жертвы снимается с помощью графитовой пудры и липкой ленты-скотча; со слепка (еще лучше, с нескольких слепков) делается цифровой снимок, качество папиллярного рисунка улучшается специальной графической программой, которая переводит изображение на покрытую светочувствительным слоем фольгу печатной платы; после травления на плате остается объемный рельеф нужного пальца, и по этой форме из жидкого латекса изготовляется ложный отпечаток. После высыхания небольшая тонкая полоска прикрепляется к пальцу и становится практически незаметна. При надлежащем навыке на всю процедуру подделки уходит меньше 10 минут.

Starbug и Lisa подчеркнули, что целенаправленно занялись разработкой своей атаки для того, чтобы продемонстрировать серьезность угрозы и неискренность изготовителей. Поэтому способ немецких хакеров не только базируется на уже известных приемах, но и продемонстрирован в реальной эксплуатации. Чтобы не конфликтовать с законом, Starbug и Lisa сделали отпечатки пальцев друг друга и сделали в магазине компьютерного оборудования «контрольные закупки» с помощью поддельных накладок [АНОЗ].

Мифы биометрии или Почему биометрическое опознание следует запретить

Проведенный в конце 2002 года в США социологический опрос показал, что предупреждения компетентных экспертов о недостаточной надежности и небезопасности биометрических систем идентификации явно не доходят до массового сознания американского общества. Исследование, проведенное по заказу Бюро судебной статистики США, свидетельствует, что от 75 до 90 процентов опрошенных по телефону американцев хотели бы видеть большее применение биометрии как в частном, так и в общественном секторе. В частности, респонденты полагают, что системы

биометрического сканирования повысят безопасность жизни, если их применять в таких областях: проверка личности по базам осужденных преступников при покупке оружия (91%); верификация личности при покупке по кредитной карте (85%); снятие наличных в банкомате (78%); доступ к документам с конфиденциальной информацией, таким как медицинская карта или финансовая отчетность (77%); проверка биографических данных (76%). Это же исследование показывает, что в представлениях общественности биометрия тесно связана с защитой от «краж личности», сильно возросших за последние годы [LR03].

Достаточно очевидно, что подобные взгляды общественного сознания, не понимающего особенностей технологии, являются прямым результатом весьма успешной государственной «промывки мозгов» через СМИ и шумного рекламного гвалта коммерческих фирм, продвигающих это оборудование в качестве «наиболее надежного, современного и универсального средства безопасности».

Интересно, что в ноябре 2002 г., практически одновременно с социологическим опросом, в специализированном журнале по защите информации Info Security Magazine было опубликовано любопытное интервью с Джимом Уэйманом, несколько последних лет возглавлявшим национальный Центр тестирования биометрии США (U.S. Biometrics Test Center). Данный материал интересен прежде всего тем, что это – очень редко встречаемые в прессе честные и здравые суждения о биометрических системах защиты с точки зрения профессионала, занимающего серьезный пост в официальных структурах (точнее говоря, занимавшего, потому что ныне Уэйман уже не возглавляет Центр биометрии).

В самом кратком изложении суть оценок этого авторитетного эксперта выглядит так. Еще в 1998 году Джим Уэйман предупреждал индустрию, что сделанная ею установка на провозглашение биометрии в качестве надежного средства идентификации – это ошибка, которая будет иметь самые негативные последствия. Во-первых, потому что биометрия не является надежной. И во-вторых, потому что на самом деле она вовсе не для безопасности, а для удобства пользователей.

Прошедшие с той поры годы и новейшие технологические достижения ничуть не поколебали позицию Уэймана, по-прежнему убежденного, что биометрия вовсе не плоха сама по себе, просто на нее возлагают явно преждевременные и чрезмерные надежды. Выступая в прессе и на конференциях, Уэйман подчеркивает, что пока еще даже на подходе нет сколь-нибудь зрелых протоколов для серьезного тестирования биометрических устройств, а в производство и приобретение такого рода систем уже торопливо вбухиваются многие миллионы долларов.

Одним из наиболее заметных поборников сравнительно новой технологии является правительство США: в военном агентстве передовых исследований DARPA развернут 42-миллионный четырехлетний проект по разработке технологии биометрической идентификации для охраны посольств США по всему миру; Министерство обороны выразило желание закупить системы распознавания лиц, выделяющие и идентифицирующие людей из толпы. Список этот можно продолжать, по мнению же Уэймана, столь истовая вера правительственных боссов в биометрические системы

распознавания в определенной степени вызвана откровенными преувеличениями в заявлениях производителей биометрического оборудования – достаточно познакомиться с тем, что они провозглашают на своих сайтах и в рекламных релизах [AS02][AH02].

Другой серьезный эксперт в области биометрических систем, австралийский профессор Роджер Кларк, идет в своих заключениях существенно дальше и доказывает, что в современных условиях биометрия вообще должна быть запрещена. В работах Кларка проанализировано, сколь гигантское количество проблем возникает при широком внедрении биометрических систем опознания, сколь стремительно растет сложность мер защиты этих систем при появлении контрмер и необходимости выработки контр-контрмер.

Неизбежным следствием этого становится снижение дружелюбности систем к пользователю, высокий процент ложных-положительных и ложных-отрицательных идентификаций. Вследствие незрелости технологии, процент откровенной халтуры, и близко не делающей того, что сулят недобросовестные изготовители, в этом секторе рынка намного выше, чем в других областях индустрии инфотехнологий. Широкому распространению биометрии на рынке способствует устоявшийся в обществе миф о том, что «это круто». Вопреки другому распространенному мифу, биометрия вовсе не решает проблемы подделки и кражи личности. Более того, биометрия в действительности сама является частью этой проблемы, поскольку часто лишь упрощает такие подделки.

Наконец, биометрия закладывает чрезвычайно мощный и опасный фундамент для злоупотреблений государства и корпораций, которые получают удобнейшую технологическую возможность управлять правами доступа и вообще процедурами идентификации любой отдельно взятой личности.

При этом в современном обществе пока что абсолютно никак не отработаны механизмы борьбы со злоупотреблениями биометрией. Нет ни юридических норм, ни законов, которые бы регулировали встраивание биометрии в технологии и товары, процессы разработки биометрических приложений, практику поведения корпораций и правительственных ведомств в этой области. Как это ни поразительно, но у общества нет вообще никаких средств для адекватной защиты от биометрии. Единственное, что есть – это «дискуссии по соответствующим вопросам» в индустрии с участием правительственных чиновников.

Потенциально биометрические технологии представляют для общества чрезвычайную опасность, если и дальше допускать их нерегулируемое использование. А потому, убежден Кларк, до выработки соответствующих норм и законов, использование систем биометрической идентификации следует запретить [DV03].

Несколько иначе ту же самую мысль о необходимости законодательного запрета биометрии правозащитники формулируют следующим образом. Распознавание лиц и всякая другая биометрическая технология безопасности не должны внедряться до тех пор, пока не получены ответы на два вопроса. Первое, эффективна ли данная технология? Говоря иначе, существенно ли она повышает нашу защиту и безопасность? Если ответ «нет», то дальнейшее обсуждение утрачивает

смысл. Если же ответ «да», то следует задаться вторым вопросом: нарушает ли технология целесообразный баланс между безопасностью и свободой. Фактически, говорят правозащитники, биометрия не подходит обществу по обоим из указанных критериев. Поскольку технология работает ненадежно, она не способна сколь-нибудь существенно обеспечить безопасность. Но при этом несет в себе очень значительную угрозу гражданским свободам и правам на тайну личной жизни [QA03].

Игры в умные карты

Важнейшей технологией, лежащей в фундаменте практически всех новых хайтек-паспортов и прочих современных идентификационных документов, являются интеллектуальные пластиковые карточки, кратко именуемые смарт-карты. В настоящем разделе собраны достаточно глубокие технические подробности о реальной ситуации с (не)безопасностью смарт-карт, как технологии самого широкого назначения. Имеет смысл предупредить, что для понимания основной части данного материала подразумевается наличие у читателя хотя бы базовых знаний об основах функционирования и устройства компьютеров, а также некоторого представления о криптографии.

4 миллиона подопытных кроликов

На самом излете клинтоновской госадминистрации, осенью 2000 г. в Министерстве обороны США был начат крупномасштабный ввод новых хайтек-бейджей для идентификации персонала на основе технологии смарт-карт. В итоге свыше 4 миллионов человек, работающих в военном ведомстве, получают личные устройства с микропроцессором и памятью, получившие название «карта общего доступа».

Такая смарт-карта ценой около 8 долларов и размером примерно со стандартную кредитную карточку обеспечивает военному и гражданскому персоналу не только проход на режимные объекты или загрузку в секретные компьютерные сети, но и несет в себе массу личной информации о владельце: имя, должность и звание, номер социального страхования, фотографию. Благодаря хранящемуся в карте «сертификату» ее владелец может ставить цифровую подпись под своей электронной почтой и служебными приказами.

Кроме того, испытываются и такие варианты применения, как внесение в карту расчетных сумм за еду в служебной столовой, хранение медицинской и стоматологической информации, результаты сдачи нормативов по физической подготовке и стрельбе… Как выразился тогдашний заместитель министра обороны по кадровым вопросам Бернард Росткер, руководство Пентагона «очень возбуждено от вроде бы безграничных возможностей технологии смарт-карт». К середине 2003 года непрекращающиеся эксперименты с картами общего доступа привели к занесению в память чипа биометрической информации о владельце и к появлению возможностей бесконтактной идентификации, когда информация считывается с карты дистанционно [REOO][BBO3].

Правозащитные организации с самого начала экспериментов не

разделяли возбуждения военных начальников из Пентагона, справедливо усмотрев в этой акции закладывание основ для повсеместного внедрения цифровых идентификаторов в национальных масштабах. В том же 2000 году Дэвид Бэнисар, юрист известной правозащитной организации EPIC, предупреждал, что «военных очень часто используют как подопытных кроликов в тех ситуациях, когда опробование новшеств на гражданских лицах представляется слишком сомнительным. […] В конечном счете, опасность заключается в том, что людей станет возможным отслеживать на постоянной основе. А накапливаемые данные затем можно запросто использовать для таких целей, которые вовсе не подразумевались первоначально».

Как здесь с безопасностью?

Не подлежит сомнению, что индустрия смарт-карт переживает ныне период мощного расцвета. В 2002 году по всему миру было продано чуть меньше 2 миллиардов интеллектуальных карточек со встроенным микрочипом, а в ближайшие годы ожидается рост этих цифр в разы. Причины тому просты, коль скоро области применения смарт-карт все время расширяются: от телефонной карты до жетона аутентификации пользователя ПК, от «электронного кошелька» для хранения цифровых наличных до цифрового паспорта-идентификатора граждан. Массовое внедрение смарт-карт в повседневную жизнь сопровождается непременными заверениями официальных представителей индустрии и властей о том, что чип-карты – это наиболее безопасная из существующих на сегодня технологий, потому что такие карты чрезвычайно очень сложно, практически невозможно вскрывать. Но так ли обстоят дела на самом деле?

Типичная смарт-карта – это 8-битный микропроцессор, постоянное запоминающее устройство (ROM), оперативная память (RAM), электрически перепрограммируемая память (EEPROM или Flash, где, в частности хранится криптографический ключевой материал), последовательные вход и выход. Все это хозяйство размещается в одном чипе, заключенном в корпус – обычно, пластиковую карту размером с кредитку.

Нравится это кому-то или нет, но в действительности вскрытие смарт-карт – явление весьма давнее и распространенное повсеместно. Как свидетельствуют специалисты, примерно с 1994 года практически все типы смарт-карточных чипов, использовавшихся, к примеру, в европейских, а затем в американских и азиатских системах платного телевидения, были успешно вскрыты кракерами (т.е. криминальными хакерами) методами обратной инженерной разработки. Скомпрометированные секреты карт – схема и ключевой материал – затем продавались на черном рынке в виде нелегальных клон-карт для просмотра закрытых ТВ-каналов без оплаты компании-вещателю. Менее освещенной в прессе остается такая деятельность, как подделка телефонных смарт-карт или электронных кошельков, однако известно, что и в этой области далеко не все в порядке с противодействием взлому. Индустрии приходится регулярно заниматься обновлением технологий защиты процессора смарт-карт, кракеры в ответ разрабатывают более изощренные методы вскрытия, так что это

состязание еще далеко не закончено.

Смарт-карты в своих потенциальных возможностях имеют целый ряд очень важных преимуществ в сравнении с другими технологиями. Обладая собственным процессором и памятью, они могут участвовать в криптографических протоколах обмена информацией, и, в отличие от карточек с магнитной полоской, здесь хранимые данные можно защищать от неавторизованного доступа. Серьезная проблема лишь в том, что реальная стойкость этой защиты очень часто переоценивается. Далее будет представлен краткий обзор наиболее важных технологий, используемых при вскрытии смарт-карт. Эта информация важна для любого человека, желающего получить реальное представление о том, как происходит вскрытие защищенных устройств и каких затрат это стоит.

Вскрытие бывает разное

Классификация методов вскрытия смарт-карт может несколько различаться у разных авторов, однако наиболее часто выделяются следующие категории атак, которые обычно применяются в разных сочетаниях друг с другом.

Технологии микрозондирования, с помощью микроскопа и иглы микропробника позволяющие получить доступ непосредственно к поверхности чипа, где атакующий может регистрировать прохождение битов информации, манипулировать ими и вмешиваться в работу интегральной схемы.

Программные атаки, использующие обычный коммуникационный интерфейс процессора смарт-карты и эксплуатирующие уязвимости защиты, выявленные в протоколах, криптографических алгоритмах и других особенностях конкретной реализации схемы. Чем более зрелой является технология защиты, тем чаще приходится сочетать этот метод с двумя следующими методами атак.

Анализ побочных каналов утечки информации, когда атакующий с высокой по времени частотой снимает аналоговые характеристики колебаний в питании и интерфейсных соединениях, а также любые другие электромагнитные излучения, порождаемые элементами схемы процессора (транзисторами, триггерами и т.д.) в ходе обычной работы.

Технологии индуцирования сбоев, где, напротив, используют нештатные условия эксплуатации, чтобы вызвать ошибки в работе процессора и открыть таким образом дополнительные каналы доступа к защищенной информации.

Все технологии микрозондирования по сути своей являются разрушающими атаками. Это значит, что для их реализации требуются многие часы, иногда недели работы в условиях специализированной лаборатории, а сам исследуемый чип при этом разрушается. Остальные три категории относятся к неразрушающим атакам. Иначе говоря, после того, как злоумышленник подготовил такую атаку в отношении конкретного типа процессора и уже известной версии программного обеспечения, он может с легкостью воспроизвести ее в течение минут или даже нескольких секунд в отношении любой другой карты того же типа. При этом атакуемая карта физически не повреждается, а оборудование, использованное для атаки,

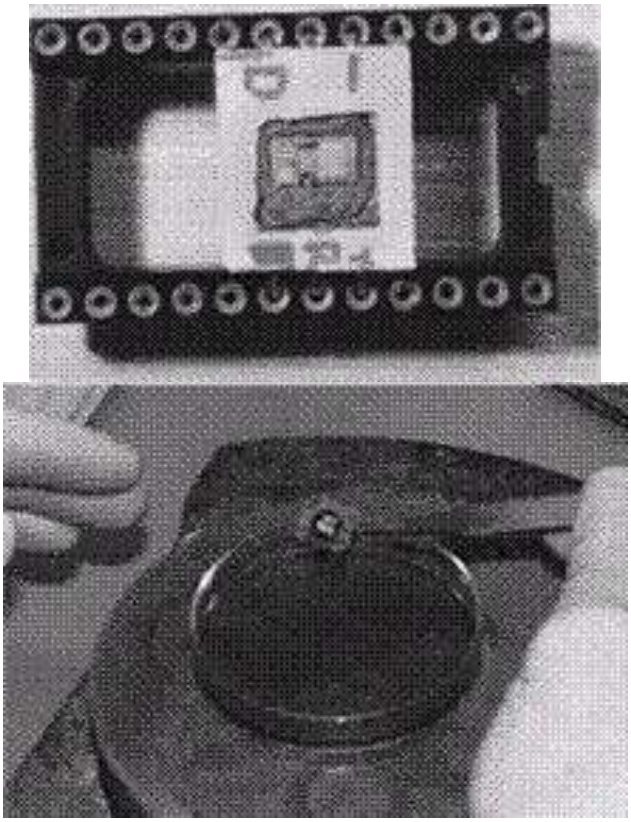
обычно можно замаскировать под обычный ридер, т.е. считыватель смарт-карт.

Очевидно, что неразрушающие атаки особо опасны, поскольку не оставляют за собой следов компрометации. Но понятно и то, что сама природа атак такого рода подразумевает детальное знание как процессора, так и программного обеспечения конкретной карты. С другой стороны, для разрушающих атак микрозондированием требуется очень мало исходных знаний о конкретной конструкции, поэтому при относительно небольшом наборе приемов они обычно срабатывают в отношении весьма широкого ряда разных чипов. Таким образом, можно говорить, что атака на новую смарт-карту обычно начинается с разрушающей обратной инженерной разработки, результаты которой помогают создать более дешевые и быстрые неразрушающие атаки. В частности, именно такая последовательность событий многократно отмечена при вскрытии карт условного доступа в системах платного телевидения [КК99].

Разрушающие атаки

Итак, к этому типу атак принято относить такие способы компрометации смарт-карт, которые сопровождаются вскрытием корпуса устройства. Публичное представление таких методов, применяемых в кракерском подполье, впервые, похоже, было сделано в 1996 году исследователями из Кембриджского университета Россом Андерсоном и Маркусом Куном в ходе Второго семинара USENIX по электронной коммерции. Еще более подробно эти технологии описаны в совместной статье Куна и Оливера Кеммерлинга 1999 года «Принципы конструирования защищенных процессоров смарт-карт», а также в последующей докторской диссертации Куна, которая, правда, в отличие от первых двух статей в Интернете не опубликована. В самом кратком изложении суть этих работ примерно такова [АК96][КК99].

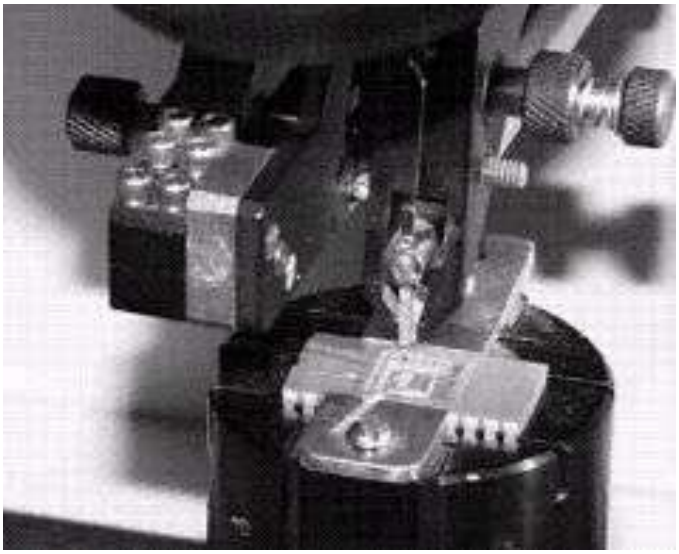
Типичный чиповый модуль смарт-карты имеет тонкое пластиковое основание размером около квадратного сантиметра с контактными зонами с обеих сторон. Одна сторона модуля видна на самой смарт-карте и контактирует со считывателем; кремниевая матрица приклеена к другой стороне основания, подсоединяясь с помощью тонких золотых или алюминиевых проводов. Та сторона пластины, где находится чип, покрыта эпоксидной смолой, там чиповый модуль вклеивается в карту. Вынуть чип из карты легко. Прежде это делали с помощью острого ножа или ланцета, срезая пластик тыльной стороны карты до тех пор, пока не покажется эпоксидная смола. Потом научились быстро вынимать чип, просто разогревая пластмассу до мягкого состояния. Далее удаляют эпоксидный слой, нанося несколько капель концентрированной азотной кислоты (» 98%). Прежде, чем кислота успевает растворить слишком много эпоксидного слоя и затвердеть, кислоту и смолу смывают ацетоном. Эта процедура повторяется от 5 до 10 раз, пока полностью не покажется кремниевая матрица. Если все было сделано аккуратно и соединительная проводка осталась неповрежденной, то чип остается полностью функциональным.



Полностью функциональный процессор смарт-карты, пластиковый корпус которой удален для экспериментов с микропробником.

Следующим этапом, если процессор совершенно новый и неизвестный, становится создание карты его схем. Сейчас для этого обычно применяют оптический микроскоп и цифровую камеру, с помощью которых делают большую, размером несколько метров, мозаику из высокого разрешения снимков поверхности чипа. У большинства чипов имеется защитный поверхностный слой (пассивация) из оксида или нитрата кремния, который предохраняет их от излучений оборудования и диффузии ионов. Азотная кислота на него не действует, поэтому для его удаления специалисты используют сложный метод сухого травления. Но это не единственная возможность для доступа к поверхности. Другим методом, особенно когда схема в целом известна, является использование игл-микропробников, которые с помощью ультразвуковой вибрации удаляют защитный слой непосредственно под точкой контакта. Кроме того, для локального удаления защитного слоя применяются лазерные резаки-микроскопы, используемые в лабораториях клеточной биологии.

Описанная техника вскрытия успешно применяется любителями-кракерами. Далее же вкратце будут описаны некоторые технологии, доступные хорошо оснащенным лабораториям, занимающимся изучением полупроводников. В мире сейчас насчитываются сотни таких лабораторий – в университетах и промышленных исследовательских центрах, к примеру. Имеется достоверная информация, что наиболее продвинутые кракеры арендуют эту технику и тщательно изучают новейшие промышленные технологии обратной инженерной разработки (подробнее об этом в следующем разделе «Возня в подполье, война на небесах»).



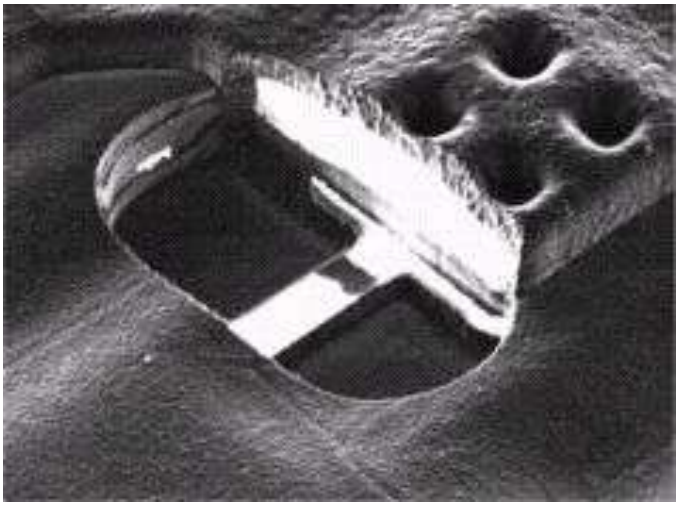
Микрозондирование чипа, извлеченного из смарт-карты

В начале 1990-х годов в Кавендишской лаборатории Кембриджа создана технология обратного восстановления схемы сложных кремниевых чипов, позволяющая аккуратно снимать слои микросхемы один за другим. Одно из примененных там новшеств – техника показа примесных N и P слоев на основе эффекта Шоттки: тонкая пленка из золота или палладия накладывается на чип, образуя диод, который может быть виден в электронном луче. Изображения последовательных слоев чипа вводятся в компьютер, специальное программное обеспечение очищает первоначально нечеткие образы, выдает их ясное представление и распознает стандартные элементы чипа. Данная система была протестирована на процессоре Intel 80386 и ряде других устройств. Работа над восстановлением 80386 заняла две недели, причем для правильной реконструкции обычно требуется около шести образцов чипа. Результатом работ могут быть диаграммы масок и схем или даже список библиотечных ячеек, из которых чип был сконструирован.

В условиях, когда конструкция и принципы функционирования чипа уже известны, существует очень мощная технология, разработанная в ШМ для исследования чипа в работе даже без удаления защитного слоя. Для измерения рабочих характеристик устройства над ним помещают кристалл ниобата лития. Показатель преломления этой субстанции изменяется при изменении электрического поля, и потенциал находящегося под ней кремния может считываться с помощью ультрафиолетового лазерного луча, проходящего через кристалл под скользящим углом наклона. Возможности этой технологии таковы, что можно считывать сигнал в 5 В и с частотой до 25 МГц. По сути дела, это стандартный путь для хорошо оснащенных лабораторий при восстановлении криптоключей в чипах, конструкция которых известна.

Исследование техники разрезания чипа ведет к более общей (и сравнительно меньше изученной) проблеме – атакам, которые включают в себя активную модификацию исследуемого чипа, а не просто пассивное его исследование. К примеру, есть все основания полагать, что некоторые успешные атаки пиратов на систему платного ТВ проводились с

использованием рабочих станций с фокусированием ионного пучка (Focused Ion Beam workstation – FIB). Такой аппарат может вырезать траки в металлизированном слое чипа и формировать новые траки или изолирующие слои. Кроме того, FIB может имплантировать ионы для изменения толщины слоя кремния и даже строить сквозные переходы к проводящим структурам в нижележащих слоях чипа. Такие аппараты стоят несколько миллионов долларов, но, как показывает практика, не слишком богатые злоумышленники арендуют дорогое оборудование на некоторое время у крупных полупроводниковых компаний.



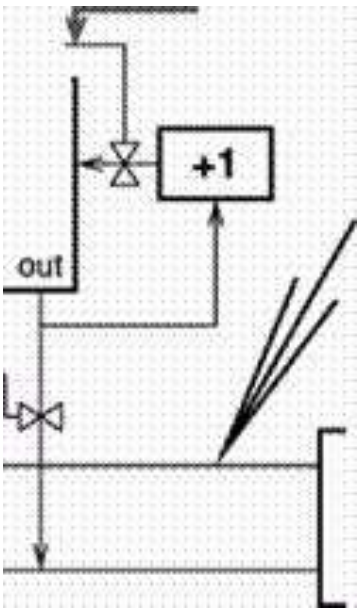
Снимок электронным микроскопом, демонстрирующий результаты обработки чипа сфокусированным ионным пучком (FIB)

Обеспеченные таким инструментарием атаки на смарт-карты становятся более простыми и мощными. Типичная атака заключается в отсоединении почти всех процессов ЦПУ от шины, кроме памяти EEPROM и той компоненты ЦПУ, что генерирует доступ по чтению. Например, программный счетчик может быть оставлен подсоединенным таким образом, что области памяти становятся по порядку доступны на считывание по мере подачи тактовых импульсов.

Как только это сделано, атакующему требуется лишь одна игла микропробника для считывания всего содержимого EEPROM. В результате процесс анализа становится более легким, чем при пассивном исследовании, когда обычно анализируется только трасса выполнения. Также это помогает избежать чисто механических трудностей одновременной работы с несколькими иглами-микропробниками на линиях шины, ширина которых составляет лишь несколько микрон.

Program Counter load

load low high



Microcode Control Unit
1
земля
X X
шина данных (8 bit)
адресная шина (16 bit)
игла микропробника
сигнал синхронизации
EEPROM
X-удаленное соединение, *-созданное новое соединение

Модифицированная атака на криптопроцессор с помощью рабочей станции FIB , позволяющая легко осуществить доступ к засекреченному содержимому EEPROM , используя единственную иглу-микропробник

Индуцирование сбоев (глич-атаки)

В принципе, создателям вычислительной техники давно известно, что к инженерно-защищенным устройствам типа смарт-карт, которые обычно малы и компактны, с целью вызова вычислительной ошибки можно применить некоторые уровни радиационного облучения или нагревания, подачу неправильного напряжения питания или нестандартную тактовую частоту. Известно также и то, что при возникновении сбоя в вычислениях компьютерное устройство может выдать информацию, полезную для восстановления секретных данных. Однако, насколько серьезна эта угроза в действительности, долгое время мало кто подозревал.

В конце сентября 1996 г. коллектив авторов из Bellcore, научно-исследовательского центра американской компании Bell, сообщил о том, что обнаружена серьезная потенциальная слабость общего характера в защищенных криптографических устройствах, в частности, в смарт-картах для электронных платежей. Авторы – Бонэ, ДеМилло и Липтон – назвали свой метод вскрытия «криптоанализом при сбоях оборудования», суть же его в том, что искусственно вызывая ошибку в работе электронной схемы с помощью ионизации или микроволнового

облучения, а затем сравнивая сбойные значения на выходе устройства с заведомо правильными значениями, теоретически можно восстанавливать криптографическую информацию, хранящуюся в смарт-карте [BD97].

Исследования ученых показали, что новой угрозе подвержены все устройства, использующие криптоалгоритмы с открытыми ключами для шифрования информации и аутентификации пользователя. Это могут быть смарт-карты, применяемые для хранения данных (например, электронных денег); SIM-карточки для сотовой телефонии; карточки, генерирующие электронные подписи или обеспечивающие аутентификацию пользователя при удаленном доступе к корпоративным сетям. Правда, разработанная в Bellcore атака была применима для вскрытия ключей исключительно в криптосхемах с открытым ключом – RSA, алгоритм цифровой подписи Рабина, схема идентификации Фиата-Шамира и тому подобные конструкции.

Главным же результатом публикации Bellcore стало то, что к известной, вообще говоря, в узком кругу проблеме было привлечено внимание гораздо большего числа исследователей. И меньше чем через месяц после появления статьи Бонэ и его коллег, в октябре 1996 г., стало известно и о разработке аналогичной теоретической атаки в отношении симметричных шифров, т.е. криптоалгоритмов закрытия данных с общим секретным ключом. Новый метод был разработан знаменитым тандемом израильских криптографов Эли Бихамом и Ади Шамиром, получив название «Дифференциальный анализ искажений» или ДАИ (по-английски DFA).

На примере самого распространенного блочного шифра DES эти авторы продемонстрировали, что в рамках той же «беллкоровской» модели сбоя в работе аппаратуры можно «вытащить» полный ключ DES из защищенной смарт-карты путем анализа менее 200 блоков шифртекста (блок DES – 8 байт). Более того, впоследствии появился еще ряд работ Бихама-Шамира с описанием методов извлечения ключа из смарт-карты в условиях, когда о реализованной внутри криптосхеме не известно практически ничего [BS97].

Наиболее часто критика в адрес ДАИ, особенно со стороны выпускающих смарт-карты фирм, сводилась к тому, что вся эта методика носит сугубо теоретический характер. Ведь никто, дескать, не продемонстрировал на практике, что сбойные ошибки можно вызывать именно в криптосхеме, причем конкретно в алгоритме разворачивания ключа…

Но уже весной 1997 года появилось описание не теоретической, а весьма практичной атаки, получившей название «усовершенствованный метод ДАИ». Авторы атаки, уже упоминавшиеся кембриджский профессор Росс Андерсон и его (в те времена) аспирант из Германии Маркус Кун, продемонстрировали, что могут извлекать ключ из смарт-карты менее чем по 10 блокам шифртекста. В основу нового метода была положена модель принудительных искажений или «глич-атак» (от английского glitch – всплеск, выброс), реально практикуемых кракерами при вскрытии смарт-карт платного телевидения. Под глич-атаками понимаются манипуляции с тактовой частотой или напряжением питания смарт-карт, что позволяет выдавать дампы с ключевым материалом на порт выхода

устройства. Эффективность глич-атак продемонстрирована кембриджскими авторами как на симметричных криптосхемах, так и на вскрытии алгоритмов с открытым ключом [АК97].

Анализ побочных каналов утечки

Летом 1998 г. пришло известие еще об одном методе вскрытия смарт-карт, также более чем успешно реализованном на практике. Совсем небольшая, состоящая из 4 человек консалтинговая криптофирма Cryptography Research из Сан-Франциско разработала чрезвычайно эффективный аналитический инструментарий для извлечения секретных ключей из криптографических устройств. По словам главы фирмы Пола Кочера, которому в ту пору было 25 лет, исследователям «не удалось найти ни одной карты, которую нельзя было бы вскрыть».

Кочер, надо отметить, по образованию биолог, а хакерством занимался с детства как хобби. Не исключено, что именно биологическое образование помогло ему выработать собственный стиль анализа «черных ящиков», относясь к ним как к живым организмам и внимательно исследуя все доступные признаки их «жизнедеятельности». В традиционном анализе криптоустроиств и защищенных протоколов принято предполагать, что входное и выходное сообщения доступны злоумышленнику, а какая-либо информация о хранимых внутри данных (криптоключах, например) ему неизвестна. Однако, любое электронное устройство состоит из конкретных элементов, выдающих в окружающую среду информацию о своей работе. А значит на самом деле атакующей стороне может быть доступна и всевозможная побочная информация, выдаваемая криптоустройством: электромагнитное излучение, сигналы об ошибках или об интервалах времени между выполняемыми инструкциями, колебания в потреблении электропитания и другие данные.

Вообще говоря, все это очень хорошо известно военным и спецслужбам, где разработаны специальные методы работы с побочными каналами утечки информации, но тема эта – под кодовым наименованием Tempest – строго засекречена и открытых публикаций о ней очень мало (подробнее см. раздел «Мужчины с ошеломительным оснащением»).

Кочер и его коллеги, можно сказать, переизобрели секретные методы спецслужб и научились вскрывать защиту смарт-карт с помощью привлечения аппарата математической статистики и алгебраических методов исправления ошибок для анализа флуктуации в потреблении чипом электропитания. Делалось это примерно в течение полутора лет с 1996 по 1998 год, когда специалисты Cryptography Research занимались задачей о том, каким образом можно было бы повысить стойкость портативных криптографических жетонов, включая смарт-карты. Не предавая свои исследования широкой огласке, они знакомили сообщество производителей смарт-карт с разработанными в фирме видами атак, получившими названия ПАП (простой анализ питания) и ДАЛ (дифференциальный анализ питания, или DPA) [KJ99].

Вполне очевидно, что данные методы анализа заслуживают самого серьезного внимания, поскольку атаки такого рода можно проводить быстро и используя уже готовое оборудование ценой от нескольких сотен

до нескольких тысяч долларов. Базовые же концепции новой методики вскрытия сформулированы в более ранней и достаточно известной работе Пола Кочера «Криптоанализ на основе таймерной атаки» [РК96], где было продемонстрировано, что можно вскрывать криптоустройства, просто точно замеряя интервалы времени, которые тем требуются на обработку данных.

Что же касается ПАП-атак, то здесь аналитик непосредственно наблюдает за динамикой потребления энергии системой. Количество расходуемой энергии изменяется в зависимости от выполняемой микропроцессором инструкции, а для точного отслеживания флуктуации в потреблении питания можно использовать чувствительный амперметр. Так выявляются большие блоки инструкций– циклы DES, операции RSA и т.д., – поскольку эти операции, выполняемые процессором, имеют внутри себя существенно различающиеся по виду фрагменты. При более сильном усилении удается выделять и отдельные инструкции. В то время как ПАП-атаки главным образом строятся на визуальном анализе с целью выделения значимых флуктуации питания, значительно более эффективный метод ДАЛ построен на статистическом анализе и технологиях исправления ошибок для выделения информации, имеющей корреляции с секретными ключами.

Кое-что новое

В июне 2002 г. был обнародован еще один метод вскрытия смарт-карт и защищенных микроконтроллеров, получивший название «атака оптическим индуцированием сбоев» (optical fault induction attack). Этот класс атак был обнаружен и исследован в Кембриджском университете русским аспирантом Сергеем Скоробогатовым и его руководителем Россом Андерсоном. Суть метода в том, что сфокусированное освещение конкретного транзистора в электронной схеме стимулирует в нем проводимость, чем вызывается кратковременный сбой. Такого рода атаки оказываются довольно дешевыми и практичными, для них не требуется сложного и дорогого лазерного оборудования.

Например, сами кембриджские исследователи в качестве мощного источника света использовали фотовспышку, купленную в магазине подержанных товаров за 20 фунтов стерлингов. Для иллюстрации мощи новой атаки была разработана методика, позволяющая с помощью вспышки и микроскопа выставлять в нужное значение (0 или 1) любой бит в SRAM-памяти микроконтроллера. Методом «оптического зондирования» (optical probing) можно индуцировать сбои в работе криптографических алгоритмов или протоколов, а также вносить искажения в поток управляющих команд процессора. Понятно, что перечисленные возможности существенно расширяют уже известные «сбойные» методы вскрытия криптосхем и извлечения секретной информации из смарт-карт [SA02].

Индустрия, как обычно, пытается всячески принизить значимость нового метода вскрытия, поскольку он относится к классу разрушающих атак, сопровождающихся повреждением защитного слоя в чипе смарт-карты. Однако, по свидетельству Андерсона, злоумышленники могут обойтись и минимальным физическим вмешательством: кремний прозрачен

в инфракрасном диапазоне, поэтому атаку можно проводить прямо через кремниевую подложку с задней стороны чипа, сняв лишь пластик. Используя же рентгеновское излучение, карту и вовсе можно оставить нетронутой.

Этими же специалистами из Кембриджа совместно с учеными компьютерной лаборатории Лувенского университета (Бельгия) недавно разработаны еще несколько новых методов считывания информации из защищенных чипов смарт-карт. Общим для данных методов является то, что они индуцируют поддающиеся замерам изменения в аналоговых характеристиках ячеек памяти. Например, сканируя ячейки сфокусированным лазером или наводя в них вихревые токи с помощью индуктивной спирали на игле микропробника, можно повысить электромагнитные утечки, выдающие записанное там значение бита, но при этом само это значение сохраняется в ячейке ненарушенным. Сильным охлаждением чипа в нужный момент времени можно «заморозить» содержимое интересующего регистра и считать из него (ключевую) информацию, обычно хранящуюся или передаваемую в зашифрованном виде. Эта технология применима к самым разным типам памяти от RAM до FLASH и реально продемонстрирована считыванием ключей DES из ячеек RAM без какого-либо физического контакта с чипом [SQ02].

Данная работа проведена учеными по заказу проекта Евросоюза GSCard и ставит перед собой цель создания смарт-карт следующего поколения, способных максимально противостоять современным атакам вплоть до «полуразрушающих». Создание абсолютной защиты, естественно, не является реалистичным для реально применяемых устройств, одно из главных достоинств которых – дешевизна.

Наглядно и убедительно, но – для своих

Арсенал средств защиты смарт-карт на сегодняшний день весьма разнообразен. Разрушающим методам вскрытия могут противостоять емкостные датчики или оптические сенсоры под светонепроницаемой оболочкой (что кракеры давно научились обходить), либо «специальный клей» – особое покрытие для чипов, которое не только непрозрачно и обладает проводимостью, но также надежно противостоит попыткам уничтожить его, обычно разрушая кремниевый слой, находящийся под ним. Такие покрытия относятся к федеральному стандарту США FIPS 140-1 и широко используются в американской военной промышленности, но повсеместно распространенными в быту их назвать нельзя.

Ряд недорогих и эффективных методов противодействия методам ДАЛ и ДАИ известен по разработкам Cryptography Research. В частности, созданы особые аппаратные и программные методы, обеспечивающие значительно меньший уровень утечек компрометирующей информации, внесение шума в измерения, декоррелирование (разделение взаимозависимостей) внутренних переменных и секретных параметров, а также декоррелирование по времени криптографических операций. Значительный ряд новых методов защиты предложен компьютерными лабораториями Лувена и Кембриджа [http://www.dice.ucl.ac.be/crypto; http://www.cl.cam.ac.uk/Research/Security/tamper/].

Разработкой мер защиты смарт-карт от вскрытия, конечно же, занимаются не только в университетах или маленьких фирмах вроде Cryptography Research Пола Кочера или Advanced Digital Security Research Оливера Кеммерлинга. Большая работа ведется и непосредственно в смарт-карточной индустрии, где, правда, предпочитают эту деликатную тему публично не обсуждать. Но иногда кое-какая информация все же просачивается. Так, на криптографической выставке-конференции RSA-2002 интереснейшая экспозиция была устроена компанией Datacard Group, специализирующейся на разработке смарт-карт.

На своем выставочном стенде сотрудники фирмы развернули некий «полевой вариант» небольшой электронной лаборатории. Буквально на глазах изумленной публики демонстрировалось вскрытие смарт-карт с помощью описанных выше методов ДАЛ и ДАИ. Оборудования для этих работ требовалось совсем немного – осциллограф, компьютер да несколько «специальных коробочек».

Для зрителей процесс вскрытия смарт-карты выглядел примерно так: «Сейчас вы видите на экране осциллографа последовательность вертикальных всплесков. Это циклы DES-алгоритма, шифрующего информацию в чипе карты. Давайте увеличим разрешение картинки. Внутри цикла вы видите пики характерной формы – это S-боксы, преобразующие нужный нам ключ. Давайте запустим программу вскрытия, которая по особенностям этих сигналов отыскивает биты секретной информации, и вот через минуту или две мы получаем ключ на выходе программы».

Значительно более стойкий криптоалгоритм Triple-DES вскрывался аналогично, но примерно раза в 3 раза больше по времени. Те же самые несколько минут уходили у аналитиков Datacard на отыскание пары больших простых чисел, образующих ключ в алгоритме RSA. Для этого не использовались, ясное дело, ужасно трудоемкие методы факторизации (разложения числа на множители), а «просто» внимательно анализировались реакции чипа смарт-карты на небольшие варьирования в напряжении и частоте при подаче питания…

Самый эффектный, пожалуй, трюк – это извлечение информации из бесконтактных смарт-карт, когда вскрытие устройства и считывание секретного ключа делается с помощью специального радиочастотного интерфейса – дистанционно и абсолютно незаметно для владельца [CP02].

Одно дело читать обо всех этих методах в абстрактных исследовательских статьях и совсем другое – увидеть, как данная кухня функционирует реально. По свидетельству специалистов, открывающаяся картина действительно впечатляет. И заставляет очень серьезно переосмыслить реальную безопасность технологии.

Возня в подполье, война на небесах

В начале 2002 г. властями Гонконга принято решение о том, что начиная с 11-летнего возраста все жители этого особого региона Китая должны иметь идентификационную смарт-карту, содержащую фотографию, имя, пол, дату рождения, статус проживания и биометрическую информацию об отпечатках больших пальцев обеих рук. В принципе,

жителям Гонконга к паспортам не привыкать, поскольку их ввели еще в 1949 году, когда из завоеванного Мао Цзэдуном Китая в эту британскую колонию хлынул поток мигрантов, не испытывавших энтузиазма в отношении коммунистов. Тогда-то властям и понадобилось срочно разделить народ на «местных» и «приезжих». Уже несколько лет, как Гонконг вновь стал частью Китая, однако особый экономический статус, отдельное управление и жесткий контроль за иммиграцией лишь упрочили паспортную систему.

Введение смарт-карт с биометрической информацией в качестве идентификационных документов набирает масштабы во многих технологически продвинутых странах мира, от Финляндии и Италии до Малайзии и Японии. Но попутно растут опасения, что технологии компьютерной идентификации делают слишком простыми злоупотребления как на почве хищения личности, так и тотальной слежки за гражданами. Для Гонконга это особо актуально, потому что, как хорошо известно, именно здесь сосредоточено значительное количество квалифицированных кракеров, специализирующихся на взломе смарт-карт, используемых в системах платного телевидения, электронных платежей и прочих коммерческих приложениях.

Новые электронные карточки-паспорта гонконгцев предназначены, среди прочего, и для ускоренного прохождения пограничного контроля. Через автоматические «киоски самообслуживания» это можно делать в обход чиновников и традиционно длинных очередей прибывающих или отъезжающих. Для работы подобных киосков не предусмотрено централизованной базы данных с отпечатками пальцев всех граждан (поскольку подобные базы признаны слишком уязвимыми для посягательств злоумышленников), так что здесь происходит лишь сличение отпечатка пальца владельца карты с кодом, хранящимся в памяти микросхемы. Все эти обстоятельства порождают благодатную почву для зарождения нелегального рынка идентификационных смарт-карт. Принимая в учет реальность подобной угрозы, власти Гонконга на всякий случай исключили из карточек-паспортов планировавшиеся поначалу функции водительских прав и библиотечных удостоверений. По всей видимости, дабы не стимулировать собственными руками рост черного рынка фальшивых паспортов [HK02].

Хайтек-паспорта на основе смарт-карт – дело пока что довольно новое, поэтому по состоянию на конец 2003 г. в прессе и Интернете еще не появлялось сколь-нибудь достоверной информации о масштабах и степени серьезности злоупотреблений в этой области. Зато о другой, технологически весьма близкой сфере – взломе систем спутникового платного телевидения – публикаций более чем достаточно.

Как это работает

Количество одних лишь легальных подписчиков систем спутникового ТВ перевалило уже за сотню миллионов. Разнообразные, спонтанно рождавшиеся с 1970-х годов технологии защиты сигнала постепенно сходятся и ныне, во многом благодаря смарт-картам, уже почти обрели единый комплекс стандартов, обеспечивающих беспроблемную работу

аппаратуры в разных частях планеты и в условиях разных кодировок.

Что, в самых общих чертах, представляет собой современная система платного спутникового ТВ? С точки зрения ТВ-компании и обычного легального подписчика, самое главное в этой системе – карта доступа, т.е. смарт-карта, приобретаемая вместе с ТВ-аппаратурой спутникового приема, либо отдельно (если комплект из антенны-тарелки и приемника-ресивера уже имеется). Карта доступа размером примерно со стандартную кредитку вставляется в слот ресивера и представляет собой полноценный микрокомпьютер с процессором, встроенным программным обеспечением и памятью. Программное обеспечение, прошитое в смарт-карту, управляет приемом и декодированием пакета каналов той компании, что выпустила карту доступа. После установки оборудования абонент выбирает интересующий его набор каналов, делает их оплату и каким-либо образом – обычно по телефону – связывает ресивер/карту с ТВ-компанией. Происходит активизация смарт-карты, открытие доступа к оплаченным каналам и, достаточно часто, привязка к конкретному приемному оборудованию (как мера против клонирования карт).

Одна из характерных черт платного ТВ – это весьма большое количество разнообразных систем шифрования, применяемых вещательными компаниями в тысячах спутниковых каналов. Изготовителям же приемного оборудования – цифровых медиа-терминалов – по всему миру пришлось столкнуться с серьезной проблемой несовместимости схем управления доступом к платным каналам. Решена эта задача с помощью устройства-декодера CAM (Conditional Access Module, «модуль условного доступа»). Именно в CAM в качестве ключа вставляется смарт-карта, обеспечивающая доступ к пакету каналов.

Принимая спутниковый сигнал, CAM-модуль транслирует карте всю служебную информацию, идущую в канале параллельно видеосигналу (примерно как телетекст). На закрытых каналах в этой информации есть, среди прочего, и схема восстановления (криптопараметры) телесигнала. Эти криптопараметры зашифрованы и именно для их расшифровки в смарт-карте есть ключи. Получив от CAM-модуля эту информацию, карта ее расшифровывает собственным процессором и возвращает назад. А CAM-модуль, который часто называют декодером, с помощью этой расшифрованной схемы восстанавливает телесигнал (у смарт-карты для самостоятельного расшифрования видеоизображения недостаточно вычислительной мощности). Криптопараметры сигнала изменяются каждые 10-15 секунд, но зашифрованы они одним ключом, который хранится в смарт-карте и меняется значительно реже. Впрочем, «реже», понятие относительное и может подразумевать срок от нескольких недель до нескольких часов, в зависимости от конкретной телекомпании.

Поскольку современная смарт-карта – сама по себе небольшой компьютер, то компания-вещатель имеет возможность передавать через спутник по служебному каналу управляющие команды конкретно для карты, что называется «управление через эфир» или OTA (Over-The-Air). Так можно загружать в карту новые ключи или давать команду на их самостоятельное внутреннее обновление (в зависимости от конкретной технологии). Кроме того, через эфир для телекомпании очень удобно включать-выключать конкретные карточки задолжавших подписчиков,

поскольку каждая смарт-карта имеет уникальный номер-адрес.

Если смотреть на технологию с точки зрения пиратов, то самый очевидный способ нелегального просмотра защищенных ТВ-каналов – клонировать легальную карту. Для этого на специальном оборудовании, иногда весьма дорогом, изготовляется ее полный аналог, неотличимый по функциональным возможностям от оригинала. Работать такой клон будет до тех пор, пока работает оригинал. Чем-то это напоминает печатание фальшивых денег, только технически проще и окупается быстрее. Среди других способов в настоящее время у большинства пиратов наиболее популярна разного рода эмуляция фирменных смарт-карт. Чаще всего это бывают либо так называемые DPSC-карты (digital pirate smart card – цифровая пиратская смарт карта, целенаправленно изготовленная для нелегального просмотра), либо MOSC-карты (modified original smart card – модифицированная оригинальная смарт карта, изначально выпущенная для официальной подписки, но затем модифицированная соответствующим образом для просмотра шифрованных каналов без оплаты).

Контрмеры на примере

Конкретные формы пиратской деятельности и борьбы компаний платного ТВ с нелегальным просмотром имеет смысл рассмотреть на примере американской DirecTV – крупнейшей в мире фирмы спутникового ТВ с числом подписчиков порядка 15 миллионов.

Под электронными контрмерами или ECM (Electronic Counter Measure), вообще говоря, принято понимать любые мероприятия, дистанционно проводимые ТВ-компаниями для препятствования пиратской деятельности. Обычно под этим понимается внеплановая или просто учащенная смена криптографических ключей. Однако в последнее время под ECM стали понимать нечто значительно более существенное – модификацию схемы устройства.

В двадцатых числах января 2001 г. сразу несколько крупных компаний спутникового телевидения – американские DirecTV и EchoStar Dish Network, а также испанская Canal Satelite Digital – практически одновременно нанесли массированные «удары возмездия» по пиратским ресиверам и смарт-картам, обеспечивающим бесплатный просмотр. При этом были использованы электронные контрмеры по активному воздействию на аппаратуру, что обычно принято рассматривать как сугубо военное «информационное оружие» [KP01].

Наиболее эффективные контрмеры были продемонстрированы компанией DirecTV. В соответствии с устоявшейся в отрасли технологией, здесь каждая смарт-карта доступа (разработка британской фирмы NDS) запрограммирована собственным кодом, который идентифицирует легального абонента и позволяет ему смотреть только те каналы из спутникового цифрового сигнала DirecTV, которые оплачены. Все остальные каналы остаются зашифрованными и в теории считаются недоступными для просмотра. Однако, буквально с самых первых месяцев вещания DirecTV в 1994 г., кракерским сообществом была развернута деятельность по обеспечению пиратского просмотра телеканалов безо всякой абонентской платы. Особую популярность весьма прибыльный

бизнес по продаже пиратских карт и «серых» ресиверов приобрел в Канаде, где у DirecTV нет лицензии на вещание и где продажа кракнутых карт вплоть до 2002 года не являлась преступлением.

В DirecTV, естественно, постоянно работают над укреплением защиты своей системы. Однако в течение 2000-2001 гг. кракерским подпольем были взломаны криптосхемы практически всех популярных систем защиты спутникового вещания, и в конце 2000 г. многим уже казалось, что DirecTV в этой нескончаемой игре в кошки-мышки начала безнадежно проигрывать. Пиратам удалось полностью дешифровать весь сигнал DirecTV, включая самые дорогие каналы с оплатой за каждый просмотр и трансляцией новейших кинофильмов-хитов. Однако в начале 2001 года по пиратским картам был нанесен удар такой силы, что стало ясно – вопрос о победителях в данном противостоянии еще весьма далек от разрешения.

Главным объектом январской ECM-атаки DirecTV стали так называемые H-карты (типа MOSC), пользовавшиеся у пиратов наибольшей популярностью вследствие своих конструктивных особенностей. H-карты продавались в комплекте с ресиверами с 1996 до начала 1999 года. Это была одна из исходных смарт-карт, имевшая в своей защите ряд слабостей, которые позволили кракерам провести обратную инженерную разработку микрочипа, а затем научиться самим его перепрограммировать. Это позволило так изменять модель абонентской подписки, чтобы становилось возможным открывать все каналы сразу.

Но в телекомпаниях ныне тоже работают свои хакеры, которые встроили в систему механизм, позволяющий обновлять содержимое смарт-карт с помощью команд в транслируемом спутниковом сигнале. Этот механизм обновлений в DirecTV стали применять для поиска и уничтожения «кракнутых» карт, записывая в микрочип такие коды, которые нарушали работу лишь пиратских продуктов. По сути дела, нелегальные смарт-карты запирались в состоянии бесконечного цикла. Пиратское сообщество ответило на этот ход новым устройством, получившим название unlooper (специальный программатор-«расцикловщик» для восстановления поврежденных карт). Затем кракеры разработали программу-троянца, которая записывалась в смарт-карту и эффективно блокировала возможности ресивера по обновлению содержимого карты. В такой ситуации DirecTV оставалось лишь рассылать свои обновления с повышенной частотой, одновременно проверяя, чтобы обновление непременно присутствовало в ресивере. Лишь на этом условии видеосигнал поддавался декодированию. Обновления стали проходить практически каждый месяц. После каждого такого апдейта, спустя примерно минут 15, пираты изготовляли и распространяли через Интернет программную заплатку, обходящую новую помеху.

Однако с началом осени 2000 г. в поведении DirecTV стали отмечать нечто новое. Байты обновления стали рассылать значительно чаще, практически еженедельно, причем по несколько порций зараз, явно нарушая давно сложившуюся традицию. Кракеры по-прежнему легко обходили все эти обновления, но не очень понимали, к чему пошло дело. Некоторые подумали, что компания решила взять их на измор, заставляя перепрограммировать смарт-карты пиратской клиентуры практически непрерывно. Ко всем этим обновлениям в общем-то привыкли, сами по

себе они представляли достаточно бессмысленные наборы байт, но их наличие было необходимо, чтобы кракнутое оборудование тоже могло принимать видеосигнал. Поэтому волей-неволей все эти байты приходилось накапливать и в пиратских программах-прошивках.

Но затем в ноябре прошел еще один цикл обновлений, и тут кракеры увидели, в чем был замысел DirecTV. Благодаря последней порции байт все ранее загруженные фрагменты кода объединились в единое целое, образовав динамическую программу или «логическую бомбу», являющуюся неотъемлемой частью смарт-карты. Новая динамическая программа изменила всю структуру работы старой технологии, придав ей дополнительную мощь и гибкость. Пираты уже поняли, что новые возможности дали DirecTV эффективное тайное оружие, но каким именно образом оно будет применено, оставалось непонятным.

Все встало на свои места воскресным вечером 21 января 2001 г., когда Америка поголовно прилипла к телеэкранам, следя за матчами своего футбольного суперкубка Super Bowl. Время «удара возмездия» было рассчитано точно и именно теперь был «нажат курок». В видеосигнале DirecTV прошла команда, которая разом вырубила все пиратские H-карты. По мере наступления вечера на всей территории США, эта команда давалась еще несколько раз, так что по некоторым подсчетам в один день были «отстрелены» около 98% всех кракнутых карт, число которых составляло, по грубым оценкам, около 200 тысяч штук. На этот раз бесконечный цикл, запирающий чип, был прописан в «одноразовый» раздел памяти, в принципе не поддающийся повторной перезаписи, что превратило карту в абсолютно бесполезную вещь. Причем специалисты из DirecTV, разработавшие эту атаку, подписали свою акцию с чисто хакерской глумливостью. В каждой навечно запертой смарт-карте первые восемь байт перезаписанной программы теперь стали читаться как GAME OVER – «игра окончена».

Впрочем, игра вовсе не окончена. Кракнутые смарт-карты DirecTV нового поколения (HU-карты) начали появляться на сером рынке чуть ли не одновременно с поступлением легальных карт к дилерам. Другая современная технология пиратов вообще не опирается на карты доступа, а полностью эмулируется программно на персональном компьютере. Технологии такого рода абсолютно никак не пострадали от январской атаки. Конечно, теперь последуют новые контратаки DirecTV, но, как комментируют ситуацию участники противостояния, «это война, причем такая, которая будет длиться вечно».

Три источника и три составные части пиратства

Среди главных причин массового распространения нелегальных смарт-карт выделяются три, которые довольно условно можно назвать социальной, экономической и технической.

Социальная причина заключается в том, что в обществе имеется спрос, на который далеко не всегда есть легальные предложения. И это совершенно очевидный источник массового распространения пиратства в сфере спутникового ТВ, поскольку нелегальный просмотр – нередко единственный для людей способ доступа к интересным закрытым каналам.

Вызвано это огромным несоответствием между техническими возможностями аппаратуры и правовыми нормами межгосударственных отношений. Спутниковое ТВ – это не Интернет, здесь для вещания на другие страны нужна лицензия. И хотя каналы многих вещателей «видны» по всей Европе, свою подписку они могут продавать лишь резидентам очень немногих стран. Или вообще одной страны, где имеется лицензия на вещание. Лицензия же стоит немалых денег и часто сопровождается условиями к содержанию (переводу) передач, причем в каждой стране эти условия разные. Поэтому, например, американские компании не имеют лицензии на вещание в Канаде (где, в частности, весьма строгие законы о двуязычном сопровождении передач), а в России вообще лишь один официальный оператор платного спутникового ТВ (пиратить которого, естественно, дело абсолютно противозаконное). Зато все остальные сотни доступных телеканалов поневоле придется смотреть нелегально, но и судебное преследование за это вряд ли кому грозит.

Из первой причины естественным образом вытекает вторая, экономическая. В описанных условиях сформировался массовый серый рынок со своими, ныне уже весьма крупными, финансовыми интересами и мощными стимулами для поощрения пиратства. На продаже ресиверов, тарелок и смарт-карт для нелицензированного просмотра спутникового ТВ делаются ныне десятки миллионов долларов, а постоянно подпитывать этот рынок можно лишь одним путем– финансируя непрерывное вскрытие регулярно обновляемой защиты систем вещания.

Еще одна важная – техническая – причина массового пиратства в том, что декларируемая компаниями защита смарт-карт существенно отличается от защиты реальной. Несмотря на все заверения о «гарантированной стойкости нового продукта к вскрытию», практика показывает, что при наличии достаточно мощного финансового интереса взламываются любые карты любой компании, причем зачастую при непосредственном участии фирм-конкурентов.

Игра без правил

Летом 2003 г. базирующаяся в Великобритании транснациональная компания NDS Group, один из главных в мире разработчиков смарт-карт условного доступа для систем платного ТВ, выпустила интересный пресс-релиз [ND03]. Заголовок этого документа говорит сам за себя: «NDS отвергает судебный иск компании EchoStar как безосновательный и оппортунистический». Суть же обвинений медиа-компании EchoStar – владеющей в США второй по величине, после DirecTV, спутниковой ТВ-сетью Dish Network – и близко родственной ей американо-швейцарской фирмы NagraStar сводится к тому, что NDS тайно занимается промышленным шпионажем и взломом смарт-карт конкурентов, а добытую столь нечестным путем информацию «сливает» затем через Интернет в сети пиратского подполья.

Через пресс-релиз NDS глава компании Абе Пелед дал весьма решительную отповедь всем этим обвинениям, заявив, что его фирма «не имеет ничего общего с пиратским взломом EchoStar или каких-либо других смарт-карт; NDS – ведущий в мире поставщик систем защиты платного ТВ,

давно и прочно приверженный искоренению пиратства в индустрии, а иск EchoStar/NagraStar – это по сути дела повторение другого безосновательного судебного дела, затеянного против нас около года назад и с тех пор прекращенного». И вообще, добавляется в релизе, «если бы за данными обвинениями реально что-то стояло, все выяснилось бы давным-давно, а так – это просто несерьезные попытки судебными тяжбами нанести вред NDS и помешать честной конкуренции»…

Здесь следует заметить, что все эти громкие, но довольно неискренние, как будет показано далее, слова скрывают за собой весьма интригующую историю, которую имеет смысл разобрать в доступных подробностях. Ибо на протяжении всего последнего десятилетия сфера платного телевидения демонстрирует весьма парадоксальную картину.

Как известно, в качестве наиболее удобного «ключа» для гибкого управления просмотром защищенных телеканалов здесь выбрана технология смарт-карт, и по самым грубым подсчетам сейчас сети платного ТВ по всему миру защищают от 80 до 100 миллионов таких чип-карт разных систем. При этом, несмотря на участие в столь прибыльном бизнесе нескольких многомиллиардных корпораций, вкладывающих массу сил и средств в защиту своих карточек доступа, буквально все они быстро и эффективно вскрываются пиратами, наводняющими рынок контрафактной продукцией. И что показательно, осуществляется взлом столь профессионально и стремительно, что порою пиратские карты новых моделей появляются на черном рынке даже раньше, чем у официальных продавцов-реселлеров на местах. Другими словами, иногда это может происходить чуть ли не синхронно с публикацией гордого пресс-релиза компании спутникового ТВ о разработке и выпуске новой сверхнадежной технологии защиты от нелегального доступа.

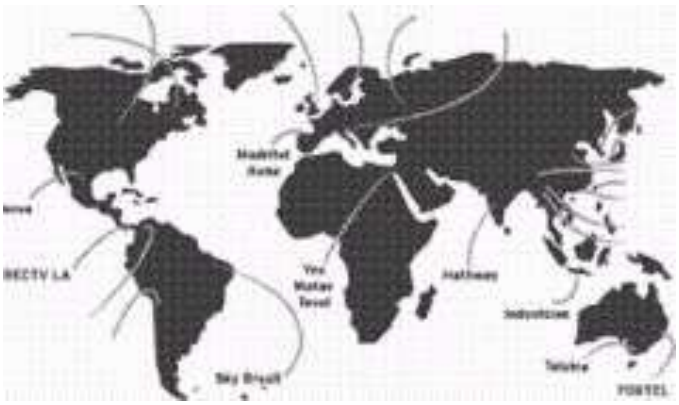
Факты таковы, что наряду с продажами легального рынка на черном и сером рынках крутятся миллионы таких же (по сути, идентичных фирменным) смарт-карт «темного» происхождения. По этой причине в интернет-сообществе уже много лет ходят слухи, будто столь грандиозный расцвет пиратства тайно подпитывают сами же корпорации, ведущие между собой острую конкурентную борьбу. Ведь вскрытие секретного кода конкурента с последующей его широкой публикацией делают ТВ-каналы соперника практически бесплатными, а значит, тому неминуемо грозят крупные убытки, а быть может и вообще разорение.

Выдвинуто несколько предположений и об иных, более тонких механизмах, обеспечивающих нелегальное обогащение на пиратстве для определенных прослоек в руководстве ТВ-компаний. Однако, все это были лишь слухи, а самых разнообразных и нелепых домыслов, как известно, гуляет по Сети более чем достаточно. Конкретных же свидетельств долгое время ни у кого не было. Но вот весной 2002 года разразился грандиозный скандал.

В тот год, а именно 12 марта, европейская группа компаний Canal Plus объявила о возбуждении открытого судебного разбирательства против фирмы NDS Group, обвинив конкурентов в том, что они «затратили большие деньги и ресурсы» на взлом системы смарт-карт MediaGuard для защиты платного ТВ Canal+. А взломав, опубликовали критично важную информацию в Интернете, чем способствовали наводнению рынка

пиратскими картами и гигантскому росту нелегального бесплатного пользования системой. В исковом заявлении, сопровождающем обвинение, Canal Plus оценила понесенные в результате этого убытки суммой 1,2 миллиарда долларов.

DIRECTVUSACablevision
Sky Italia
SkyLlfe BCable TV INC Chine CCTV
Sichuan Cable Network China Network Systems Galaxy STAR
Chongqing Cable– TV Guizhou Cable TV
Sky Colombia
Sky Chile



География распространения системы NDS VideoGuard

Чтобы стал более понятен грандиозный, воистину глобальный характер данного скандала, надо пояснить, что Canal Plus – это телевизионное подразделение франко-американского медиа-гиганта Vivendi Universal, а компания NDS, в свою очередь, на 80% принадлежит Sky Global Networks, подразделению спутникового телевидения медиа-империи News Corporation австралийца Руперта Мердока. Его News Corp. – это сотни газет и журналов на всех пяти континентах, книжное издательство HarperCollins, в киноиндустрии – компания **XX** Century Fox, в сетях ТВ-вещания компании BSkyB в Великобритании, Fox Cable, Fox Broadcasting и на конец 2003 уже фактически купленная DirecTV в США, Star TV в Китае и Sky Latin America в южноамериканском регионе.

В этой империи NDS Group занимается разработкой и продвижением собственной смарт-картной технологии VideoGuard, управляющей доступом к каналам платного ТВ, а клиентами этой технологии являются не только компании самой News по всему миру, но и многие другие крупные фирмы, такие как DirecTV или Discovery Communications. В общей сложности легальными картами VideoGuard пользуются сейчас в мире свыше 30 миллионов подписчиков.

В медиа-империи Vivendi Universal разработкой собственных смарт-карт условного доступа MediaGuard занималась французская компания Canal Plus Technologies, технологическое подразделение Canal Plus. Карты MediaGuard также весьма широко распространены в мире и по общему числу подписчиков -более 10 миллионов – занимают третье место.

В судебном иске французов было заявлено, что о широком распространении контрафактных карт доступа к ТВ-сетям Canal+ стало известно в конце 1999 года, после того, как код, компрометирующий

MediaGuard, был опубликован на веб-сайте канадских хакеров Digital Reference (www.dr7.com). По следам публикации этого кода специалисты Canal+, имеющие связи в хакерских кругах, провели собственное расследование с целью установления, каким образом была похищена информация и кто именно это сделал. Результаты же данного расследования оказались «шокирующими», поскольку выяснилось, что за всей этой историей стоит компания NDS, вскрывшая смарт-карту MediaGuard в своем исследовательском подразделении в Израиле, а затем переправившая критичный фрагмент кода в Америку для распространения через Интернет [CM02].

Судебный иск, обвиняющий NDS в тайных действиях, направленных на подрыв конкурентноспособности Canal+ на рынке цифрового телевидения, был подан в американский окружной суд штата Калифорния, поскольку здесь, в Сан-Франциско, находится региональная штаб-квартира Vivendi Universal, а по соседству – в Южной Калифорнии – и американское представительство NDS. Согласно американским законам, в случае доказательства вины ответчика по конкретно предъявленным обвинениям, суд может обязать нарушителя к возмещению нанесенного ущерба в троекратном размере, не считая издержек на судопроизводство. Трехмиллиардные суммы ущерба от промышленного шпионажа фигурируют в судах не часто, и, видимо, поэтому сугубо коммерческим делом даже заинтересовалась контрразведка Франции, решившая провести собственное расследование случившегося [JD02].

С другой стороны, вынос всей этой истории на широкое публичное обсуждение многими в индустрии был встречен, мягко говоря, без энтузиазма и одобрения. Причина тому достаточно проста – в той или иной форме обратной инженерной разработкой, т.е. негласным вскрытием программ и оборудования конкурентов, занимаются на рынке практически все серьезные игроки. Разница состоит лишь в том, что делается впоследствии с добытой подобным способом информацией и насколько далеко она «утекает».

Не случайно первое, что заявила в свою защиту NDS, – это намерение подать встречный иск против Canal Plus, поскольку Canal Plus Technologies также занимается работами по вскрытию защиты чужих смарт-карт и переманиванием к себе для этого программистов-хакеров из других фирм. А затеянный судебный иск – это, мол, просто месть более удачливому конкуренту после неудавшихся переговоров о слиянии в декабре 2001 года.

Как прокомментировал ситуацию Аира Уинклер, главный стратег по безопасности фирмы Hewlett-Packard, а в прошлом аналитик Агентства национальной безопасности США, полный демонтаж всякой новой продукции конкурентов входит ныне в стандартную корпоративную практику. Например, по словам Уинклера, «как только новая машина появляется на рынке, всякий автопроизводитель в мире знает, что первыми покупателями непременно будут соперники, которые по-тихому разберут ее до последнего болта, чтобы посмотреть как там все работает». И тому имеется более чем достаточно подтверждений. Ясно, что громкий прецедент с криминализацией обратной инженерной разработки ставит в крайне неловкое положение очень многие солидные фирмы. Однако,

соглашается Уинклер, повсеместная корпоративная практика еще не дошла до того, чтобы выкладывать на веб-сайтах фирменные секреты конкурентов или инструкции по их компрометации. И вряд ли какая-то из компаний захочет этим прославиться, поскольку удар по репутации будет нанесен самый серьезный [SU02].

Невзирая на явные и скрытые угрозы NDS тоже предать огласке имеющийся компромат на истца, компания Canal Plus все же решилась пойти на открытое выяснение отношений, чувствуя собственную правоту и располагая значительным количеством убедительных улик против конкурента. В последующие месяцы часть этих документов была запущена в прессу и Интернет, продемонстрировав публике, насколько тесно переплетены совместные дела большого ТВ-бизнеса и хакерского андеграунда.

Вообще говоря, не является секретом, что наиболее известные хакеры, по преимуществу немцы, успешно вскрывавшие в подполье чип-карты ТВ-доступа в первой половине 1990-х годов, и сегодня занимаются тем же самым, но уже вполне официально. Неоднократно упоминаемый в данной книге Маркус Кун сделал заметную научную карьеру, блестяще защитив в Кембридже докторскую диссертацию по способам взлома и методам защиты смарт-карт. Приятель Куна Оливер Кеммерлинг также перебрался в Англию и возглавляет небольшую лондонскую фирму ADSR, которая занимается тестовым вскрытием, разработкой способов защиты и техническим консультированием фирм, использующих смарт-карты.

Примерно в том же направлении намечалась и судьба знаменитого хакера Бориса Флоричича, более известного в Интернете под псевдонимом Tron. Он получил осенью 1998 года конфиденциальное, но вполне официальное приглашение на работу в NDS, однако две недели спустя был найден повешенным в одном из парков Берлина. Еще один давний знакомый Куна, Кеммерлинга и Флоричича, американец Крис Тарновски, более известный под сетевыми никами Big Gun и Von, в начале 1990-х занимался в Германии спутниковой связью на одной из военных баз США, а затем вернулся в Америку. Ныне уже многим известно, что с 1997 года Тарновски стал штатным, хотя и тайным сотрудником NDS, работая там под именем Майк Джордж и по-прежнему сохраняя тесные контакты с компьютерным андеграундом [SL02][BO02].

Значительно меньше известно о том, что эти люди – Кеммерлинг и Тарновски, – являясь наиболее авторитетными специалистами в своей области, работали одновременно по заказам сразу нескольких конкурирующих сторон, а потому попали в крайне затруднительное положение, когда тайные махинации их работодателей начали становиться достоянием гласности и суда.

Стараясь оставаться честным, Оливер Кеммерлинг в официальных показаниях подтвердил, что он и его фирма помогали NDS оборудовать в Хайфе, Израиль специальную лабораторию по вскрытию смарт-карт, одновременно обучая сотрудников эффективным методам взлома, разработанным им совместно с Маркусом Куном. Впоследствии от своих подопечных в Хайфе Кеммерлинг узнал, что NDS закупила партию смарт-карт Canal+, которые через некоторое время были в Израиле

успешно взломаны. К Кеммерлингу попал на ознакомление соответствующий внутренний документ NDS с извлеченным из карты MediaGuard кодом и описанием методики преодоления защиты. Когда в конце 1999 г. аналогичные материалы всплыли в Интернете, на канадском хакерском сайте www.dr7.com, Кеммерлинг без труда узнал в них файлы лаборатории в Хайфе. Чуть позже это же подтвердил ему и знакомый из NDS, сообщивший, что из Израиля данные материалы были переправлены в Южную Калифорнию Крису Тарновски, на которого возлагалась задача по собственным каналам запустить материал в Интернет.

Как показали последующие события, избранный «канал» оказался не слишком удачен – в 2000 г. американская таможня задержала предназначавшуюся Тарновски оплату в размере 40 тысяч долларов, поскольку деньги следовали из Канады в пачках банкнот, упрятанных в корпусах радиоэлектронного оборудования. Собственно говоря, тогда-то и стало известно, что знаменитый в андеграунде Big Gun является тайным сотрудником NDS, поскольку именно ушлые адвокаты компании «отмазали» в тот раз Тарновски от карающей руки правосудия.

В итоге же в высшей степени двусмысленном положении оказался Оливер Кеммерлинг, поскольку его фирма работала по заказам не только NDS, но и Canal+, и других фирм платного ТВ. Кроме того, компания ADSR принадлежит Кеммерлингу лишь на 60%, в то время как остальной долей владеет NDS, не желающая ее продавать основному хозяину. В достаточно похожей ситуации оказался и Крис Тарновски, который, как выяснилось в ходе суда, также имел с Canal+ соглашение на исследование защиты смарт-карт нового поколения MediaGuard2, одновременно являясь сотрудником NDS. Судя по заявлениям адвокатов Canal+, Тарновски тоже вроде бы согласился дать честные показания о своем участии в интернет-публикации кода в 1999 году, хотя и не скрывал, что боится.

Но еще больший интерес вызвало появление в печати материалов о специфических контактах с хакерскими кругами со стороны высшего менеджерского звена в империи Руперта Мердока. Бывший руководящий чин Скотланд-Ярда, а ныне глава службы безопасности в компаниях NDS и BSkyB Рэй Эдамс, как выяснилось, лично финансировал английский хакерский веб-сайт The house of ill compute (Thoic.com). Через Thoic шла бойкая торговля контрафактными смарт-картами доступа к ТВ-сети главного конкурента BSkyB в Великобритании, компании ITV Digital, использующей карты MediaGuard. Особую пикантность этой истории придает то обстоятельство, что как полномочный представитель News Corporation Рэй Эдамс является членом совета директоров организации AEPOC – Европейской промышленной группы по противодействию пиратству… [CL02].

Естественно, Рэй Эдамс немедленно стал категорически отрицать свою причастность к распространению пиратских смарт-карт, объясняя затраты в несколько тысяч фунтов стерлингов на финансирование сомнительного сайта исключительно «сбором разведывательной информации о хакерской деятельности». Однако владелец сайта Thoic.com, некто Ли Гиблинг, куда-то бесследно исчез, а сам Эдамс наотрез отказался добровольно раскрыть шифрованную переписку с Гиблингом, поскольку «не намерен обсуждать оперативную деятельность фирмы». Если же учесть и тот факт,

что в совет директоров NDS к этому времени входили два сына Руперта Мердока, Джеймс и Лахлен, то разбирательство в Калифорнии обещало получиться чрезвычайно интересным, поскольку судом уже был издан вердикт, запрещающий NDS уничтожать какие-либо документальные материалы, а высшему руководству – выступать свидетелями по обвинению, предъявленному компании.

Итак, явно назревала шумная разборка, сулившая пролить свет на весьма скрытный и темный сектор индустрии развлечений. Сектор, где руководители и сотрудники известнейших компаний оказываются теснейшим образом переплетены с нелегальным компьютерным андеграундом, а программисты корпораций и кракеры пиратского бизнеса – одними и теми же лицами. Этот суд обещал раскрыть очень многие неясные вопросы, будоражившие интернет-сообщество.

Например, кто стоял за вскрытием смарт-карт ТВ-сети Dish Network компании EchoStar, второго важнейшего игрока на рынке спутникового телевидения в США? Ведь по добытым Canal+ сведениям, Крис Тарновски одновременно с кодом к MediaGuard получил и код к смарт-карте Nagra, закрывающей каналы EchoStar. Если и это сделали в Хайфе, то кто же тогда столь эффективно постоянно вскрывает смарт-карты самой NDS? Ведь компания DirecTV, к примеру, много лет применяющая разновидность VideoGuard, уже до того отчаялась бороться с пиратами, что пошла на разрыв контракта с NDS, решив заняться разработкой смарт-карт собственными силами. (Вместе с недавней покупкой DirecTV Рупертом Мердоком этот демарш, правда, ныне уже свернут). Наконец, почему анализ разброса серийных номеров смарт-карт показывает, что их выпускается чуть ли не в три раза больше, чем количество официальных абонентов платного ТВ? И куда уходят все эти десятки миллионов «резервных» смарт-карт?

Увы, никаких ответов на эти вопросы пока получить не удалось. Уже к началу июня 2002 г., когда в империи Руперта Мердока убедились, что угрозами и через адвокатов замять скандальное дело не удается, в ход был пущен самый решающий аргумент – большие деньги. Взяв в учет сильные финансовые трудности конкурента, корпорация News объявила, что за миллиард евро покупает у Vivendi Universal итальянскую компанию платного ТВ Telepiu. Эта сеть принадлежала Canal+ и чуть ли не более всех пострадала от пиратов – по некоторым подсчетам, среди общего числа зрителей платного спутникового телевидения в Италии пиратскими картами в 2001 г. пользовались почти три четверти. Одним же из главных условий сделки стало то, что Vivendi обязалась прекратить судебное разбирательство в Калифорнии.

С фирмой Canal Plus Technologies в новых условиях обошлись примерно так же, как с Telepiu, – дирекция Vivendi и ее тоже выставила на продажу. В сентябре 2002 г. это подразделение купила французская фирма радиоэлектроники Thomson, но направление смарт-карт условного доступа пришлось здесь не ко двору. Тут же в качестве потенциального покупателя всплыла фирма NDS, и, произойди эта сделка, столь шумный недавно скандал оказался бы окончательно погребенным.

Но в конечном итоге, в августе 2003 г. технологию MediaGuard (и всю сопутствующую ей интеллектуальную собственность) выкупила у Thomson

швейцарская фирма Kudelski. Причем Kudelski – это разработчик тех самых карт Nagra, что закрывают, среди прочего, и платные ТВ-каналы EchoStar. А именно EchoStar, напомним, и ее совместное с Kudelski предприятие NagraStar возродили угробленный было судебный процесс против NDS и жаждут ныне справедливости.

А потому есть шанс, что правда об этой темной истории все же станет известна.

Глава 9. Следить всегда, следить везде

Страницы жизни героя, 1961. Хвост виляет собакой

В 1961 году новый энергичный министр юстиции Роберт (Бобби) Кеннеди объявил «крестовый поход» против организованной преступности. Директор ФБР (долгие годы отрицавший сам факт существования мафии в США) теперь, соответственно, тоже провозгласил борьбу с оргпреступностью главным приоритетом в работе Бюро. В поддержку более решительных действий сил правопорядка были подготовлены новые законы, прохождение которых в Конгрессе сопровождал лично Бобби Кеннеди. Эти законы существенно расширяли и усиливали юрисдикцию ФБР в случаях расследования действий мафиозных структур.

Была здесь, правда, довольно серьезная, чреватая осложнениями проблема – Гувер уже давным давно и в широких масштабах использовал технологии слежки, официально считавшиеся в США незаконными. И теперь директора ФБР беспокоило, что Кеннеди непременно об этом узнает. Ведь традиционные методы подслушивания разговоров и прослушивания телефонов подозреваемых обычно сопровождались нелегальным проникновением в частные жилища и офисы для установки электронных «жучков».

Все же Гувер и далее, как прежде, не стал испрашивать разрешения на установку спецтехники, но зато, с другой стороны, регулярно предоставлял Роберту Кеннеди содержательные оперативные материалы с информацией, собранной с помощью нелегальных микрофонов прослушки. Признавая ценность материалов, министр юстиции вынужден был закрывать глаза на беззаконие и, таким образом, поневоле оказывался пассивным соучастником.

У Эдгара Гувера имелся огромный опыт в умелых манипуляциях столь деликатной вещью, как технические средства полицейского наблюдения. Свою формальную (и, как обычно, абсолютно лицемерную) точку зрения по этому вопросу директор Бюро сформулировал давно и определенно. Еще в первом уставе ФБР, подготовленном в 1928 году, было прописано, что подслушивание является «недопустимым, незаконным… неэтичным», а руководство Бюро подобных мер, соответственно, не потерпит. Тогда же Эдгар Гувер заверил Конгресс, что всякий агент, уличенный в телефонном подслушивании, будет немедленно уволен с работы. На самом деле, конечно же, все было совершенно иначе. Имеется достаточное количество свидетельств сотрудников (в том числе и в суде), работавших в ФБР в

1930-е годы, занимавшихся круглосуточным прослушиванием телефонов и полагавших это вполне обычным делом Бюро.

Весной 1940 года президент Рузвельт, убежденный в том, что в столь тревожное время подслушивание телефонов стало жизненно необходимым для обеспечения национальной безопасности, пошел на серьезное нарушение действовавших в стране законов. Президент тайно наделил министра юстиции несвойственными ему полномочиями – разрешать подслушивание «лиц, подозреваемых в ведении подрывной деятельности против Соединенных Штатов, а также в шпионаже». Как признал многие годы спустя тогдашний министр юстиции Фрэнсис Биддл, эта президентская директива «открыла широкие двери для подслушивания телефонов любого человека, заподозренного в подрывной деятельности». Фактическим результатом данного решения стало то, что Эдгар Гувер получил возможности для неограниченного прослушивания любого не понравившегося ему человека – достаточно было лишь занести его в категорию подозреваемых лиц. Однажды утвердившись в условиях особой предвоенной ситуации, эта беззаконная практика продолжалась и в послевоенные десятилетия.

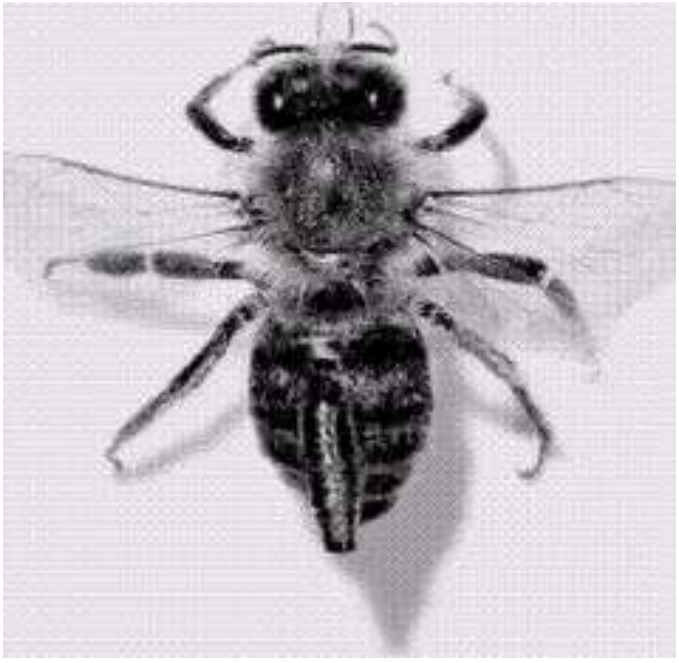
Приход к власти каждой новой госадминистрации неизменно сопровождался для Гувера проворачиванием примерно одной и той же комбинации. Всякий президент и его министр юстиции на словах выступали за строгое соблюдение законов, а на деле охотно и часто прибегали к совершенно нелегальным методам слежки ФБР. При наиболее приятной для Гувера эйзенхауэровской администрации новый министр юстиции Герберт Браунел даже выдал Гуверу официальную санкцию на использование микрофонов прослушивания – но только в случаях угрозы национальной безопасности. С приходом братьев Кеннеди директору ФБР удалось успешно развить законность электронных методов слежки и на расследования иного рода.

По свидетельству Ричарда Никсона – единственного, кто был смещен с президентского поста из-за нелегального шпионажа за политическими противниками – Эдгар Гувер рассказывал ему, что каждый президент со времен Рузвельта давал директору ФБР подобные задания. Иначе говоря, тихий и нераскрытый «Уотергейт» сопровождал каждую госадминистрацию США по меньшей мере с начала 1930-х годов. Скандал же разразился только после смерти Гувера всемогущего. То же самое документально подтвердил в 1975 году сенатский комитет по разведке, установивший, что президенты Трумэн, Эйзенхауэр, Кеннеди, Джонсон и Никсон, – все они использовали ФБР для подслушивания и слежки в целях, не имевших ничего общего ни с национальной безопасностью, ни с борьбой с преступностью. По сути дела, Федеральное бюро расследований использовалось как политическая полиция, преследуя тех людей, чьи взгляды и идеология не нравились лично Эдгару Гуверу, либо его начальству. Вовлекая каждого нового президента в это заманчивое беззаконие, шеф ФБР одновременно получал и эффективное прикрытие для продолжения нелегальной слежки, и мощный компромат на первых лиц государства.

Шпионский зоопарк

Всевозможные хитрые устройства и технологии для поиска врагов, скрытного наблюдения, прослушивания и вообще для «тотальной информационной осведомленности» вот уже многие десятилетия вдохновляют фантазии авторов шпионских романов и кинофильмов. Но попутно над многими из этих «фантастических» проектов вовсю идет вполне реальная работа в секретных лабораториях спецслужб и закрытых исследовательских центров, а порой – и в обычных университетах или коммерческих фирмах. В этом разделе дается краткий обзор подобного рода специальных технологий, так или иначе связанных с биологическими организмами.

Пчелы-бомбоискатели



Американское агентство передовых военных исследований, DARPA, финансирует работы федеральных и академических исследовательских центров по изучению пчел и возможностей использования их более тонкого, чем у собак, обоняния в серьезных розыскных мероприятиях. В частности, смешивая тротил с сахаром, ученым удается натаскивать пчел на поиск взрывчатки. К насекомым прикрепляют миниатюрные радиочастотные метки-идентификаторы (RFID) изготовляемые швейцарской фирмы Sokymat. В сочетании с сенсорами в ульях, улавливающими запахи принесенных пчелами опасных химикатов, в принципе становится возможным автоматизировать весь процесс поиска и обнаружения мин.

Есть, правда, довольно существенная проблема – пчелы хоть и трудолюбивы, но не любят работать в непогоду [SI03][MN02].

Помесь дрожжей и тараканов

Осенью 2003 г. стало известно, что ученые ядерного исследовательского центра Sandia National Labs, занимающиеся также

вопросами выявления оружия массового уничтожения, разработали необычную и сравнительно дешевую новую технологию для отыскания опасных химических или биологических веществ. В самом кратком изложении суть нового метода звучит оригинально – скрещивание дрожжей и тараканов. Если чуть более подробно, то, по словам одного из руководителей проекта Джефа Бринкера, тараканы давно привлекают исследователей своими «эксплуатационными характеристиками» – живучестью и надежностью. К спинкам этих насекомых можно прикреплять специальные устройства-сенсоры, а затем скрытно запускать тараканов в те места, где есть подозрение на изготовление/хранение химического оружия. Роль же удобного и чувствительного сенсора-индикатора могут играть дрожжи, поскольку генетической модификацией клеток их можно настраивать для реакции на конкретные химические соединения. И если в среде обнаружатся молекулы искомого вида, то клетки дрожжей изменяют свою окраску. Конечно, при таком методе разведки возникает естественная проблема – возвращать тараканов для анализа датчиков. Пока что одним из простых решений этой проблемы ученым видится использование тараканов-роботов [SV03].

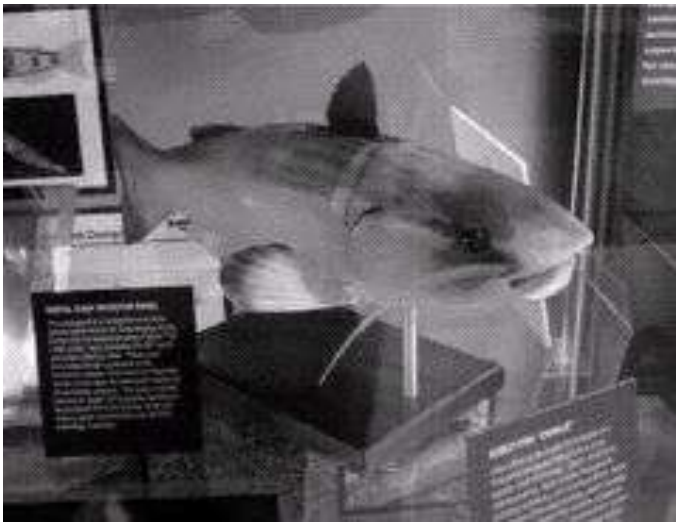
Чуткая стрекоза и сом Чарли

Для кого-то идеи ученых из Sandia могут звучать чистой фантастикой, однако широкая публика имеет очень слабое представление о реальных достижениях в области шпионских технологий. Ярчайший пример тому – специальная выставка в штаб-квартире ЦРУ в Лэнгли, приуроченная к 40-й годовщине здешнего Управления науки и технологий, образованного в августе 1963 года. Выставка эта недоступна для обычных людей с улицы, однако благодаря получившим специальное приглашение корреспондентам информационных агентств имеется возможность познакомиться хотя бы с некоторыми из представленных здесь многочисленных шпионских гаджетов.

Если говорить о роботах-насекомых, то еще 1970-е годы в ЦРУ создали механическую стрекозу, несущую на себе крошечное подслушивающее устройство. Рассказывая историю этого экспоната по порядку, гиды сообщают, что сначала конструкторы ЦРУ создали миниатюрный микрофон-передатчик, для доставки которого в нужное место требовалась какая-нибудь эффективная система транспортировки. Сначала решили построить робота-шмеля. Однако вскоре выяснилось, что полет шмеля – вещь крайне экзотическая и весьма сложная для моделирования, поэтому от этой идеи отказались. Один из любителей-энтомологов, участвовавший в проекте, предложил стрекозу, результатом чего и стал первый летающий робот-прототип размером с насекомое. Для своего времени это был весьма выдающийся аппарат-«инсектотоптер» с крошечным «топливным баком» для ракетного двигателя и тонко сработанным мастером-часовщиком специальным механизмом для хлопанья крылышками. Полет стрекозы к нужной точке направлял лазерный луч. Однако, вся изобретательность конструкторов оказалась напрасной, поскольку роботом было невозможно управлять даже при слабом ветерке, а при малейшем порыве он безнадежно сбивался с курса. Поскольку самое главное в устройстве было

не полет, а доставка микрофона строго в заданную точку, то от проекта пришлось отказаться.

Другой впечатляющий экспонат выставки – это довольно крупный, 60 см длиной, робот-сом в резиновом корпусе, изготовленный в 2000 г. и получивший имя «Чарли». Этот сом должен был незаметно плавать среди других рыб, выполняя столь ответственное задание, что суть его по сию пору остается засекреченной и не раскрывается посетителям даже закрытой выставки. Сообщается лишь, что это пример разработок ЦРУ в области подводной роботехники [SG03].



Робот-сом «Чарли»

Кошка, гулявшая не сама по себе

Этого экспоната по целому ряду причин нет на выставке достижений шпионского хозяйства в Лэнгли. Хотя суперсекретный проект под названием «Акустическая киса» (Acoustic Kitty) тоже был составной – причем довольно дорогостоящей – частью исследовательских работ на самом раннем этапе истории Управления науки и технологий ЦРУ. Информация об этом жутковатом эксперименте попала в руки историков-исследователей разведки, в общем-то, случайно, среди целой партии старых архивов ЦРУ, рассекреченных в 2001 г. по запросу ученых на основании закона FOIA (о праве граждан на доступ к информации). Среди документов об уже известных тайных программах ЦРУ под кодовыми именами ARTICHOKE и MKULTRA, экспериментировавших с наркотическими веществами, изменяющими человеческое сознание, оказался и обзор проекта Acoustic Kitty.

Суть его в том, что в середине 1960-х годов инженеры и ученые разведслужбы пытались встроить в тело живой кошки подслушивающую аппаратуру и передатчик. С помощью этого изуродованного животного-«киборга», натасканного двигаться на звук и забираться на нужные подоконники, американские шпионы намеревались выведать самые секретные планы Кремля.

Несчастного кота с зашитыми в потроха батарейками-микрофонами и с антенной передатчика в хвосте один раз даже вывезли на «полевые

испытания» в парк, где он должен был приблизиться к двум беседующим на скамейке людям. Но едва животное выпустили из набитого электроникой шпионского автофургона, как оно тут же угодило под колеса проезжавшего мимо такси. Собственно, этим печальным происшествием и завершилась многолетняя, научно-исследовательская программа ведущей разведслужбы Америки, обошедшаяся налогоплательщикам в 15 миллионов долларов [GB01].

Исследователи-историки, знакомившиеся с итоговым отчетом о проделанной работе, не могли не обратить внимание, что материалы почти сорокалетней давности рассекречены с заметными купюрами. Значит, часть исследований не потеряла актуальности и далеко не все из когда-то содеянного расценивается как ошибка.

Настоящая шпионская крыса

Очень скоро, весной 2002 года пришло известие, что навязчивая идея о шпионских животных-киборгах по-прежнему продолжает будоражить умы американского военно-разведывательного сообщества и работающих по его заданию исследователей. Ученые SUNY, университета штата Нью-Йорк, опубликовали в майском номере журнала Nature статью с отчетом о том, как они создали целое небольшое подразделение из пяти радиоуправляемых «крысоботов» (ratbots), т.е. крыс с вживленными в мозг электродами для дистанционного манипулирования поведением животных.

Крысобот и его создатель

Функционирует крыса-киборг следующим образом. В «центр удовольствия», т.е. в особый нервный узел, находящийся в срединно-передней части мозга, вживлен главный стимулирующий электрод, а в нервные узлы левых и правых пучков усов крысы вживлены «поворотные» электроды. Животное очень быстро осваивает дрессировку, когда для получения нового импульса блаженства надо просто свернуть в ту сторону, с которой поступает очередной управляющий сигнал. Попутно эмпирическим путем ученые выяснили, что при простой небольшой стимуляции центра удовольствия крыса продолжает двигаться прямо, а при более интенсивной готова на «подвиги»: при возможности забирается на дерево или лестницу, прыгает с высоты, бегает по рельсам или выходит на ярко освещенные участки (чего в обычной жизни, как правило, делать

избегает). Правда, установлено и то, что инстинкт самосохранения в животном действует все же мощнее, так что с опасной для жизни высоты крысу-робота не удается заставить прыгнуть никакими электростимуляциями «нирваны».

Американские ученые, вероятно, осознают, что все эти их нынешние изыскания весьма мерзко попахивают, поэтому ими всячески отрицаются какие-либо параллели с печально известными экспериментами 1960-х годов в университете Tulane, где с помощью вживления в мозг электродов пытались управлять поведением человека. Для получения хотя бы молчаливого одобрения общественности, под проект подведена «благородная» идеологическая база – крысы-роботы, мол, в перспективе способны оказать неоценимую помощь при спасении людей из-под развалин зданий. То, что развалины зданий обычно в избытке заполнены обычной пищей крыс и заставить их работать в этих условиях будет крайне проблематично – на этом предпочитают не фокусироваться. Пока же полным ходом развернуты работы по прилаживанию к крысам микро-телекамер и по миниатюризации всей «заплечной» радиоэлектроники беспроводной связи, чтобы со временем ее можно было имплантировать непосредственно в тело животного. Финансирование всей этой крысиной работы ведет, естественно, Министерство обороны США [DG02].

Глаза в небесах

Вполне естественное желание всякой власти, получающей в свое распоряжение эффективные технологии слежки, – распространить их как можно шире. Но добиться этого сравнительно просто – были бы деньги – лишь в военном деле и в зарубежной разведке, где дозволены практически любые доступные формы шпионажа. Внутри же всякой цивилизованной страны, имеющей представление о презумпции невиновности, обычно действуют вполне определенные правовые нормы, запрещающие, вообще говоря, слежку за гражданами, не совершившими никаких преступлений. Для обхода этой крайне обременительной для власти проблемы изобретено множество всевозможных хитростей и уловок. Например, сначала применить новую технологию в отношении стопроцентных преступников или мошенников, убедив общество, что так – с новым приглядом – ему станет жить намного лучше. Или, скажем, ввести некое постоянное «полуособое-полувоенное» положение для защиты страны от террористов, ради чего населению, ясное дело, придется перетерпеть утрату некоторых гражданских прав и свобод. Наконец, можно просто тщательно засекретить наиболее заманчивые технологии слежки, а дальше просто делать вид, что ничего необычного не происходит.

Большой Брат следит за тобой

Для начала – пример одного из весьма нечастых пока что случаев использования спутниковой видовой разведки для обвинения частных лиц в США. Дело происходило летом 2001 года, когда федеральная власть строго, более чем на 300 тысяч долларов, наказала семью нерадивых

арканзасских фермеров за ложные заявления и обманным путем полученную страховку.

Крупно застраховав свои поля на случай непогоды и плохого урожая, эти фермеры выждали нужный срок и заявили в страховую компанию, что вследствие заморозков и чрезмерных осадков урожай их хлопка погиб фактически подчистую. Страховку им компания выплатила, причем особо не вдаваясь в подробности дела, благо по действующим сейчас в США правилам «сельскохозяйственные» риски компенсируются выплатами из федерального бюджета. Именно поэтому делом заинтересовались сотрудники прокуратуры, быстро заметившие в этой истории нестыковки – путаницу в отчетах о закупке семян, на редкость приличный урожай фермера-соседа и тому подобное. Но дело было уже давнее, и достоверно восстановить картину, как подсказал один из сведущих людей, могли лишь спутниковые снимки фермерских полей за соответствующий период.

Поначалу следователь прокуратуры отправил запросы в американские спецслужбы, занимающиеся спутниковой разведкой, но там сходу дали от ворот поворот, заявив, что заниматься подобными вещами внутри страны им запрещает закон. Тогда следователь расширил поиск и нашел то, что нужно– Управление геологических изысканий, где постоянно накапливаются инфракрасные спутниковые снимки всей территории Штатов. Снимки делаются в любую погоду, и с их помощью специалисты не только могут сказать, вспахано поле или нет, но даже какого типа растения там посажены. После того, как в базе данных были подняты снимки нужных территорий за нужные даты, эксперты-дешифровщики изображений установили, что свыше 80% земли «пострадавшей от заморозков» вообще в тот год не распахивалось… Когда все эти факты были представлены на суде, фермеры и их адвокаты были настолько ошарашены, что даже не смогли решить, имеет ли теперь смысл подавать на апелляцию [DB01].

У нас свой Хаббл

Нельзя сказать, что современный уровень технологий слежки является каким-то особым секретом. Просто обыкновенные люди, профессионально никак не связанные с данной областью, слишком заняты своими текущими делами, чтобы интересоваться информационными проспектами или веб-сайтами фирм-изготовителей такого рода аппаратуры.

Вот, скажем, как обстоят сейчас дела с новейшими системами визуального наблюдения, устанавливаемыми ныне в вертолетах полиции и вооруженных сил. Здесь прогресс в электронных и механических технологиях позволил объединить видеокамеры и оптику высокого разрешения с мощными системами стабилизации, что дает возможность, к примеру, определять номер автомобиля практически с любой высоты полета, а ограничения на дальнодействие аппаратуры накладывает лишь линия горизонта и естественная дымка атмосферы.

Ведущий поставщик систем наблюдения для полиции, компания Wescam (канадское подразделение фирмы Westinghouse) несколько лет назад создала новое, третье поколение систем стабилизации, радикально превосходящее прежние конструкции на основе механических гасителей

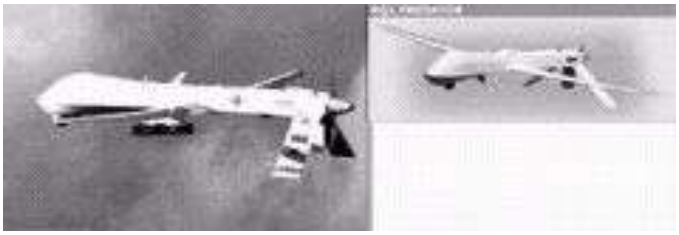
вибрации и гироскопов. В новейшей системе на смену вращающимся механическим гироскопам пришли их оптоволоконные аналоги, где малейшие смещения в расположении камеры вычисляются благодаря лазерным импульсам и постоянному пересчету координат компьютером. После чего коррекция положения производится с помощью новой технологии «приводов магнитного крутящего момента», прикладывающих усилие в строго определенном направлении, оставляя свободным движение во всех остальных плоскостях. За последнее время о создании собственных оптоволоконных систем гиростабилизации объявили также компании Raytheon и FLIR Systems, тоже выпускающие оборудование наблюдения для военного и полицейского использования.

Именно благодаря этой системе стабилизации теперь стало возможным применять мощные увеличительные линзы, в результате чего полиция стала в шутку называть прибор «наш наземный Хаббл», имея в виду, конечно, мощнейший орбитальный телескоп астрономов. При сравнении же характеристик системы Wescam со спутниковыми разведывательными системами наблюдения, радиус обзора последних, естественно, оказывается значительно шире, однако камеры на самолетах и вертолетах дают возможность «живой» видеосъемки происходящего, а не трансляцию фотоснимков, что свойственно орбитальным аппаратам. Стоимость нового оборудования видеослежения довольно велика – порядка 650 тысяч долларов для наиболее продвинутых моделей, однако в Wescam надеются на расширение бизнеса, поскольку живой интерес к новой технологии проявляют не только военные и правоохранительные органы, но также киноиндустрия и телевизионные службы новостей [IA02].

Кара небесная

Чрезвычайно модная на сегодняшний день технология – беспилотные летательные аппараты, БПЛА, обычно именуемые «дронами» (drones) или более официально UAV, от Unmanned Aerial Vehicle. Подобные аппараты – эдаких летающих роботов – очень любят военные всех стран, выделяющих много денег на оборону, поскольку дроны могут находиться в воздухе очень долго (до суток), а их потеря не сопряжена с рисками гибели летного состава. С каждым годом БПЛА все больше применяют для воздушной разведки на местности, а в последнее время и для уничтожения людей или техники противника.

В ноябре 2002 года беспилотный разведывательный самолет Predator, дистанционно управляемый ЦРУ США и вооруженный двумя противотанковыми ракетами Hellfire, уничтожил в Йемене автомобиль и находившихся в нем 6 человек. Предполагается, что это были террористы «Аль-Каиды» во главе с одним из лидеров этой организации Каедом аль-Харети по прозвищу Абу Али. Данная операция стала первым известным случаем применения Соединенными Штатами разведсамолетов-роботов для уничтожения людей вне зоны боевых действий. Первые же сообщения о применении таких самолетов-разведчиков для уничтожения военных целей стали появляться в ходе боевых действий США и их союзников в Афганистане в начале 2002 года [WK02].



длина: 8,2 м Скорость *max :* 225 км/ч
высота: 2,1 м Дальность действия: 740 км
размах кр.: 14,8 м
вес: 430 кг Цена: 25 млн $
БПЛА Predator с ракетным вооружением (слева)

Министр обороны США Дональд Рамсфелд наотрез отказался комментировать подробности военной операции в Йемене, но выразил вполне однозначное удовлетворение известием о предполагаемом уничтожении Каеда аль-Харети: «Он находился в розыске как член Аль-Каиды и был одним из террористов, подозреваемых в организации подрыва эсминца ВМС США Cole. Поэтому было бы очень хорошо, если его удалось вывести из дела». То, что людей в Йемене уничтожили абсолютно такими же террористическими методами – на чужой мирной территории, без арестов, разбирательства и суда, простым запуском двух ракет – эта проблема осталась полностью за рамками обсуждения.

Зато в новом оборонном бюджете на 2004 год американские военные отдельно выделили 1 миллиард долларов на дальнейшее развитие технологии как вооруженных, так и просто шпионских БПЛА. Всем хороши для милитаристов эти аппараты – не задумываясь палят, куда им велят, да и потерять их, случись чего, не так жалко – летчика-то внутри у них нет, значит и спросу меньше. Не очень удобно лишь то, что самолеты-роботы не могут находиться в воздухе долгое время и регулярно требуют заправки горючим. Вот над этой проблемой и бьется ныне военная инженерная мысль. Причем небезрезультатно.

БПЛА Global Hawk

Научно-исследовательский центр ВВС США AFRL (US Air Force Research Laboratory) финансирует сейчас создание по крайней мере двух версий самолетов-шпионов с ядерным двигателем на базе тяжелых беспилотных летательных аппаратов Global Hawk компании Northrop-Grumman. На

проходившей в феврале 2003 г. Конференции аэрокосмических технологий в Альбукерке, шт. Нью-Мексико ученые AFRL представили последние результаты этой разработки, обещающие за счет ядерного двигателя продлить срок полета БПЛА с нескольких часов до многих месяцев.

Вообще говоря, аэропланы с ядерным мотором – идея не новая. Еще в 1950-е годы и в США, и в СССР пытались разработать реактивный двигатель на ядерном топливе для пилотируемых самолетов. Но от мысли этой в конце концов пришлось отказаться, поскольку и конструкция получалась непомерно тяжелая, да и экипаж защищать от ядерного реактора на борту было слишком дорого. Однако научная мысль не стоит на месте, и ныне авиаторам вместо традиционного реактора ядерного деления предложен существенной иной тип энергогенератора под названием квантовый нуклеонный реактор. Здесь энергия получается за счет использования рентгеновского излучения, которое стимулирует ядра радиоактивного гафния-178 к переходу на более низкие энергетические уровни и высвобождению энергии в форме гамма-излучения. В самолете-шпионе на ядерном ходу тяга будет создаваться за счет использования этой энергии для формирования реактивной струи раскаленного воздуха. Вся эта разработка была инициирована военными конструкторами после публикации 1999 года группы Карла Коллинза из Техасского университета, которая обнаружила, что рентгеновским облучением гафния можно высвобождать энергии в 60 раз больше, нежели затрачено [DR03].

Конечно, вся эта конструкция получается изрядно радиоактивной, однако, как пытаются успокоить публику американские военные, при умелом обращении рентгеновские и гамма-лучи вовсе не так опасны для обслуживающего персонала. Но тут же возникает и другая проблема – ведь беспилотные самолеты-шпионы весьма часто сбивают, а гафний имеет период полураспада 31 год, что по данным радиологов эквивалентно высокорадиоактивному цезию-137. Другими словами, уничтожение постоянно висящего в небе вражеского самолета-шпиона становится эквивалентно подрыву «грязной бомбы», надолго отравляющей все вокруг. Понятно, что подобная технология сразу порождает серьезнейшие политические вопросы о допустимости ее применения. На подобные сомнения у американских военных находится потрясающий аргумент: «Ну, наверное это такая штука, от которой вы захотели бы держаться подальше, но она вас не убьет». Это дословная цитата из комментариев Кристофера Хэмилтона, руководителя нынешних американских исследований ядерных БПЛА. Интересно было бы услышать, как заговорил бы этот человек, упади такой самолет при испытаниях возле его собственного дома?

Всевидящее око

В марте 2002 года на «разоблачительном» сайте www.almartinraw.com, принадлежащем американцу Элу Мартину, появилась статья с неуклюжим, но задиристым названием «Летающий фашизм у твоего порога». Большую часть статьи занимал рассказ некоего анонимного полковника, своими глазами увидевшего на военной ярмарке Redstone Arsenal's Arms Bazaar небывалое чудо техники – аппарат под названием DCHD, или Domestic

Control Hover Drone, что можно перевести как «парящий робот внутреннего надзора» [AM02].

Формой этот беспилотный аппарат представляет собой тор (или, говоря проще, бублик) с двумя соосными винтами по центру, для устойчивости машины вращающимися в противоположных направлениях. Он может вертикально взлетать и садиться, а также зависать на любой высоте до 200 м. Летает практически бесшумно, в движение приводится электромотором, источник энергии – топливный элемент, позволяющий находиться в воздухе до трех часов. Такую «летающую тарелку» можно оснастить самой разнообразной аппаратурой слежения, от телекамер с мощной оптикой и приборов ночного видения до направленных микрофонов. Кроме того, летающий робот может комплектоваться оружием нелетального поражения для лишения подвижности подозрительных лиц, мощным громкоговорителем и телескопическим кронштейном, который увенчан считывателем смарт-карт – для проверки идентификационных удостоверений граждан.

Дистанционное управление системой осуществляется либо с мобильного наземного пункта (автомобиля), либо удаленно через спутниковую систему. По свидетельству демонстрировавшей оборудование компании (в статье Мартина ее имя не названо), аппарат можно купить хоть сейчас по цене от 180 до 350 тысяч долларов в зависимости от комплектации…

Что бы там ни говорил никому неведомый полковник, без конкретных сведений о модели и фирме-изготовителе аппарата-шпиона вся эта информация, конечно, весьма смахивала на обычную «утку», каких в Интернете пруд пруди. По этой причине можно было бы просто скептически хмыкнуть да и пойти себе бродить по Сети дальше, если б не личность автора публикации Эла Мартина. Человек этот – бывший старший офицер ВМС США и ветеран военно-морского разведуправления ONI (Office of Navy Intelligence). В 1980-е годы Мартин был одной из центральных фигур в самом громком политическом скандале той поры – так называемом деле «Иран-Контрас», где его фамилия фигурирует обычно в одном ряду с Оливером Портом, Джорджем Бушем-папой и сыном его Джебом Бушем (с 1999 года– губернатором ключевого в президентских выборах штата Флорида).

Американским властям не без труда, но удалось все-таки замять эту неприглядную историю, однако у Мартина, тяжело болеющего в последние годы, проснулась совесть, и он излил душу в книге «Заговорщики. Тайны инсайдера дела Иран-Контрас» [AM01]. Эта книга – личный отчет участника многочисленных нелегальных операций, санкционированных американским правительством. Мартин сообщает все, что знает о тайно санкционированных властями США крупномасштабных акциях в области производства и торговли наркотиками, о гигантской нелегальной сети торговцев оружием и о миллиардных мошенничествах с банковскими счетами, недвижимостью и страхованием. С приходом к власти представителя «клана Бушей» Эл Мартин посчитал целесообразным уйти, по сути дела, в подполье, а с миром стал общаться через свой веб-сайт.

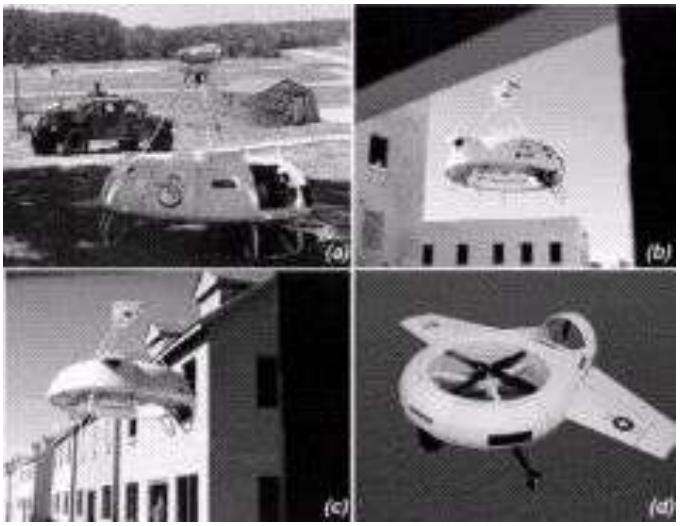
Принимая во внимание все эти обстоятельства, отмахнуться от информации о новой необычной технологии было бы, мягко говоря,

опрометчиво. К тому же поиск дополнительных данных в Интернете свидетельствует, что шпионская тарелка-робот, похоже, вовсе не фантазия. Так, еще в 1982-88 годах по заказу Корпуса морской пехоты США разрабатывался беспилотный разведывательный аппарат AROD (Airborne Remotely Operated Device – «дистанционно управляемое летательное устройство»). Уже этот AROD имел характерные черты нынешнего робота с выставки в Redstone Arsenal: форма небольшой летающей тарелки, упрятанные в кожух винты, электромотор, вертикальные взлет и посадка. Правда, для аппаратов второго поколения, которые конструировала Национальная лаборатория Sandia, потребовалась большая подъемная сила, и электромотор заменили бензиновым 26-сильным двигателем. Летающий робот-наблюдатель управлялся с помощью манипулятора-джойстика, а пара телекамер на борту и шлем со стереодисплеем у оператора давали возможность для полноценного объемного обзора местности. AROD был испытан в свободном полете, однако посредственные аэродинамические качества и неустойчивость аппарата в воздухе привели к сворачиванию проекта [RO99].

В начале 90-х за тот же проект взялась корпорация Sikorsky Aircraft, разработавшая такие знаменитые вертолеты, как Comanche и Black Hawk. Уже в 1992 году она продемонстрировала в «привязанном» полете собственный прототип беспилотного аппарата, названного Cypher. Позже появлялась информация по меньшей мере о четырех его модификациях, о полутысяче налетанных часов, а также о десятке успешных демонстраций на правительственном уровне.

БПЛА Cypher , базовая модель

Базовая модель Cypher имеет диаметр чуть более двух метров, роторную систему из двух коаксиальных винтов и 50-сильный двигатель, позволяющий развивать скорость до 80 узлов (150 км/час) при потолке 260 метров, время в полете – до трех часов. Модель Cypher II (Dragon Warrior), разработанная с учетом требований Корпуса морской пехоты, имеет чуть меньший диаметр. Есть модификация с крыльями – для действий в прибрежной полосе, а есть точно такая же, но без крыльев, – для разведки в условиях города. Известно также о моделях Mini-Cypher диаметром около метра и крупном аппарате Cypher III для военно-морских сил.



Cypher и мобильный пункт управления (а), демонстрация в Форт-Беннинге (Ь,с), модель Cypher II (d)

Еще в начале 2002 г. на сайте корпорации Sikorsky страницы и фотографии, посвященные этому проекту, сопровождала гордая надпись: «То, что вы видите, – это не научная фантастика, это беспилотный летательный аппарат Cypher для военных и гражданских применений». Интересно, что примерно одновременно с публикацией Эла Мартина о «летающем фашизме у порога» все страницы о Cypher с сайта www.sikorsky.com исчезли. Но в Интернете по-прежнему можно найти множество сообщений об этом проекте, в частности об эффектной демонстрации в Форт-Беннинге, на полигоне для отработки военных операций в городской местности. Аппарат уверенно летал по улицам на уровне окон домов, садился на крыши и между зданиями, в зазоры около четырех метров. Испытывался он и с разведывательной аппаратурой. К примеру, Cypher демонстрировал, как в автоматическом режиме может отыскивать и сопровождать цели величиной с человека, применялся он и в учениях военной полиции, посвященных отработке мер противодействия наркоторговцам. А для Министерства энергетики США робот отыскивал подземные сооружения и туннели с помощью установленных на борту магнитометров [www.sikorsky.com/programs/cypher/, www.sikorsky.com/programs/cypher/cypher_more.html, копии см. на http://gbop.nm.ru/cypher.htm].

Из самых последних сообщений (до перевода аппарата в «засекреченные») следует отметить пресс-релиз Sikorsky, датированный июлем 2001 года и сообщающий об успешных испытаниях дрона Cypher II, специально построенного для Лабораторий ночного видения армии США (U.S. Army Night Vision Labs). В режиме «умного прибора» робот может самостоятельно взлетать, садиться и работать в воздухе, ориентируясь на местности с помощью системы GPS. В качестве же основного предусмотрен режим ручного управления с мобильной наземной станции [SC01].

Короче говоря, даже при поверхностном обзоре ресурсов Сети многим «фантастическим» подробностям в рассказе полковника-приятеля Эла Мартина находятся документальные подтверждения. Вполне возможно, что более тщательные поиски существенно дополнят картину. Впрочем,

некоторым и искать ничего не надо. Ведь по свидетельству все того же полковника, из зарубежных посетителей выставки в Redstone Arsenal наибольший интерес к летающей тарелке-роботу проявили гости-специалисты из Британии, Китая и России.

Ну, а пока доработка бесшумного летающего робота Cypher идет под завесой секретности, в структурах власти США тем временем понемногу внедряется идея об использовании дронов-наблюдателей внутри страны. Для начала – чтобы слишком не пугать обывателей – беспилотные летательные аппараты предложено использовать в охране границы с Мексикой, откуда в страну прибывает наибольшее число нелегальных иммигрантов (а значит – также наркоторговцев и террористов). Выступая перед членами сенатского комитета по торговле, науке и транспорту, глава Управления безопасности отечества Том Ридж обосновал необходимость применения БПЛА очень просто: «Если мы действительно намерены победить терроризм, то нам просто необходимо оснастить их (пограничные патрули) такого рода технологией» [DT03].

На тебя, техника, уповаем

После 11 сентября 2001 года в США, где привыкли считать себя технологическим авангардом человечества, весьма популярны дискуссии на тему «Что еще можно сделать, чтобы техника обеспечила государству максимальную безопасность». Конечно, хватает и таких людей, для кого вполне очевидна наивность упований на технологическую защиту в условиях, когда «поле сражения» – всюду, а всякий случайный прохожий – потенциальный террорист. И что все проблемы сводятся вовсе не к технике, а к людям…

Но подобные идеи сейчас никак не назовешь популярными. Власти крупных американских городов, напротив, при всяком удобном случае скандируют, что они по-прежнему столь же беззащитны, как и до 11 сентября известно-какого-года, так как им, дескать, катастрофически не хватает денег на установку всевозможных сенсоров, систем выявления и мудреного оборудования реагирования на опасность. Возможно, вздыхают мэры, ситуация сдвинется, когда начнут поступать те 3,5 миллиарда долларов, которые Белый дом обещает выделять местным властям на техническое оснащение.

А пока что предмет всеобщей мэрской зависти – это Вашингтон, который благодаря столичному статусу, сравнительно небольшому размеру и солидной помощи из федерального бюджета являет собой образец технологических ответов на террористические угрозы. Достаточно лишь окинуть взором транспортную систему города. Местные власти, надо сказать, всерьез озаботились безопасностью еще в 1995 году, отреагировав на газовую атаку с применением зарина в токийском метро, когда погибло двенадцать человек и пострадало несколько тысяч. Сразу же после 11 сентября, в октябре 2001 года, столичная администрация запросила у Конгресса и президента 190 миллионов на укрепление безопасности города. В апреле 2002 года – еще 107 миллионов долларов. На эти деньги чего только не придумали. И детекторы перемещений для автобусных парков и железнодорожных депо – если кто-то вдруг

попытается заложить бомбу с часовым механизмом. И специальные GPS-локаторы, которые подают сигнал тревоги, если рейсовый автобус уклоняется от маршрута или угнан со стоянки. Еще запущена пилотная программа по установке цифровых камер слежения в автобусах, а также задуман план прокладки оптоволокна для объединения всех следящих телекамер на станциях метро.

Метро столичного округа Колумбия вообще заслуживает отдельного разговора. Достаточно сказать, что это первая подземка в мире, которая оборудуется сенсорами химического оружия (даже в Токио нет ничего подобного). Две подземные станции были оснащены такого рода датчиками еще до 11 сентября. Еще десять станций начали оснащать в первый же год «затяжной войны с терроризмом», а 20 млн. долларов из дополнительных 107 миллионов запланировано потратить на пятнадцать следующих станций. Со временем предполагается оборудовать такими же сенсорами вообще все станции метро, но и на этом процесс модернизации вовсе не закончится, поскольку в будущем ожидается появление детекторов биологического оружия, а значит – станции будут дооснащаться и ими. Кроме того, на случай химической атаки все работники метрополитена обеспечиваются защитными костюмами и масками-противогазами [MN02].

Естественно, находятся и такие эксперты, которые взирают на всю эту бесконечную и весьма дорогостоящую суету с глубочайшим скепсисом и тоской, поскольку, по их убеждению, в принципе невозможно создать техническую систему раннего оповещения обо всех возможных биологических, химических или взрывчатых угрозах. Достаточно взглянуть на пример Израиля, где не помогают никакие технологии, а ради предотвращения взрывов, по сути дела, пришлось бы тщательно обыскивать каждого прохожего.

В качестве слабого, но зато реализуемого на практике аналога тотального обыска выступают ныне телекамеры наблюдения, которые власти пытаются устанавливать во всех мыслимых публичных местах. Разумеется, далеко не всем это по нраву. В июне 2002 года городской совет Вашингтона обсуждал план создания интегрированной сети телекамер наблюдения, объединяющей камеры полиции, метрополитена и школ. В ходе этого обсуждения правозащитная организация ACLU (активно выступающая против данной технологии) напомнила, что в Лондоне для борьбы с терроризмом с начала 1990-х годов установлено более 150 тыс. телекамер, однако за десяток лет эксплуатации не отмечено ни единого случая поимки с их помощью хоть какого-нибудь завалящего террориста. (Впоследствии, правда, ACLU все же пришлось поправиться, поскольку однажды, в 1993 году после взрыва в универмаге Harrods анализ видеозаписи привел к нескольким арестам.)

Великобританию, очевидно, следует считать страной с наибольшим опытом использования телекамер наблюдения. Хотя бы потому, что в 2002 году из 25 миллионов таких камер, в общей сложности установленных по всему миру, 10% (2,5 млн) приходилось на Соединенное королевство. Причем закупки осуществляются в таком темпе, что еще через пять лет, в 2007 году аналитики предсказывают 10-кратное увеличение уже имеющегося количества. Другими словами, уже на одну Британию будет приходиться камер столько, сколько совсем недавно их было на весь мир.

В настоящее время, согласно статистике, средний британский гражданин попадает в поле зрения камер наблюдения свыше 300 раз в день – на оживленных улицах, в магазинах, на перронах железных дорог и подземки, в аэропортах и административных зданиях. Появление недорогих и функционально более гибких цифровых камер на смену аналоговым называют главной причиной резкого роста новых точек постоянного наблюдения. Помимо всего прочего, множество цифровых камер можно сводить в единую сеть и вести удаленное наблюдение через Интернет (технические особенности аналоговых телекамер допускали передачу лишь по выделенным линиям на расстояние не более 170 километров).

Изготовители новых систем наблюдения уже предвкушают грандиозные прибыли от своего бизнеса, поскольку вместе с приходом Интернета в каждый дом им уже видится картина, когда телекамеры слежения в изобилии появятся не только абсолютно во всех общественных местах, но и чуть ли не в каждой комнате частных жилищ. Какой из заботливых родителей, спрашивают они, откажет себе в недорогом удобстве проследить за тем, чем занята няня, вызванная посидеть с маленьким ребенком? Или просто заглянуть с работы в детскую, когда ребенок подрастет? Или, наконец, окинуть взглядом оставленную квартиру, находясь с семьей где-нибудь в отпускной поездке?

Насколько очевидны ответы на подобные вопросы, каждому человеку еще предстоит разобраться самостоятельно. Для общества же в настоящее время гораздо более насущным является другой вопрос. Действительно ли, как заверяет правительство, повсеместно устанавливаемые на улицах и в общественных местах телекамеры наблюдения сокращают преступность? По убеждению английской полиции, в этом не может быть никаких сомнений. Логика аргументов правоохранительных органов очень проста – ни один нормальный преступник не станет заниматься уличным грабежом или торговать наркотиками под пристальным взором телекамер.

Но с подобными доводами соглашаются далеко не все специалисты по преступности. Например, всеобъемлющее исследование влияния камер наблюдения, проведенное недавно аналитиками в Глазго, продемонстрировало, что на самом деле телекамеры не сокращают количество преступлений и не являются мерой, способной их предотвращать. В этом же исследовании делается вывод, что простое улучшение освещения оказывается более эффективным и менее дорогостоящим способом сокращения преступлений в общественных местах. В чем же реально телекамеры оказываются полезны, так это в ускорении сроков прибытия нарядов полиции к местам беспорядков, следствием чего становится сокращение тяжелых травм при массовых драках [JW02][CCO3].

Одна из интересных идей, сама собою рождающихся на фоне тотального распространения шпионских телекамер слежки, – что все это, кто знает, может оказаться и благом, ведущим в перспективе к более прозрачному и открытому обществу людей, которым нечего скрывать. Но ключевым условием этого должны непременно стать общедоступные мониторы слежения за кабинетами менеджеров и директоров крупных корпораций, за офисами руководителей правительственных и прочих

государственных учреждений. Например, во Франции публичные веб-камеры установлены на ядерных электростанциях, чтобы у граждан всегда была возможность убедиться – там все в порядке и под контролем.

Но в целом, конечно же, до столь радикального переворачивания идеи Большого Брата, постоянно находящегося начеку, ни одно общество, даже самое демократическое, пока еще не дозрело. Впрочем, определенные сдвиги в этом направлении обозначились вполне отчетливо.

Глава 10. Альтернативы есть всегда

Страницы жизни героя, 1965-2003. Все тайное вырождается

В ноябре 2003 года Комитет по правительственной реформе Конгресса США опубликовал большой и очень сердитый отчет[CR03] о проведенном здесь расследовании одного из эпизодов в деятельности ФБР, уходящего корнями в начало 1960-х годов. Этот документ, озаглавленный «Все секретное вырождается. Об использовании убийц в качестве информаторов Федерального бюро расследований», не только в подробностях раскрывает тщательно скрываемую практику вербовки органами правопорядка профессиональных бандитов-киллеров в качестве своих «помощников», но и остро критикует администрацию Буша за препятствование ходу парламентского расследования [GJ01].

В отчете Комитета показано, как из-за неразборчивости ФБР в выборе своих информаторов-киллеров происходит так, что другие люди проводят всю оставшуюся жизнь или преждевременно умирают в тюрьме за преступления, которых они не совершали. Кроме того, несколько человек были убиты лишь за то, что приходили в правительственные органы с информацией о преступлениях осведомителей ФБР. При этом правительственные служащие разлагались коррупцией настолько, что сами становились непосредственными соучастниками преступлений.

На протяжении всей работы парламентского следствия сотрудники комитета постоянно сталкивались с активным нежеланием министерства юстиции отчитываться о содеянном перед органом законодательной власти. Кроме того, расследование Комитета было искусственно задержано на многие месяцы из-за попыток президента Буша воспользоваться привилегией главы исполнительной власти и не допустить выдачи целого пакета ключевых в этом деле документов. В конечном счете конгрессмены все же получили те материалы, в которых нуждались, а попытки президента назвали «прискорбными и излишними». При этом, судя по комментариям, для некоторых законодателей так и осталось, похоже, невдомек, с какой это стати президент-республиканец столь отчаянно пытается оградить от огласки деяния администрации демократов почти 40-летней давности.

Вся эта история закручена вокруг противостояния двух наиболее влиятельных групп мафии города Бостона («итальянской» и «ирландской»), в разборках которых активное участие принимало и ФБР. Вскрытые нынешним расследованием документы свидетельствуют, что

Эдгар Гувер лично контролировал ход событий, приведших к фактической ликвидации в середине 1960-х гг. одной из бостонских мафиозных групп (клана Патриарка) и к закреплению на главных позициях местного преступного мира банды Winter Hill, некоторые члены и даже главари которой были тайными осведомителями ФБР. В результате этого сговора ФБР не только многие годы закрывало глаза на преступления «своей» мафии, но и занималось сокрытием улик о многочисленных убийствах ради того, чтобы выгородить киллеров-информаторов [JE02].

Подробное изложение фактов о сотрудничестве бостонской мафии и федеральной полиции в 1970-1980-е годы представлено в обстоятельной книге-расследовании [LN03] Дика Лера и Джерарда О'Нила «Черная месса: ирландская банда, ФБР и договор с дьяволом». Начало же череде всех этих грязных дел было положено в 1965 году, когда в результате сделки ФБР с бандитами четыре человека были упрятаны пожизненно в тюрьму за убийство авторитетного гангстера Эдварда «Тедди» Дигана, хотя имелись достоверные свидетельства о невиновности всех этих людей. Единственной причиной их «нейтрализации» стало то, что они, возможно, располагали кое-какой информацией о реальных убийцах. Двое из осужденных так и скончались за решеткой, двое других провели в тюрьме более 30 лет своей жизни по сути дела лишь из-за одного, заведомо ложного свидетельства субъекта по имени Джозеф «Скотина» Барбоза.

Барбоза в документах на имя Гувера представлен как «профессиональный наемный киллер, ответственный за множество убийств и признанный всеми правоохранительными органами Новой Англии как наиболее опасный из известных преступников». В суде Барбоза давал показания в защиту своего приятеля, Джеймса Винсента Флемми, который в действительности и убил Дигана. Кроме того, Флемми был осведомителем ФБР, где были в курсе о висящих на нем по меньшей мере 7 убийствах. С помощью этого киллера и еще двух головорезов, чуть позже ставших информаторами ФБР – Стивена «Стрелка» Флемми (старшего брата Джеймса) и Джеймса «Уитни» Балджера – ФБР фактически уничтожило мафиозный бостонский клан Патриарка. В результате этого контроль за рэкетом в Бостоне перешел к Джеймсу Балджеру и «Стрелку» Флемми.

После суда по делу об убийстве Дигана в отношении лжеца Джозефа Барбозы была запущена федеральная программа защиты свидетелей, его переправили в Калифорнию, где вскоре Барбоза совершил еще одно убийство. ФБР вновь пришло на выручку, непосредственно помогало защите, Барбоза получил небольшой срок, а о его досрочном освобождении ходатайствовал не кто-нибудь, а федеральный прокурор. Один из сотрудников ФБР, Пол Рико, вербовавший в качестве осведомителей киллеров Флемми и Барбозу, уйдя с работы в правоохранительных органах, стал главой службы безопасности фирмы World Jai Alai, тесно связанной с организованной преступностью. В последние годы, когда американское правосудие все же решило разобраться с бостонской историей, Пол Рико попал под следствие в деле об убийстве Роджера Уилера, главы World Jai Alai. Как установлено следствием парламентской комиссии, бандиты-информаторы, когда-то взятые под опеку Эдгаром Гувером, продолжали заниматься преступной деятельностью вплоть до 1990-х годов, совершив несколько десятков

убийств.

Завершив парламентское расследования и соответствующие слушания в Конгрессе, глава Комитета по правительственной реформе, республиканец Дэн Бертон внес на обсуждение Палаты представителей законопроект об удалении имени Дж. Эдгара Гувера со штаб-квартиры ФБР в Вашингтоне. Подводя итог вскрытым фактам, Бертон заявил, что деятельность легендарного директора ФБР – это форменное издевательство над законом: «Совершенно очевидно, что Эдгар Гувер злоупотреблял своим постом директора ФБР. Символика занимает важное место в Соединенных Штатах, и было бы ошибкой продолжать почитать человека, который часто манипулировал законом для достижения своих личных целей» [AU03].

Доверие и Свобода

В середине 1990-х годов одной из самых наглядных демонстраций того, насколько американское общество не доверяет собственной власти, стал полнейший крах инициативы с «депонированием криптографических ключей» (key escrow). Суть данной инициативы, родившейся в недрах спецслужб, сводилась к тому, что вместе с персональными компьютерами широкие слои населения получили свободный доступ к мощным средствам шифрования информации, а сильную криптографию государство издавна приравнивает к опасному военному снаряжению, распространение которого подлежит строгому контролю. А потому, решили спецслужбы, следует навязать обществу такую систему, при которой к каждому сильному шифру должен на этапе изготовления прилагаться еще один, специальный криптоключ, позволяющий компетентным органам вскрывать любую зашифрованную информацию, если возникнет такая потребность. Ну а чтобы эти специальные криптоключи находились у властей всегда под рукой, и была рождена идея об их централизованном хранении (депонировании) в единой базе данных.

Идея, что ни говори, была чрезвычайно заманчивая. Не рассчитали власти лишь одного – насколько сильно все это не понравится народу. Как только инициатива с депонированием была озвучена клинтоновской администрацией, в обществе поднялся буквально ураган протестов. Аргументы против экзотического новшества были выдвинуты самые разные, от технических до моральных, но лейтмотив у них был единый – любые властные структуры состоят из людей, которые имеют склонность злоупотреблять данной им властью. И весь предшествовавший опыт свидетельствует, что у граждан нет абсолютно никаких оснований доверять тайны своей личной жизни государству лишь на том основании, что так ему проще обеспечивать всеобщую безопасность [EF03].

Поскольку никакого доверия не получилось, всю программу депонирования ключей (с лежавшим в ее основе техническим решением под названием «клиппер-чип») пришлось властям свернуть. На какое-то время. А затем, в 2000-е годы примерно с той же идеей, но уже совсем под другим соусом, выступили крупнейшие компьютерные фирмы. Теперь обществу предложено довериться корпорациям.

Платформе партии – доверяем... Или все-таки нет?

Начиная с лета 2002 года регулярно приходят известия о все более отчетливой и конкретной материализации инициативы под завлекательным, на первый взгляд, названием Trusted Computing (TC). На русский доходчивее всего это можно перевести как «ДоверяйКо», от Доверяемый Компьютер. Суть данной инициативы в том, что несколько лет назад группа ведущих фирм-изготовителей компьютерной индустрии – Intel, IBM, AMD, HP, Compaq и Microsoft– объединилась в консорциум TCP A [Trusted Computing Platform Alliance, 1999, [LG02], чтобы «более широко внедрять доверие и безопасность в разнообразные компьютерные платформы и устройства – от ПК и серверов до карманных компьютеров и цифровых телефонов». С апреля 2003 года все затеянные работы по внедрению доверия ведутся под эгидой специально созданной ради этого «открытой промышленной группы» Trusted Computing Group (TCG, www.trustedcomputinggroup.org). По состоянию на конец того же года членами TCG являлись уже свыше 200 компаний самого разного профиля и масштаба.

Судя по названию и декларациям, цель, поставленная альянсом, звучит очень благородно – «создание архитектурной платформы для более безопасного компьютера». Вот только позиции, с которых в TCG определяют «безопасность», вызывают сильные возражения у очень многих независимых и авторитетных экспертов в области защиты информации. Потому что машины, создаваемые по спецификациям Trusted Computing, будут более «доверяемыми» с точки зрения индустрии развлекательного контента и компьютерных корпораций. А вот у самих владельцев новых компьютеров доверия к машинам станет значительно меньше. Потому что совершенно очевидно – в конечном счете спецификации «Доверяй-Ко» перемещают весь контроль за работой ПК от пользователя к тем, кто изготовил программы и создал файлы по лицензии TCG.

С лета 2002 года, когда публика впервые узнала о секретном прежде проекте Microsoft под названием Palladium (составная часть инициативы TCP A), в альянсе происходит непрерывная чехарда со сменой названий. Проект Palladium, однозначно вызвавший негативную реакцию общественности, вскоре сменил свое звучное имя на спотыкучее NGSCB (читается как «энскюб», а расшифровывается как Next-Generation Secure Computing Base, т.е. «безопасная вычислительная база следующего поколения»). Консорциум TCP A по каким-то, даже не разъясненным рядовым участникам, причинам стал называться TCG. В корпорации Intel новый курс предпочитают называть Safer Computing, т.е. «более безопасный компьютинг». Короче, поскольку за всем этим мельтешением продолжают оставаться те же самые центральные игроки с прежними целями, у многих создается подозрение, что это своего рода дымовая завеса. Или как бы маневры, призванные отвлечь внимание публики от того, что же в действительности реализуют схемы «ДоверяйКо» [DF03][RJ03].

Что и как делает Trusted Computing? Если воспользоваться разъяснениями Росса Андерсона, уже знакомого нам профессора

Кембриджа и весьма известного в мире компьютерной безопасности эксперта, то «ДоверяйКо» обеспечивает такую компьютерную платформу, в условиях которой вы уже не можете вмешиваться в работу программных приложений, а приложения эти, в свою очередь, способны в защищенном режиме самостоятельно связываться со своими авторами или друг с другом. Исходный мотив для разработки такой архитектуры был задан требованиями Digital Rights Management (DRM) – «управления цифровыми правами» на контент. Фирмы звукозаписи и кинокомпании желают продавать свои диски и файлы так, чтобы их было нельзя бесконтрольно в компьютере скопировать, перекодировать или выложить в Интернет. Одновременно «ДоверяйКо» предоставляет возможности очень сильно затруднить работу нелицензированного ПО, т.е. в потенциале является серьезным инструментом для борьбы с пиратскими программами.

Достигаются все эти цели сочетанием специальных аппаратных и программных средств, следящих и докладывающих «компетентным инстанциям» о том, что делается в компьютере. Важная роль здесь отводится запаиваемой в системную плату микросхеме Trusted Platform Module, кратко TPM. Этот модуль быстро получил в народе звучное имя «фриц-чип» в честь спонсируемого компанией Disney американского сенатора Фрица Холлингза, пытавшегося добиться обязательного встраивания таких микросхем в каждый выпускаемый компьютер. В целом же спецификациями TCG в версии 1.1 (2003 г.) предусмотрено пять взаимно увязанных элементов: (а) фриц-чип, (б) «экранирование памяти» внутри процессора, (в) программное ядро безопасности внутри операционной системы (в Microsoft это именуют Nexus), (г) ядро безопасности в каждом ТС-совместимом приложении (в терминологии Microsoft – NCA), (д) плюс поддерживающая все это дело специальная онлайновая инфраструктура из серверов безопасности, с помощью которых фирмы-изготовители намерены управлять правильной и согласованной работой всех компонент [LG02].

В своем идеальном (намеченном изначально) варианте ТС подразумевает, что компоненты компьютера должны при установке автоматически проходить «проверку благонадежности» с применением криптографических протоколов, а индивидуальные параметры «железа» (плат, накопителей) и ПО (ОС, драйверы и прочее) в хешированном, т.е. сжатом и шифрованном виде прописаны в модуле TPM. Вся информация хранится и пересылается между доверяемыми компонентами в зашифрованном виде. Фриц-чип надзирает за процессом загрузки, дабы ПК после включения вышел в предсказуемую рабочую точку, когда уже известны и одобрены все компоненты «железа» и ПО. Если машина загружается в «правильное состояние», то фриц предоставляет операционной системе хранимые в нем криптографические ключи для расшифровки нужных в работе приложений и их данных. Ядро безопасности в операционной системе (Nexus) обеспечивает взаимодействие между фриц-чипом и компонентами безопасности (NCA) в приложениях. Кроме того, Nexus работает совместно с «экранированной памятью» в новых процессорах, чтобы не позволить одним ТС-приложениям работать с данными (считывание/запись) других ТС-приложений. Эта новая особенность процессоров у разных

изготовителей именуется по-разному: у Intel – технология LaGrande, а у ARM, к примеру, TrustZone.

Если же загрузка вывела ПК в «неправильное состояние», когда новый хеш не совпал с хранящимся в TPM, то модуль не выдаст криптоключи, а значит на машине (в лучшем случае) можно будет запускать лишь «левые» приложения и данные, не имеющие сертификата на TC-совместимость. Поскольку на будущее мыслится, что весь достойный контент и все достойные его обрабатывать программы непременно станут TC-совместимыми, то судьба конечного пользователя легко предсказуема – делать лишь то, что дозволят компании-правообладатели.

Понятно, что даже в столь кратком изложении описанная архитектура не сулит владельцу будущего компьютера ничего хорошего. И сегодня склонить людей к покупке оборудования и программ, реализующих эту технологию – вещь, казалось бы, совершенно нереальная. Но это смотря как ее подать.

В военном деле, как известно, существуют две базовые модели боевых действий – в наступлении и в обороне. Но мудрые китайцы когда-то изобрели еще одну, весьма эффективную модель «войны без боя» – просачивание. Суть ее в том, чтобы многочисленными, но внешне неприметными и разрозненными группками проникнуть за линию фронта, распределиться в тылу противника, а уже затем согласованно ударить изнутри по ключевым точкам. Пусть на это потребуется не один год, однако эффективность решающего удара может быть очень высокой, поскольку «просочившихся» почти никто в лагере противника не воспринимает как реальную угрозу.

Совершенно очевидно, что индустрия развлекательного контента рассматривает пользователей ПК в качестве своих «противников» и ищет разные – оборонительные, наступательные, какие угодно – средства для борьбы с ними. Столь же очевидно, что флагманы компьютерной промышленности, долгое время пытавшиеся сохранять в этой борьбе нейтралитет ради интересов собственных прибылей, уже сделали свой выбор. Вполне ясны и мотивы, подтолкнувшие их к «закручиванию гаек». Упор на развлекательный контент ныне видится главным залогом успешных продаж ПК, а компьютер может стать «центром домашних развлечений» в домах будущего лишь при том условии, что будет устраивать индустрию контента. В противном случае весь куш достанется фирмам бытовой электроники, предлагающим свою версию «центра» на основе продвинутых ресиверов, игровых приставок или чего-то еще, отличного от «не в меру гибкого» компьютера.

В результате рождается альянс Trusted Computing и соответствующие спецификации на новую архитектуру. А параллельно идут аккуратные прощупывания потребителя на предмет того, в каком виде он готов все это заглотить («массовый заглот» необходим непременно – по грубым оценкам, для экономически оправданного разворачивания всей нужной инфраструктуры TC требуется набрать «критическую массу» примерно в 100 миллионов устройств – ПК, карманных компьютеров, сотовых телефонов). За первые годы «просачивания» Trusted Computing уже отмечены и анекдотические казусы, и примеры элегантного маневрирования.

Главный анекдот – это то, как в Microsoft из года в год упорно настаивают, что разработка Palladium/NGSCB абсолютно никакого отношения не имела к борьбе с нелегальным копированием Windows. Когда на одной из конференций компетентный представитель Microsoft в очередной раз озвучил эту мысль, заявив даже, что корпорации вообще «неведомо, каким образом эту технологию можно применять против пиратского копирования», один из присутствовавших хакеров [Хакер в исходном, не криминальном смысле, т.е. весьма сведущий в своем компьютерном деле человек.] – Лаки Грин, в миру более известный как Марк Брисено, возмутился настолько, что решил пойти на крайние меры. Он подал на оформление сразу две патентные заявки, описывающие методы применения NGSCB для борьбы с копированием программ. Оформление патентов – процедура долгая, но если дело выгорит, то Microsoft придется либо официально доказывать, что у них имеется в этой области приоритет (а значит, они откровенно лгали), либо просить у Лаки Грина лицензию (заведомо зная, что Грин ее ни за что не даст). Либо, наконец, продемонстрировать миру свою кристальную чистоту и никогда даже не пытаться связывать NGSCB с защитой ПО от копирования [PR02].

В корпорации Intel маневрирование ведется более тонко. Технология LaGrande впервые была представлена публике осенью 2002 года, в рамках форума разработчиков ПЖ Поначалу было объявлено, что LaGrande будет встраиваться во все грядущие процессоры фирмы. Однако публика, несмотря на посулы большей безопасности, среагировала на эту новость скорее негативно, чем положительно. В 1999 году у Intel уже был крайне неприятный опыт, когда корпорация начала добавлять в процессоры Pentium III уникальный серийный номер, позволявший индивидуально отслеживать с Сети каждую машину. Последовавшая буря протестов, призывы к бойкоту и общий ущерб репутации явно произвели на корпорацию впечатление. Поэтому теперь планы относительно LaGrande скорректированы с учетом начальной реакции публики. Осенью 2003 года объявлено, что новая технология не будет внедряться тотально и ориентирована в основном на корпоративный, а не на потребительский рынок. Обещано, что пользователь сам будет выбирать, нужен ему чип с LaGrande или же без этой системы [MR03].

Но как бы ни проходили все эти маневры, суть их остается одна. Спецификации Trusted Computing постепенно усовершенствуются и реализуются в рыночных товарах, а в продажу понемногу выводятся настольные системы (Hewlett-Packard), ноутбуки (IBM) и материнские платы (Intel) с запаянным в схему фриц-чипом TPM. Пока что изготовители заверяют, что эта микросхема не имеет никакого отношения к управлению цифровыми правами на контент, а просто служит надежным «сейфом» для хранения криптографических ключей пользователя. Но вполне очевидно, что это – технология «двойного назначения», как принято говорить в военно-промышленном комплексе.

То, что принципы Trusted Computing откровенно противоречат интересам общества, наиболее отчетливо видно по реакции практически всех экспертов в сфере инфобезопасности, не связанных с корпорациями. Ни один из них, насколько можно судить по прессе, не выступил с одобрением ТС, а вот публичных выступлений с острой критикой – сколько

угодно. Так, весной 2003 года на крупнейшем в мире отраслевом форуме – RSA Conference – по поводу Palladium специально выступали «отцы» криптографии с открытым ключом Уитфилд Диффи и Рональд Райвест. Как подчеркнул Диффи, интеграция схем безопасности в компьютерную архитектуру – вещь, безусловно, неизбежная и нужная. Однако, избранный подход к решению этой задачи в корне порочен, поскольку пытается увести из рук пользователя контроль за его собственной системой. Детали технологии, просочившиеся в СМИ, свидетельствуют, что главные цели новых инициатив – не столько безопасность, сколько рыночное доминирование ведущих корпораций, изоляция ключевых элементов компьютера и фактически лишение прав пользователя на владение собственной машиной. Но, подчеркнул Диффи, именно хозяину должны принадлежать ключи от собственного компьютера, а не государству или крупным корпорациям. Рональд Райвест вполне согласился с мнением коллеги, призвав к широким общественным дебатам относительно действий индустрии. Потому что именно общество (а не крупнейшие корпорации) должно определять, какого уровня поддержку своей защиты оно желает [MEO3].

Достаточно очевидно, что чем больше человек понимает суть «ДоверяйКо», тем определеннее его несогласие с таким «доверием». На сегодняшний день главным, пожалуй, форпостом противников Trusted Computing можно считать специально созданную Россом Андерсоном веб-страницу «Часто задаваемые вопросы о Trusted Computing» (www.cl.cam.ac.uk/~rjal4/tcpa-faq.html). Английский текст страницы переведен энтузиастами-добровольцами на немецкий, испанский, французский, иврит, китайский – короче говоря, на полтора (примерно) десятка распространенных языков планеты. Остается лишь надеяться, что истинная суть ТС все же дойдет до разума покупателей, беспечно формирующих ныне для коварной технологии набор критической массы [RA03].

Сеть свободы

Примерно с середины 2000 года в интернет-мире наблюдался взрывной рост интереса к пиринговым (от peer-to-peer) сетевым технологиям. Главным образом, это было вызвано феноменальным успехом файлообменных сетей вроде Napster и Gnutella, предоставивших людям крайне эффективный инструмент для поисков и обмена музыкой в формате MP3. Но свободный доступ к музыке – это лишь одна, возможно, самая яркая сторона намного более значительной области – организации свободного доступа к информации вообще. Иначе говоря, специалистам стали крайне интересны специфические способы построения полезных информационных систем, состоящих из большого количества равноправных машин, соединяемых друг с другом не постоянно, а лишь время от времени, с помощью виртуальных инфраструктур, созданных и настроенных под какое-то конкретное приложение.

Случилось так (вероятно, неслучайно), что одну из основополагающих работ для этой области исследований – статью [RA96] под названием «Сервис The Eternity» – представил на Pragocrypt 96, международной

криптографический конференции в столице Чехии, все тот же кембриджский профессор Росс Андерсон. Музыкальным сетевым бумом в 1996 году еще и не пахло, толчком же к исследованиям Андерсона послужили совсем другие события – весьма неприятные прецеденты подавления одной из фундаментальных демократических свобод – свободы слова – в Интернете. В одном из случаев крайне агрессивная церковь сайентологии через суд добилась закрытия в Финляндии весьма популярного сервиса-пересыльщика, обеспечивавшего анонимность авторам электронной почты (через этот сервис прошли публикации, компрометировавшие хаббардистов). Второй же случай непосредственно касался уже самого Андерсона, поскольку ему угрожали судом адвокаты банков, всячески старавшихся подавить распространение через Сеть информации об уязвимостях машин-банкоматов (статья на эту тему принесла Андерсону известность в начале 1990-х годов) [WG95].

Произошедшее весьма наглядно продемонстрировало ученому серьезность проблемы – то, что электронные публикации очень несложно подавить, если это зачем-либо понадобится богатым и безжалостным силам. Такие публикации обычно размещены всего лишь на нескольких серверах, владельцев которых можно либо засудить, либо силой принудить к подчинению. По ощущениям Андерсона, ситуация выглядела столь же неуютно, как, скажем, с рукописными книгами в средневековье. Тогда новые времена смогли начаться лишь после появления печатного станка, позволившего распространять идеи вольнодумцев столь широко, что запретить их уже стало невозможно. Поэтому сервис The Eternity зародился как средство размещать электронные документы настолько вне досягаемости цепких рук цензоров, насколько возможно.

Насколько эта работа оказалась актуальна для защиты свободы слова, свидетельствует хотя бы такой совсем свежий факт. Британское правосудие недавно официально постановило, что по решению суда отныне можно вносить изменения в содержание онлайновых архивов газет, если публикация сочтена клеветой. Иными словами, богатейший опыт тоталитарного СССР – страны с постоянно изменявшимся прошлым – оказывается очень привлекательным для нынешних западных демократий. Но намного более мощно стремление властей к цензуре и подавлению свободного распространения информации проявилось в борьбе с бесконтрольным распространением в Сети развлекательного контента – в первую очередь, музыки и фильмов. Потому что, дескать, это анархическое безобразие посягает на самое святое из достижений цивилизованного общества – на священный копирайт.

Обсуждение нетривиальной проблемы защиты прав на интеллектуальную собственность в эпоху цифрового копирования информации уведет данную книгу очень далеко в сторону. Поэтому здесь – просто для обозначения позиции – ограничимся лишь краткой и емкой формулировкой, к которой обычно прибегают все люди, признающие неотъемлемые права каждого человека на доступ к знаниям: «ИНФОРМАЦИЯ ДОЛЖНА БЫТЬ СВОБОДНОЙ».

Жесткие и агрессивные действия индустрии развлечений по подавлению наиболее популярной файлообменной сети Napster многому научили разработчиков пиринговых технологий, занимающихся созданием

сетей, недоступных для цензуры и произвола властей. На основе идей и криптографических протоколов Eternity Service созданы несколько систем, надежно, распределенно и в защищенном виде хранящих документы на множестве компьютеров сети. Чаще других среди систем такого рода упоминают Publius, Mojonation и Freenet [csl.cs.nyu.edu/~waldman/publius/, www.mojonation.net, freenetproject.org]. О последней из них, как о наиболее, вероятно, знаменитой, имеет смысл рассказать подробнее.

Freenet, как представляют систему ее создатели [WF03], – это свободное (с открытым исходным кодом) программное обеспечение, которое позволяет публиковать и получать информацию в Интернете, совершенно не опасаясь цензуры. Для достижения этой свободы сеть Freenet полностью децентрализована, т.е. не имеет никаких главных узлов, а все участники, публикующие и потребляющие информацию, остаются полностью анонимны. Условие анонимности членов сети заложено в качестве фундаментальной основы системы, потому что без права на анонимность не может быть подлинной свободы слова. Аналогично – без децентрализации сеть всегда будет оставаться уязвимой в отношении самого разного рода атак.

«Отцом» всего проекта по праву считается молодой программист Иэн Кларк, уроженец Дублина и выпускник Эдинбургского университета, где Freenet и родилась в конце 1990-х годов как основная часть выпускной дипломной работы. После публикации проекта в Интернете идея получила грандиозную популярность, к работам начали активно присоединяться другие исследователи-программисты, а их базовая статья «Freenet: распределенная система для анонимного хранения и получения информации» стала наиболее цитируемой публикацией 2000 года в области компьютерных наук (по данным службы Citeseer) [CSOO].

Все перемещения информации между узлами сети Freenet зашифрованы и организованы посредством «сквозной маршрутизации» через другие узлы, чтобы максимально затруднить любые попытки по выявлению того, кто именно запрашивает информацию и каково содержимое конкретного файла. Каждый из участников сети вносит свой вклад в инфраструктуру системы, предоставляя часть пропускной полосы своего компьютера для коммуникаций Freenet и часть пространства на жестком диске машины («хранилище данных») для размещения файлов. В отличие от других пиринговых файлообменных сетей, всякий участник Freenet сам не знает, что за информация лежит у него в «хранилище данных». Это содержимое постоянно меняется, потому что файлы сохраняются или уничтожаются в зависимости от того, насколько велик на них спрос. Так что наименее популярные отбраковываются, чтобы освободить место для более нового или более популярного контента. Одновременно конкретные файлы перемещаются ближе к тем пользователям, которые их чаще запрашивают. Все содержимое хранилищ тщательно зашифровано, в том числе и для того, чтобы оградить владельца компьютера от преследований тех сил, которые могут пожелать поставить наполнение Freenet под свой контроль [JBOO].

Эта сеть может использоваться множеством разных способов и не ограничена только лишь функциями файлообмена, как другие пиринговые системы. Данная система действует скорее как особый Интернет внутри

всего Интернета. Например, Freenet можно использовать для создания веб-сайтов (именуемых здесь «свободные сайты»), для общения через доски объявлений, для распространения контента, наконец.

Никто точно не знает, сколько пользователей насчитывает сегодня сеть Freenet. В самых общих чертах о популярности проекта свидетельствует тот факт, что за время его существования программное обеспечение, требуемое для установки на машине-участнике сети, скачали более двух миллионов человек. Известно также, что ПО Freenet используется для распространения свободной от цензуры информации в тех странах и регионах, где имеется очень сильное давление на свободу слова со стороны государственных, религиозных и других официальных структур – в частности, в Китае и на Ближнем Востоке. В октябре 2003 года авторитетный и уважаемый журнал MIT Technology Review назвал Иэна Кларка в числе 100 главных молодых новаторов, оказавших своими работами и изобретениями наибольшее влияние на наш мир [ТЕОЗ].

Технологии умной толпы

Народная энциклопедия

В середине января 2004 г. своеобразный двойной юбилей отметила Wikipedia (www.wikipedia.org) – бесплатная онлайновая энциклопедия «обо всем на свете», главная особенность которой даже не в том, что она бесплатна, а в том, что собственную статью для этого издания может предложить любой желающий. Информационный фонд энциклопедии достиг круглой и весьма внушительной цифры в 200 тысяч (англоязычных) статей, а 15 января проект отметил всего лишь третью годовщину своего существования (в Интернете каждый год существования – как юбилей). За прошедшее время Wikipedia успела набрать столь большую популярность среди интернациональной аудитории, что параллельно была запущена многоязычная версия энциклопедии, суммарно насчитывающая также свыше 200 000 статей на разных языках планеты. Одновременно развивается еще один родственный проект Wiktionary (www.wiktionary.org) – бесплатный многоязычный словарь и тезаурус.

Стремительный рост энциклопедии – за 2001-й год было составлено 20 000 статей, за 2002-й добавлено 80 000, за 2003 еще свыше 90 тысяч (все цифры для англоязычного издания) – объясняется, безусловно, тем, что статьи могут добавлять и пополнять сами читатели, сведущие в том или ином предмете. Например, вы большой любитель чисел Фибоначчи, знаете о них уйму интереснейших вещей и хотели бы поделиться своими познаниями с окружающими. Энциклопедия Wikipedia – это и есть тот самый шанс, который дается всем желающим. Сюда можно просто зайти и начать писать, причем даже имени вашего настоящего никто спрашивать не будет. Важно лишь то, что вы имеете изложить. С интересом принимаются не только научные статьи, но и информативные тексты сугубо бытовой или практической направленности. К примеру, для людей, часто испытывающих проблемы с эксплуатацией компьютера, имеется раздел под названием «Синий экран смерти» (вещь, знакомая всякому

пользователю Windows), где может оставить свой след в истории всякий толковый (а иногда и бестолковый) специалист. Энциклопедию ежемесячно пополняют несколько тысяч статей самой разнообразной тематики, от магнитно-ядерного резонанса и комет до покера и сериала «Стартрек».

Самое удивительное в этом проекте то, что несмотря на свою полную открытость издание непрерывно прирастает по-настоящему содержательными статьями, не становясь ни жертвой вандализма, ни гигантским скоплением полнейшей чепухи. Главную тому причину видят в постоянном участии большого количества добровольцев-«википедистов» (как они сами себя называют), непрерывно участвующих в коррекции, дописывании и комментировании статей энциклопедии. Вокруг издания сформировалось своего рода всемирное товарищество, обеспечивающее постоянно пополняющийся качественный контент.

Весь этот творческий процесс совершенно недвусмысленно напоминает создание программного обеспечения с открытым исходным кодом. И сходство это, конечно же, неслучайно. Модель «Википедии» воспроизводит ключевые идеи небезызвестного Проекта GNU Ричарда Столлмена, инициировавшего когда-то создание открытой версии ОС UNIX. Сам Столлмен назвал очевидные успехи роста проекта Wikipedia «по-настоящему волнующей новостью», среди постоянных авторов издания фигурируют авторитетные ученые из американских университетов и со всего мира, а компьютерные разделы ведут несколько десятков широко известных в профессиональной среде программистов.

В соответствии с положениями Лицензии GNU об общедоступной документации, все содержимое «Википедии» выложено во всеобщее пользование, может свободно копироваться и дополняться. Огромная аудитория и большой штат компетентных добровольных помощников одновременно являются гарантом того, что в статьях присутствует лишь содержательный информативный материал, а все попытки вандализма, хулиганства или злонамеренного искажения информации мгновенно пресекаются. Этому способствует сама структура энциклопедии, поскольку добавляемые данные выделяются как «свежие изменения», за которыми следят наиболее пристально. Более того, изначально взятый курс на нейтральную подачу информации, принципиально декларированный организаторами проекта, обеспечивает уравновешивание конфликтующих точек зрения и совместную выработку пользователями общеприемлемого взгляда на каждый спорный вопрос. Как комментируют этот процесс отцы-основатели проекта, интернет-предприниматель Джимми Уэлс и философ Ларри Сэнгер, сами читатели «непрерывно редактируют работу друг друга, и кажется удивительным, что эта схема может работать – но она работает очень хорошо» [WP04][JH01].

Преследуя Буша

Трехдневный визит американского президента Джорджа Буша в Великобританию в ноябре 2003 г. оказался для этой страны во многих отношениях событием беспрецедентным. Никогда прежде иностранные гости даже самого высокого ранга не выдвигали в качестве условий своего

пребывания такие требования, как: дипломатический иммунитет для нескольких сотен вооруженных агентов личной охраны президента; закрытие линий лондонского метрополитена, проходящих под маршрутами гостя; применение иностранных вооруженных сил (вертолетов Black Hawk и истребителей ВВС США) для прикрытия визита с воздуха; а также право на использование сугубо военного автоматического оружия («мини-пушки») против толпы в случае возникновения беспорядков [МВОЗЪ].

К чести британского министерства внутренних дел, во всех этих требованиях американцам было отказано. В частности, было твердо заявлено, что для людей с оружием, в случае открытия стрельбы, не может быть никакого иммунитета, и все виновные лица будут нести ответственность перед британским судом. Чтобы хоть как-то подсластить пилюли жестких отказов своему главному союзнику, английские власти все же пошли на ряд других существенных уступок для ограждения высокого гостя от толп протестующих. В частности, силами полиции была обеспечена значительная «стерильная зона» вокруг президента, а по маршрутам перемещений кавалькады в центральном Лондоне перекрывалось дорожное движение с выставлением специальных кордонов безопасности для удерживания публики на расстоянии. Одновременно «по оперативным причинам» были отключены веб-камеры, постоянно транслирующие в Интернет жизнь центральных районов британской столицы.

Неизвестно, какова была роль последнего обстоятельства, но современные коммуникационные технологии и политически активная интернет-общественность сыграли небывалую прежде роль в организации акций протеста в Лондоне против Буша и политики его госадминистрации. Для координации действий протестующих двое активистов организовали специальный веб-сайт www.Interwebnet.org, где в реальном масштабе времени отражалась информация обо всех замеченных перемещениях кортежа Буша по Лондону. Сайт получил название Chasing Bush – «Преследуя Буша» – и поставил своей целью фиксировать сигналы с мобильных GPRS– и камер-телефонов о текущем маршруте и остановках, чтобы с помощью случайных свидетелей быстро привлекать в это место находящихся поблизости активистов, которые могли бы «подать голос» и своим присутствием помешать возможным постановочным съемкам «ликующих горожан». Идея оказалась на редкость эффективной, и в первый же день запуска веб-страницы было зарегистрировано свыше 50 000 заходов.

George W. Bush thinks he can hide from an angry public. He's wrong.

IF YOU SEE GEORGE W. BUSH, EMAIL OR TEXT THE TIME AND LOCATION TO:

bush @ interwebnet . org

Постер общественной кампании «Преследуя Буша»

На примере этой деятельности бесцельное, по сути дела, прежде движение «мобстеров» (любителей спонтанных сборищ, организованных через Сеть) получило ныне вполне осмысленное содержание. Кто-то назвал это «вторым, умным mob-поколением». Возможно, именно благодаря грамотной координации действий, протестующим удалось собрать заметную, в несколько сотен человек толпу с плакатами против войны в Ираке даже в крошечном тихом городке Сэджфилд, насчитывающем всего 5 тысяч жителей. Это родина премьер-министра Тони Блэра, куда Буша повезли отдохнуть от многотысячных толп демонстрантов в Лондоне. Но вместо десятка специально выставленных радостных встречающих, президент вновь увидел большую толпу сердитых англичан. Кульминацией же акций протеста стал гигантский митинг на Трафальгарской площади Лондона, сопровождавшийся низвержением специально принесенной статуи американского президента. Для тех, кто не смог лично поприсутствовать на этом мероприятии, в Сети был организован «виртуальный марш протеста» из телефонных звонков, факсов и электронной почты, заполонивших все общедоступные коммуникационные линии посольства США в Великобритании [BN03].

Искусство быть честным

«Все искусство государственного управления сводится лишь к одному искусству – быть честным», – говорил когда-то автор проекта Декларации независимости США и третий президент этой страны Томас Джефферсон. Слова, что ни говори, очень красивые, и нет ничего удивительного в том, что одним из главнейших национальных достояний США, да и вообще всей человеческой цивилизации, принято считать принципы народовластия и базовых гражданских свобод, заложенные когда-то Джефферсоном и его соратниками в основу американского государства. Поразительно иное: как на этом благородном фундаменте сумел вырасти в корне иной образ типичного современного политика – лживого, беспринципного, лицемерного и корыстолюбивого. Впрочем, отцы-основатели США здесь скорее всего не причем, поскольку «политика как грязное дело» – явление интернациональное и распространенное повсеместно. Но зато именно в

Америке есть еще люди, не только хорошо помнящие, но и пытающиеся возродить благородные заветы предков.

В пятницу 4 июля 2003, явно в честь главного праздника страны, Дня независимости США, два сотрудника исследовательского центра Media Lab Массачусетского технологического института представили согражданам свой подарок – веб-сайт opengov.media.mit.edu или «Информационная осведомленность о правительстве», кратко GIA, от Government Information Awareness. Эта инициатива стала своеобразной реакцией той части американского общества, которую крайне встревожили перспективы скорого разворачивания мощной федеральной системы TIA для массовой слежки за гражданами США и иностранцами. Разработанная в Media Lab система GIA позиционирована как «симметричный ответ на TIA».

В качестве же главной задачи, поставленной перед проектом, его авторы называют создание единого, всеобъемлющего и простого в использовании хранилища информации о деятельности властей – конкретных людей, ведомств, организаций и корпораций, имеющих связи с правительством США. Эта база данных, для начала засеянная информацией о более чем 3000 государственных деятелей, накапливает и сопоставляет сведения о правительственных программах, планах и политиках, почерпнутые из множества общедоступных онлайновых источников. Кроме того, один из основополагающих принципов функционирования GIA – это предоставление возможности самим гражданам добавлять сюда содержательную информацию по всем вопросам, связанным с деятельностью властей, обеспечив при этом право на анонимность. Одновременно и всем деятелям правительства предоставлена равная возможность принимать участие в данном процессе.

Чрезвычайно интересен контекст происходящего, поскольку в США, как и в большинстве развитых (предположительно, демократических) стран, уже достаточно давно наблюдается растущий разрыв между возможностями граждан по надзору за деятельностью своего правительства и возможностями государства по слежке за гражданами. Обычные люди имеют сегодня крайне ограниченный доступ к важным правительственным документам, слабо представляя себе, кто именно принимает ключевые решения и кто конкретно влияет на их принятие. При этом доступная гражданам информация зачастую оказывается весьма невнятной и сложной для осмысления. С другой же стороны одновременно происходит очень быстрое нарастание устремлений и средств государства по надзору за личной жизнью и деятельностью своих граждан.

У этого процесса нет четких национальных границ или отчетливого начала по времени, однако особо заметно данные тенденции стали проявляться в США после событий 11 сентября 2001 года. В качестве нагляднейшей иллюстрации происходящего послужила объявленная в 2002 году программа федерального правительства TIA или «Тотальная информационная осведомленность» (Total Information Awareness, подробнее см. Главу 1). Осознавая причины тревоги людей, правительственные чиновники многократно заверяли общественность, что единственная цель TIA – выявление потенциальных террористов путем сравнения данных из множества государственных и частных инфохранилищ. Будучи сведенными вместе, эти данные могут указать на

характерные поведенческие структуры-паттерны, свидетельствующие о террористических замыслах и деяниях. Однако, многие правозащитники усматривают в TIA и ее модификациях чрезвычайно навязчивую и мощную попытку мониторинга государства за частной жизнью граждан – начиная от всех расчетов по кредитной карточке или планирования поездок до посещения врачей и обращения за ветеринарной помощью.

В условиях, когда власти расширяют внутренний надзор и наращивают взаимодействие с частными институтами для доступа к персональным данным о населении, начинает расти и потенциал возможных злоупотреблений информацией. А значит, чрезвычайно важным становится обеспечение симметрии, т.е. адекватный рост подотчетности правительственных структур перед своими гражданами. Совершенно очевидно, что если базовый принцип демократии – это «правительство, созданное народом, из народа и для народа», то важнейшим моментом является обеспечение общества инструментами, обеспечивающими надзор граждан за правительством. Причем затраты на это должны быть по крайней мере не меньшие, чем для инструментов, помогающих правительству следить за личной жизнью граждан.

Вот от этих, собственно, принципов и оттолкнулись в своей работе сотрудники MIT Media Lab, создавшие GIA, – 26-летний аспирант МТИ Райан Маккинли, разработавший основу системы в рамках своей магистерской диссертации, и его научный руководитель Кристофер Чиксентмихайи, доцент группы Computing Culture в MIT Media Lab. Подытоживая суть затеянной работы, Райан Маккинли говорит о ней, как о своего рода «гражданском разведывательном управлении», симметричном ответе на ФБР и ЦРУ, предоставляющем народу инструменты и техсредства, аналогичные тем, что имеются у властей: «Наша цель – разработать технологию, которая наделит граждан возможностями создания собственной разведслужбы, накапливающей, сортирующей и анализирующей информацию, собираемую народом о своем правительстве».

Итак, проект GIA – это комплекс программных средств, образующих для граждан некий инструментальный каркас всеобъемлющей базы данных о деятельности властей. Главный же «изюм» тут в том, что система построена на основе тех же самых идей, что и Total Information Awareness. Однако цель GIA прямо противоположна – позволить всякому рядовому гражданину проверить любое лицо в правительстве. Точно так же здесь имеется возможность просмотреть накопленные из разных источников данные, проследить последовательность событий, отыскать в информации скрытые специфические структуры, выстроить «профили риска». Информация об источниках финансирования парламентариев и политических кампаний, корпоративные, студенческие и религиозные связи – все данные подобного рода извлекаются из базы легко и естественно. Короче говоря, имеется возможность получить всю доступную о политике, чиновнике или влиятельном бизнесмене информацию для мотивации последующих действий.

Внешне GIA выглядит как стандартный веб-сайт, однако в действительности это комплекс весьма продвинутых инфотехнологий, в рамках масштабируемой базы данных активно перерабатывающих

информацию, принимающих новые записи от самых разных источников и рассылающих уведомления о происходящих событиях. Центральным моментом в GIA является расширяемая модель данных – здесь все представляет собой либо блок информации, либо ссылку-взаимосвязь. Такая модель позволяет системе расти в любом направлении, вмещая в себя всякие, даже невообразимые на этапе создания базы новые ведомства, должности и исходящие от них потенциальные угрозы обществу.

Создатели GIA с энтузиазмом приглашают всех желающих принять участие в проекте – «программистов, политических активистов всех направленностей, адвокатов и кого угодно еще, кто заинтересован в развитии проекта». Основа подхода – предоставить гражданам среду и инструментарий, с помощью которых они сами будут решать, что является заслуживающей доверия информацией, а что нет. Разработчики уверены, что подчеркнуто аполитичный подход к наполнению базы лишь увеличивает степень осведомленности публики о чиновниках своего правительства и о том, чем они занимаются.

Технология наполнения базы GIA отчасти схожа с принципами работы популярных в Интернете поисковых машин вроде Google. Программы-роботы ползают по веб-сайтам, содержащим значительное количество информации о политиках. Основное внимание уделяется независимым политическим сайтам, вроде популярных в США «Раскрытые секреты» (www.opensecrets.org, где, в частности, в соответствии с девизом Follow the Money отслеживаются источники финансирования политиков) или «Голосуй с умом» (www.vote-smart.org, где систематически накапливается «политически несмещенная» информация о кандидатах и ныне действующих народных избранниках).

Кроме того, в GIA поступает и всякая содержательная информация с сайтов, ведущихся правительственными ведомствами. Еще один важный элемент системы – непрерывное сканирование кабельной ТВ-сети C-Span, где на постоянной основе освещается деятельность всех ветвей федеральной власти. Как только на экране появляется очередной политик, программа считывает в поясняющей надписи его имя и привязывает к нему ссылку на накопленное в базе досье. Благодаря чему посетитель сайта, кликнувший в окошке с кадром из текущей ТВ-трансляции, еще до окончания речи может получить на выступающего полный «профиль» (если таковой имеется, конечно), включая и данные о том, кто финансировал кампанию по его/ее избранию.

Но помимо информации, накопленной и изначально «засеянной» разработчиками из общедоступных источников, у GIA есть очень важная особенность, аналогичная, так сказать, агентурному получению информации спецслужб. Начиная с первого дня сайт предлагает публике вносить имеющиеся у нее сведения о представителях власти. Так, чтобы эта информация стала доступна всякому, заходящему на сайт. По мнению разработчика Райана Маккинли, компьютеры сами по себе не способны отслеживать деятельность правительства. Хотя они могут накапливать уже существующие данные, множество ценной информации не хранится в существующих базах данных, находясь как бы в «коллективном сознании» американских граждан. Так что GIA – это путь к объединению

коллективного знания и превращения его в общедоступный ресурс.

Данный подход к формированию интернет-публикаций, вообще говоря, не нов. По своим принципам он сильно напоминает метод, известный в Сети как Wiki, когда содержимое сайта постоянно пополняется самими посетителями, добавляющими новую информацию. Самый знаменитый и успешный сайт на основе данного принципа – это рассмотренная ранее онлайновая энциклопедия Wikipedia (www.wikipedia.org), полностью составленная самими посетителями и содержащая ныне свыше 200 000 статей, с широким охватом разнообразных областей от физики до древнегреческой мифологии. Здесь нет никакого руководящего органа, контролирующего «правильность» статей, однако корректность данных эффективно поддерживается самими пользователями.

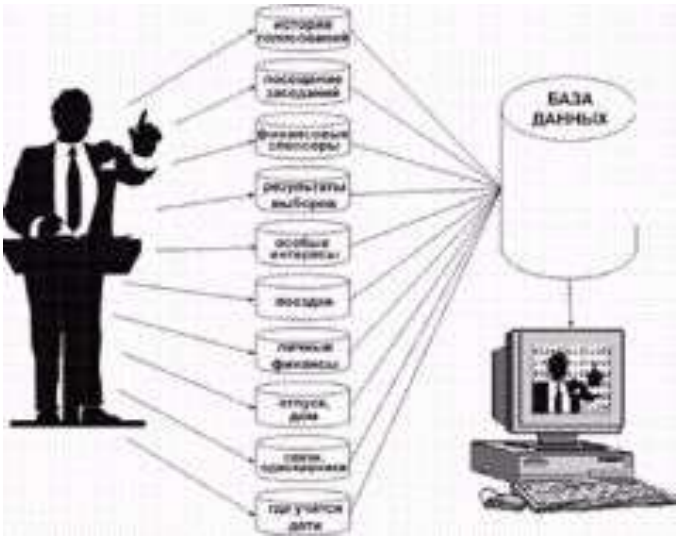
Посетители сайта GIA аналогично имеют возможность сами анонимно вносить имеющуюся у них информацию о государственных деятелях и правительственных программах. Для обеспечения аккуратности и точности данных, вносимых в базу, система автоматически связывается с соответствующими представителями властей и предлагает им подтвердить или опровергнуть появившуюся в базе информацию. Но, как и в аналогичных файлах-досье ФБР, сообщенная информация не уничтожается, если источник сомнителен или субъект отрицает ее достоверность. Опровержение просто добавляется в тот же файл. Подобно тому, как правительственные чиновники заявляют, что у честных граждан совершенно нет причин бояться TIA, создатели GIA с глумливой ухмылкой заверяют, что и правительственным чиновникам с чистой совестью совершенно не стоит опасаться их системы, построенной по тому же принципу.

Естественно, при таком механизме формирования базы данных имеется возможность помещения лживой, преднамеренно дискредитирующей людей информации (в любую спецслужбу поступают ложные доносы). Однако в системе предусмотрены достаточно гибкие механизмы, дающие возможность перепроверять надежность и достоверность источника. Так же как и в обычной жизни, где никто, пребывая в здравом уме, не верит болтовне первого встречного, в базе GIA людям дается возможность просмотреть и оценить достоверность прошлых вкладов анонимного информатора, привязанных к его псевдониму.

Вполне очевидно, что вся эта затея никак не может понравиться правительственным чиновникам, которые непременно приложат усилия для закрытия проекта, прикрывшись стандартными доводами «национальной безопасности и секретности». Однако, если вспомнить, что суть власти при демократии – служить народу, то у граждан как «работодателей» имеется гораздо больше прав на контроль за правительственными служащими, живущими за счет налогов, нежели у чиновников – прав на надзор за своими работодателями, живущими, отметим, за собственный счет.

Open Government InformationAwareness

Система «Информационная осведомленность о правительстве»



А потому гражданам любой страны, мнящей себя демократической, было бы очень полезно иметь информационную систему, похожую на GIA (тем более, что разработана она на основе принципов свободного программного обеспечения). Наверняка жителям всякого государства небезынтересно знать, в каких домах и дачах живут «слуги народа», в каких компаниях и куда ездят отдыхать их семьи, в каких школах и странах учатся их дети. Подобная информация время от времени проскакивает в средствах массовой информации, однако, собранная и систематизированная в одном месте, она гарантированно произведет намного больший эффект.

Конечно не случайность, что среди последних, самых главных вопросов на страничке GIA с «часто задаваемыми вопросами» стоит такой: «А законно ли все это?». И ответ на него очень хорош: «ЭТО должно быть законно».

В качестве же морального обоснования своей работы разработчики системы приводят слова четвертого президента США (и одного из соавторов американской конституции) Джеймса Мэдисона, который говорил так: «Знание всегда будет править невежеством, и люди, намеревающиеся править собою сами, должны вооружить себя силой, которую дает знание. Народное правительство без доступной народу информации либо средств ее обретения – это ничто, кроме пролога к фарсу или трагедии. А быть может – к тому и другому разом» [WK03][GA03].

Глава Последняя. Работа над ошибками

О смысле книги, собравшей под одной обложкой множество текстов довольно разного свойства, всякий читатель, естественно, сформирует собственное мнение. Но сам автор, он же и составитель, хотел бы заблаговременно, прежде чем последняя страница будет перевернута, предупредить о тех выводах, которые сделать легче всего и которые окажутся заведомо неверными.

Ошибка #1. Эта книга об Америке.

Подавляющее большинство материалов исследования, спору нет, действительно сделано на основе фактов и событий из жизни США. Но причины тому лежат исключительно в особенностях нынешнего этапа эволюции Интернета, благодаря ресурсам которого подготовлена книга. Просто именно «американские» источники почти всегда попадаются при поисках информации первыми. Но при желании и более серьезных затратах времени все примерно то же самое можно было бы написать на примере России, Франции, Великобритании или Китая. Там, как говорится, «труба пониже, да дым пожиже», однако технологии, специфика работы спецслужб и деятельность корпораций, по большому счету, всюду примерно одинаковы.

Ошибка #2. Эта книга об угрозах технологий.

Скромный финский парень Линус Торвальдс, волею судьбы вознесенный в статус культового героя хайтека и отца свободной ОС Linux, обронил как-то фразу: «Технологии не изменяют общество – это общество изменяет технологии». Сам он придумал этот пассаж или же вычитал в какой глубокомысленной книжке – в сущности, неважно. Важно то, что технологии сами по себе не являются ни плохими, ни хорошими. Они таковы, каково использующее и развивающее их общество. И абсолютно любая «угроза», усматриваемая в той или иной инфотехнологии, *с* равным успехом может стать ничуть не меньшим благом. Если общество этого захочет.

Ошибка #3. Эта книга о лживых властях, циничных спецслужбах и жадных корпорациях.

Любая большая организация и вообще всякая многочисленная общность людей – по некоторым прикидкам, начиная с количества примерно в тысячу человек – обретает своего рода «коллективное сознание» и начинает вести себя как живое существо. Лучше всего это видно на бюрократических организациях, при таком числе сотрудников превращающихся в самодостаточную единицу, которой, в принципе, уже не требуются для существования ни входящие сверху команды, ни исходящие вовне результаты работы. Большая организация вполне способна существовать сама ради себя, бодаться с себе подобными за ограниченные ресурсы, охранять занятую территорию и пытаться урвать что-то у соседей. Короче – бороться за выживание в соответствии с суровыми законами биологического отбора.

Самое неприятное, что у этого надбиологического существа все инстинкты – звериные, а разум – человеческий, хотя и коллективный. Но у всякого отдельно взятого индивидуума, как носителя человеческого сознания, есть то, что отличает его от всех остальных животных – совесть. А у всякой большой общности людей – будь то госадминистрация, спецслужба, церковь, корпорация или политическая партия – совести нет и сама по себе она никак не появляется. Так уж получилось.

И, к величайшему сожалению, практически всегда человек,

пытающийся занять видное место в иерархии всякой организации, начинает отождествлять себя, свое сознание, с коллективным разумом этой общности. Другими словами, вытеснять и подменять свою человеческую совесть животными интересами коллективного сознания, которые в данном случае носят всевозможные благородные названия типа: национальная безопасность, патриотизм, укрепление веры, партийная дисциплина или корпоративная этика. Еще более печально то, что с подменой совести на «общественные интересы» все наиболее мерзкие человеческие качества – алчность, жестокость, лживость, цинизм и т.д. – никуда не исчезают, а напротив, начинают цвести махровым цветом.

И это понятно, ведь главными факторами, заставляющими человека держаться «в рамках», являются собственная совесть и страх наказания. И когда совесть заглушена, а служение «высоким общественным интересам» порождает иллюзию безнаказанности, люди начинают творить черт знает что. Совесть у них, конечно, не совсем исчезла, а придавлена (люди все же остаются людьми, хоть и больными), так что они продолжают осознавать, сколь мерзкие делают вещи, а потому начинают возводить вокруг творимого плотную завесу тайн и стены секретности. И от этого ощущение безнаказанности возрастает еще больше.

Короче говоря, на самом деле эта книга – о людях. Но, по преимуществу, не о простых людях, а о мутантах. О больных людях с хронически угнетенной совестью, мыслящих себя выразителями «общественного сознания». Абсолютно бесстыжего сознания, надо подчеркнуть.

Может показаться, что новые инфотехнологии, обеспечивающие рост всепроникающего и постоянного надзора, делают общую ситуацию только хуже. Ведь личные свободы каждого отдельно взятого человека, имеющего совесть, лишь уменьшаются, а осведомленность бессовестных корпораций и властей все больше нарастает. Но в действительности здесь заложен гигантский потенциал к исцелению нашего душевнобольного общества. А именно – к наделению коллективного сознания, наконец, и своей «коллективной совестью».

Ведь именно такова роль общественного доступа к повсеместно распространяющимся средствам слежения за властью – информационным базам, веб-дневникам (блогам), мобильным средствам коммуникации, веб-камерам и так далее. Народ уже имеет под рукой практически все технические средства, способные убедить власть и корпорации, что они всегда, буквально ежеминутно находятся под пристальным и оценивающим взором небезразличного населения. Осталось только дождаться, когда и публика – носитель коллективной совести – это поймет. И начнет действовать не спонтанно, как сейчас, а осмысленно и целенаправленно.

Хочется надеяться, что данные идеи достаточно внятно проиллюстрированы настоящей книгой.

БИБЛИОГРАФИЯ

В силу непостоянной природы Интернета веб-ссылки на источники могут изменяться, а некоторые документы – вообще исчезать. По этой

причине на сайте http://gbop.nm.ru создан «архив», куда помещаются исчезающие с исходных веб-сайтов документы. Обо всех замеченных пропажах можно сообщить электронной почтой по адресу gbop@nm.ru. Практически все восстановимо.

AB02 «Out of bounds: Pinpointing workers by their mobile phones,» by Andrew Brown, CNN News, 14 Aug 2002, http://www.cnn.com/2002/WOIlLD/asiapcf/east/08/14/ mobile.pinpoint/index.html

AB03 «The Mathematics of Artificial Speech,» by Alan Burdick, DISCOVER Vol. 24 No. 01, January 2003, http://www.discover.com/issues/jan-03/departments/featmath

AC03 «Accenture Wins Two New U.S. Federal Contracts to Modernize, Integrate Military Business Operations. Defense Contracts Together Valued at $38.4 Million», Press Release, November 17, 2003, http://biz.yahoo. com/bw/031117/175602_l.html

AG03 «All the President's Votes?» by Andrew Gumbel, Independent, October 13, 2003, http://news.independent.co.uk/world/americas/story.jsp? story= 452972

AH02 «Researcher: Biometrics Unproven, Hard To Test,» By Ann Harrison, Security Focus, Aug 7,2002, http://www.securityfocusonline.com/news/ 566

AH03 «Hackers Claim New Fingerprint Biometric Attack,» by Ann Harrison, Security Focus, Aug 13, 2003, http://www.securityfocus.com/news/6717

AJ03 «VeriSign selling domain name business,» by Anick Jesdanun, Associated Press, October 16, 2003, http://www.usatoday.com/tech/techinvestor/techcorporatenews/ 2003-10–16-netsol-sold_x.htm

AK96 «Tamper Resistance – a Cautionary Note,» by Ross J. Anderson, Markus G. Kuhn, The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18-21,1996. http://www.cl.cam.ac.uk/~mgk25/tamper.pdf

AK97 «Low Cost Attacks on Tamper Resistant Devices,» by RJ. Anderson, M.G. Kuhn; In M. Lomas, et al. (eds.), Security Protocols, 5th International Workshop, LNCS 1361, Springer-Verlag, 1997

AM01 «The Conspirators: Secrets of an Iran Contra Insider» by Al Martin, National Liberty Press, 2001

AM02 «Coming Soon: Flying Fascism on Your Doorstep,» by Al Martin, www. almartin-raw.com, March 2002, http://www.federalobserver.com/archive.php?aid=1620

AM03 «Tracking tag firm exposes confidential data online,» by Andy McCue, CNET Networks, 8 July 2003, http://www.silicon.eom/news/500013/l/5037.html

AM97 Aspex Microsystems Limited home page, July 1997, http://gbop.nm.ru/am97.htm

AN03 «The Pentagon's best kept open secret. Low-profile firm heads government science efforts», AP news, July 21, 2003, http://www.cnn.com/2003/TECH/ptech/07/21/ secret.saic.ap/index.html

APOO «Bill Gates gets shipbuilder stake», AP news, 25 February 2000

AP03 «Satellite Tracking of Suspects Requires a Warrant, Court Rules» by AP news, September 12, 2003,

http://www.nytimes.com/2003/09/12/national/12GPS.html

AR02 «Secrets of the Tomb: Skull and Bones, the Ivy League, and the Hidden Paths of Power» by Alexandra Robbins, 2002, http://www.secretsofthetomb.com/

AR03 «Analysis of an Electronic Voting System,» by Tadayoshi Kohno, Adam Stubble-field, Aviel D. Rubin and Dan Wallach, Johns Hopkins University Rice, July 2003. http://avirubin.com/vote/

AS02 «Retrospective and Crystal Ball: Jim Wayman on biometrics», edited by Anne Saita, Information Security Magazine, November 2002, http://www.infosecuritymag.com/ 2002/nov/retrospective.shtml#ld

AS03 «Briton accused in leak of NSA memo charged,» by Ariel Sabar, The Baltimore Sun, November 18, 2003, http://www.sunspot.net/news/nationworld/bal-te.nsal8nov 18,0,5800698.story

AS86 «America's Secret Establishment: An Introduction To The Order Of Skull And Bones,» by Antony C. Sutton, 1986

AS93 «Official and Confidential: The Secret Life of J. Edgar Hoover,» by Anthony Summers, 1993

AS93 «Clinton Names Inman To Head Defense Department,» by Alexander M. Sullivan, USIA, December 16, 1993, http://www.fas.org/irp/news/1993/42639085-42643 185.htm

AT03 «Aspex Launches New Linedancer-HD,» Press Release, 12 September 2003, http:// www.aspextechnology.com/v2003/about/pressreleases/release_12_sep_2003. htm

AU03 «Off with his name! Boston corruption prompts drive to remove Hoover's name from FBI Headquarters,» by About Network, 2003, http://organizedcrime.about.com/ Iibrary/weekly/aa082602a.htm

BA03 «SAIC projects at a glance,» by Associated Press, July 21, 2003 http://www.boston. com/dailyglobe2/202/business/SAIC_projects_at_a_glance+.shtml

BBO3 «Revealed: US dirty tricks to win vote on Iraq war,» by Martin Bright, Ed Vulliamy and Peter Beaumont, The Observer, March 2, 2003, http://www.observer.co.uk/ iraq/story/0,12239,905936,00.html

BBO3 «Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communications», by Elad Barkan, Eli Biham, Nathan Keller, Advances in Cryptology: CRYPTO 2003,

Lecture Notes in Computer Science – 2729, Springer, http://cryptome.org/gsm-crack-bbk.pdf

BC02 «Last chance for E911 technology,» by Ben Charny, CNET News, May 29, 2002, http://news.com.com/2100-1033-928153.html

BD03 «DOD prepares for biometric-embedded smart card pilot,» by Dipka Bhambhani, GCN, Feb 20,2003, http://www.gcn.com/voll_nol/daily-updates/21180-l.html

BD97 «On the Importance of Checking Cryptographic Protocols for Faults», by D. Boneh, R.A. DeMillo, RJ. Lipton; In Advances in Cryptology – EUROCRYPT '97, LNCS 1233, Springer-Verlag, 1997. http://www.demillo.com/PDF/smart.pdf

BG99 IBM Blue Gene Project Overview, http://www.research.ibm.com/bluegene/

BHOO «Digital ads bend reality,» by Bruce Horovitz, USA TODAY, April 24, 2000, http:// www.beachbrowser.com/Archives/eVoid/April-2000/Digital-ads-bend-reality.htm

BH03 «Black Box Voting: Vote Tampering in the 21st Century» by Bev Harris, Elon House, 2003, http://www.blackboxvoting.com

BI03 «Blue Gene Is Cool for 2006,» by Salvatore Salamone, Bio-IT World, 15 July 2003, http://www.bio-itworld.com/news/071503_report2898.html

BK03 «Is It Good for the Jews?» by Bill Keller, New York Times, March 8, 2003, http://query.nytimes.com/gst/abstract.html?res=F20F16FE355BOC7B8CDDAA0894 DB404482

BM98 «Scientific Refutation of the Bible Codes,» by Brendan McKay and Friends, 1998 so on, http://cs.anu.edu.au/~bdm/dilugim/torah.html

BN03 «Mobile users told to 'chase Bush',» by BBC NEWS, 18 November, 2003, http:// news.bbc.co.uk/2Aow/technology/3280611.stm

BO02 «A hacker creates headaches for security-card company» by Bruce Orwall, The Wall Street Journal, Oct. 9, 2002, http://gbop.nm.ru/bo02.htm

BPOO «VeriSign Acquires Network Solutions,» by Bill Pietiucha, InternetNews.com, March 7,2000, http://dc.internet.com/news/print.php/316231

BP03 «Coming soon: biometric passports» by Associated Press, Aug. 23, 2003, http:// www.msnbc.com/news/956485.asp70si-

BR03 «No Surveillance Tech for Tampa» by Reuters, Aug. 21, 2003, http://www.wired. com/news/politics/0,1283,60140,00.html

BR99 «Interview: The LOpht Answers,» posted by Roblimo on December 31, 1999, http://slashdot.org/article.pl?sid=99/12/31/1030242

BSOO «Real Time Cryptanalysis of A5/1 on a PC,» by Alex Biryukov, Adi Shamir, David Wagner, Fast Software Encryption Workshop 2000, April 10-12, 2000, New York City, http://cryptome.or/a5.zip

BS02 «Fun with Fingerprint Readers» by Bruce Schneier, Crypto-Gram, May 15, 2002, http://www.schneier.com/crypto-gram-0205.html

BS03 «National Crime Information Center Database Accuracy» by Bruce Schneier, Crypto-Gram, April 15, 2003, http://www.schneier.com/crypto-gram-0304.htmltf7

BS97 «Differential Fault Analysis of Secret Key Cryptosystems,» by Eli Biham and Adi Shamir, Proceedings of Crypto'97, http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/1997/CS/CS0910.revised.ps

BW02 «Why Spielberg's Scared: 'Big Brother Is Watching Us Now' – And It Will Get Worse», by Buck Wolf, ABC NEWS, June 20, 2002, http://abcnews.go.com/ sections/entertainment/DailyNews/minorityreport020619.html

CA03 «Taiwan hands out 22 million ID cards» by CNETAsia, September 29, 2003, http://uk.news.yahoo.com/030929/152/e9ot6.html

CB02 «Connecticut moves to block car rental firm's GPS snooping» by CBC News Online, Jan 16 2002,

http://www.cbc.ca/cgi-bin/templates/view.cgi?/news/2001/07/03/Consumers/gps_speeding_010703

CBO3 «E– voting given go-ahead despite flaws,» by Celeste Biever, NewScientist.com news, 25 September 2003, http://www.newscientist.com/news/news.jsp?id= ns99994205

CC03 «CCTV no answer to street fights», BBC NEWS, 22 Dec 2003, http://news.bbc. co.uk/go/pr/fr/-/2/hi/uk_news/3339133.stm

CC98 «CCC klont D2 Kundenkarte (GSM Cloning: technischer Hintergrund)», Computer Chaos Club, http://www.ccc.de/gsm/

CD97 «J. Edgar Hoover, 33°, Grand Cross: Fidelity, Bravery, Integrity,» by Cartha D. «Deke» DeLoach (Chairman, Hoover Foundation), Scottish Rite Jurnal, May 1997, http://www.srmason-sj.org/library/hoover/j-e-hoover2.htm

CL02 «Murdoch security chief linked to TV piracy site,» by John Cassy, David Leigh and Kevin Maguire; The Guardian, March 14, 2002, http://media.guardian.co.uk/ news/story/0,7541,667040,00.html

CM02 «How codebreakers cracked the secrets of the smart card,» by John Cassy and Paul Murphy, The Guardian, March 13, 2002, http://media.guardian.co.uk/news/story/ 0,754 l,666457,00.html

CM03 «High-tech microscopes expose Americans' private lives,» by Don Campbell, USA TODAY, Nov 10, 2003, http://www.usatoday.com/news/opinion/editorials/2003-ll-10-campbell_x.htm

CM99 «OPERATEUR: Mobile Phones Tracking» by Christian Masson, 1999, http://www. seriot.ch/interception/mobile_tracegb.htm

CP02 «Smart Card Cracker at RSA tradeshow» by Bill Stewart, posting to cypherpunks, 21 Feb 2002, http://archives.abditum.com/cypherpunks/C-punks20020218/0101.html

CR03 «Everything Secret Degenerates: The FBI's Use of Murderers as Informants,» report of the US House Committee on Government Reform, 2003 Congressional Reports, November 20,2003, http://www.fas.org/irp/congress/2003_rpt/index.html#fbi

CSOO «Freenet: A Distributed Anonymous Information Storage and Retrieval System» by Ian Clarke, Oskar Sandberg, Brandon Wiley, Theodore W. Hong; in Lecture Notes in Computer Science, 2000, http://citeseer.nj.nec.com/clarkeOOfreenet.html

DA03 «Defense Contractors See Profit in Voting Machines» by David Allen, Eldorado Sun, October 03,2003, http://www.eldoradosun.com/articles/feat_allen.htm

DB01 «Satellite targets crop insurance abuse,» by David Bennett, Delta Farm Press, Jul 13, 2001, http://deltafarmpress.com/ar/farming_satellite_targets_crop/

DB03 «Concerns of Wiretapping Imperil a Planned Merger,» by Yochi J. Dreazen and Dennis K. Berman, Wall Street Jounral, July 17, 2003, http://cryptome.org/nsa-seatap.htm

DCOO Letter from Duncan Campbell to the Wall Street Journal, March 20, 2000

DC01 «COMINT Impact on International Trade,» by Duncan Campbell, Heise Online, 27.05.2001, http://www.heise.de/tp/deutsch/special/ech/7752/l.html

DC03 «Halliburton, Dick Cheney, and Wartime Spoils,» by Lee Diutman and Charlie Cray, CommonDreams.org, April 3, 2003, http://www.commondreams.org/views03/0403-10.htm

DC88 «Somebody's listening,» by Duncan Campbell, New Statesman, 12 August 1988, http://jya.com/echelon-dc.htm

DC99 «Intercepting the Internet,» by Duncan Campbell, The Guardian, April 29, 1999, http://www.guardian.co.uk/online/story/0,3605,293985,00.html

DE03 «Bush wants US to back Euro-cybercrime treaty,» by Declan McCullagh, CNET News.com, November 20, 2003, http://www.silicon.com/management/government/ 0,39024677,39116980,00.htm

DE60 «Public Papers of the Presidents», Dwight D. Eisenhower, 1960, p. 1035-1040, http://coursesa.matrk.msu.edu/~hst306/documents/indust.html

DF03 «Trusted Computing Group Forms,» by Dennis Fisher, EE Week, April 8, 2003, http://www.eweek.com/article2/0,4149,1010161,00.asp

DGOO Remarks Prepared for Delivery by NASA Administrator Daniel S. Goldin at the Jet Propulsion Laboratory, March 29, 2000, http://www.hq.nasa.gov/office/pao/ftp/ Goldin/00text/jpl_remarks.txt

DG02 «Robo-rat controlled by brain electrodes,» by Duncan Graham-Rowe, New Scientist, 01 May 2002, http://www.newscientist.com/news/print.jsp?id=ns99992237

DG03 «Cellphone positioning finds its place,» by Duncan Graham-Rowe, New Scientist, 19 October 2003, http://www.newscientist.com/news/news.jsp?id= ns99994270

DJ03 «The Case of the Diebold FTP Site,» by Douglas W. Jones, University Of Iowa, July 28,2003, http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html

DM02 «Poindexter's Incredibly Shrinking Site,» by Declan McCullagh, Dec 2002, http://www.politechbot.com/p-04262.html

DM03 «The Marshall Plan,» by Douglas McGray, WIRED, Issue 11.02 – February 2003, http://www.wired.eom/wired/archive/l 1.02/marshall.html

DM99 «Cell Phone Crypto Penetrated,» by Declan McCullagh, Wired News, 6 Dec 1999, http://www.wired.com/news/politics/0,1283,32900,00.html

DO02 «MD Implants Tracking Devices In Cars Of Convicted Drunk Drivers,» by Dennis O'Brien, Baltimore Sun, 15 Aug 2002, http://www.rense.com/general28/conv.htm

DR01 «U.S. to Close Eavesdropping Post,» by David Ruppe, ABC News, June 1, 2001, http://abcnews.go.com/sections/world/DailyNews/echelon_010601.html

DR03 «Nuclear-powered drone aircraft on drawing board,» by Duncan Graham-Rowe, New Scientist, 19 February 2003, http://www.newscientist.com/news/news.jsp?id= ns99993406

DS03 «Motorola breaks out mini-GPS module» by Dinesh C. Sharma, CNET News, September 10, 2003, http://news.com.com/2100-1037-5074015.html

DT03 «Drones To Guard Tex-Mex Border?» by Associated Press, May 13, 2003, http://www.cbsnews.com/stories/2003/05/13/national/main553760.shtml

DV03 «Why Biometrics Must Be Banned,» by Roger Clarke, presentation at the Conference on 'State Surveillance after September 11', Sydney, 8 September 2003,

http://www.anu.edu.au/people/Roger.Clarke/DV/Biom030908.html

DV98 «Spies turn to high-tech info ops,» by Daniel M. Verton, Federal Computer Week, May 25,1998, http://www.fcw.com/fcw/articles/1998/FCW_052598_483.asp

DV99 «Pentagon labels computer morphing a war crime,» by Daniel M. Verton, Federal Computer Week, November 12, 1999, http://www.fcw.com/fcw/articles/1999/ fcw_11121999_dod.asp

DW99 «The Real-Time Cryptanalysis of A5/2,» by David Wagner et al., Rump Session of Crypto '99, Santa Barbara, August 15-19,1999

EA02 «Food and Drug Administration OKs Implantable ГО Chips», EPIC Alert, Volume 9.22, November 6, 2002, http://www.epic.org/alert/EPIC_Alert_9.22.html

EB01 «This Ping Thing Didn't Take Wing,» by Elisa Batista, Wired News, Nov. 30, 2001, http://www.wired.com/news/privacy/0,1848,48631,00.html

ED03 «French home secretary announces chip ГО card,» by Estelle Dumout, Silicon.com, 1 October 2003, http://www.silicon.eom/news/500022/l/6228.html

EF03 «Privacy – Crypto – Key Escrow 1993-4 (US): Clipper/EES/Capstone/Tessera/ Skipjack», EFF Archive, Last Updated 13 Mar 2003, http://www.eff.org/ pub/Privacy/Key_escrow/Clipper/

EG02 «Trainable Videorealistic Speech Animation,» by Tony Ezzat, Gadi Geiger To-mazo Poggio, MIT Center for Biological and Computational Learning, Siggraph 2002, http://cuneus.ai.mit. edu:8000/publications/siggraph02.pdf

EH63 «What I Would Tell a Son» by J. Edgar Hoover, Family Weekly, 14 July 1963

EM75 «National Communications Security Emanations Memoranda (NACSEM) 5112, NONSTOP Evaluation Techniques», 1975, http://cryptome.org/nacsem-5112.htm

EP01 European Parliament Report on the existence of a global system for intercepting private and commercial communications (ECHELON interception system), PE 305.391, July 11,2001, http://cryptome.org/echelon-ep.htm

EP99 «Europe and ENFOPOL: Batch Release of Documents,» in Policy Archive, by FIPR: Foundation for Information Policy Research, November 1999, http://www.fipr.org/polarch/index.html

ER94 «Equidistant Letter Sequences in the Book of Genesis,» by Eliyahu Rips, Doron Witztum, Yoav Rosenberg, Statistical Science, Vol. 9 (1994) 429-438, http://www.torahcodes.co.il/wrrl/wrrl.htm

ES03 «Enterprise Solutions Division Board of Directors», About The ES Division, Information Technology Association Of America, http://www.itaa.org/es/about.cfm

ETOO «US move for Aspex with 'all pervasive' DSP core,» Electronics Times, Issue: Sept 11,2000, http://gbop.nm.ru/etOO.htm

EW03 «Aspex licenses technology to chip maker in fab deal», Electronics Weekly, 20 August 2003, http://www.electronicsweekly.co.uk/issue/newsview.asp7vpattW arti-cles/2003/08/20/story05.htm

FA01 «Frequently Asked Questions about the 3G-International Acquisition», RSA Security, 2001, http://www.rsasecurity.com/go/3gi/faq.html

FA03 '"Soldier's Ethic' Guides Powell At the FCC," by Frank Ahrens,

Washington Post, October 15,2003; http://www.bizreport.com/article.php?art_id=5179

FCOO «Son of Windows to control carrier,» Federal Computer Week, August 07, 2000, http://www.fcw.com/fcw/articles/2000/0807/news-navy-08-07-00.asp

FC01 «Funding opens carrier to Windows,» Federal Computer Week, Feb. 02, 2001, http://www.fcw.com/fcw/articles/2001/0129/web-navy-02-02-01.asp

FC03 «U.S. buys data on foreign citizens: Information lets federal agencies to track tourists, immigrants,» by Associated Press, April 13, 2003; http://www.msnbc.com/ news/899805.asp?0si=-

FD91 «The Truth Will Out: Interrogative Polygraphy With Event-Related Brain Potentials,» by L.A.Farwell and E.Donchin, Psychophysiology, 28:531-547, 1991

FN03 «Sources Say Jessica Lynch Has Amnesia», by Fox News, 05 May 2003, http://www.foxnews.com/story/0,2933,85936,00.html

FPOO «NATO used speeded-up film to excuse civilian deaths in Kosovo: newspaper,» AFP, January 6, 2000, http://gbop.nm.ru/rpOO.htm

FP03 «Rescued POW had no gunshot, knife wounds: father,» AFP, April 03, 2003, http://www.spacewar.com/2003/030403213949.0bsaiduj.html

FQ03 GSM Security FAQ, http://gsmsecurity.com/faq.shtml

FS02 «In the future, eyes are the window to the wallet,» by AP, Jun. 28, 2002, http://www.siliconvalley.com/mld/siliconvalley/news/editorial/3562920.htm

FW03 «Bioethics The Brain,» by Kenneth R. Foster, Paul Root Wolpe Arthur L. Cap-Ian, IEEE Spectrum Online, June 2003, http://www.spectnim.ieee.org/WEBONLY/ publicfeature/jun03/bio.html

FW74 «The Ultra Secret», by Frederick William Winterbotham, 1974

GA03 «Frequently Asked Questions», Government Information Awareness Program, 2003, http://opengov.media.mit.edu/FAQ.html

GA98 «List of the world's most powerful computing sites», (according to Gunter Ahrendt), August 1998, http://www.computerra.ru/download/ga_a_98.html

GB01 «Project: Acoustic Kitty,» by Julian Borger, Guardian, September 11, 2001, http://www.guardian.co.uk/elsewhere/journalist/story/0,7792,550122,00.html

GC03 «Will War Swap Privacy for Security?» by Grant Gross, IDG News Service, March 20,2003

GIOO «GILC Member Letter on Council of Europe Convention on Cyber-Crime,» Global Internet Liberty Campaign, October 18, 2000, http://www.gilc.org/privacy/coe-letter-1000.html

GI03 «MIT winds down radio tag activity,» by Alorie Gilbert, CNET News.com, October 23,2003, http://news.com.com/2100-1008-5095957.html

GJ01 «Bush Halts Inquiry of FBI and Stirs Up a Firestorm,» by Glen Johnson, Boston Globe, Dec 14, 2001, http://www.commondreams.org/headlines01/1214-01.htm

GL02 «Pentagon Defense Strategist Previews Future Warfare,» by George Lewis, U. of Kentucky News, July 11, 2002, http://www.uky.edu/PR/News/AndyMarshall.htm

GL03 «DoD enlists RFID tags in procurement battle,» by George Leopold, EE Times, October 23,2003, http://www.eetimes.com/story/OEG20031023S0054

GO03 «Maryland Proceeds with Voting Machine Installation. Independent Analyst Submits Positive Review of Diebold Machine», Maryland Governor's Office Press Release,

September 24,2003, http://www.dbm.maryland.gov/SBE

GR03 Subject: «A precis of the new attacks against GSM encryption,» by Greg Rose, posting to cryptography@c2.net mailing list, 11 Sep 2003, http://www.mit.edu: 8008/bloom-picayune/crypto/14159

GS03 «Wal-Mart cancels 'smart shelf trial,» by Alorie Gilbert and Richard Shim, CNET News.com, July 9,2003, http://news.com.com/2100-1019-1023934.html

GS91 «George Bush, Skull Bones and the New World Order» by Paul Goldstein and Jeffrey Steinberg, ParaScope, April 1991, http://www.freedomdomain. com/secretsocieties/skullO 1.html

GS98a «NT critic gets audience with DOD chieftains,» by Gregory Slabodkin, GCN, October 12,1998, http://www.gcn.com/archives/gcn/1998/Octoberl2/lc.htm

GS98b «Former Microsoft contractor Ed Curry says that the company deliberately misled government buyers,» by Gregory Slabodkin, GCN, October 26, 1998, http://www.gcn. com/archives/gcn/1998/October26/8.htm

GS98c «Software glitches leave Navy Smart Ship dead in the water,» by Gregory Slabodkin, GCN, July 13,1998, http://www.gcn.com/archives/gcn/1998/julyl3/ cov2.htm

HB02 «Tests Raise Questions of Face-Scan Technology's Reliability,» by Hiawatha Bray, NewsFactor Network, August 06, 2002, http://www.newsfactor.com/perl/story/ 18899.html

HB03 «Perle's Conflict Issue Is Shared By Others on His Defense Panel,» by Tom Hamburger and Dennis K. Berman, The Wall Street Journal, 27 March 2003

HK02 «Smart ID Card Worries Hong Kong», Associated Press, March 10, 2002, http://www.wired.com/news/technology/0,1282,50961,00.html

HM01 «The Very Strange Case Of The NSA And Lake Vostok In Antarctica,» by Harry Mason, Feb 28,2001, http://www.rense.com/general9/ant.htm

IAOO «Lying With Pixels,» by Ivan Amato, MIT Technology Review, July/August 2000, http://www.nodeception.com/articles/pkel.jsp

IA02 «For the Spy in the Sky, New Eyes,» by Ian Austen, New York Times, June 20, 2002, http://www.nytimes.com/2002/06/20/technology/circuits/20SPYY.html

ICOO «Interception Capabilities 2000,» by Duncan Campbell, April 1999, http://www. iptvreports.mcmail.com/stoa_cover.htm

ЦЩ99 «Suicide Mysterieux Au Pont Bessieres,» par Ian Hamel, L'Ulustre, 26 mai 1999, http://www.illustre.ch/1999/21/suicide_21.html

IM89 «Suggestions For Anticipating Requests Under Freedom Of Information Act,» the internal NASA memo from 1989, disclosed by Rep. Howard Wolpe in 1992, http://www.fas.org/sgp/othergov/nasafoia89.html

ЮОО3 «Iraq: Regulating the newly independent Iraqi media,» Index on

Censorship, 27 July 2003,http://www.indexonline.org/news/20030727_iraq.shtml

IR03 «Vote count marred by computer woes,» The Indianapolis Star Report, November 9, 2003, http://www.indystar.eom/articles/6/091021-1006-009.html

ISOO Iridium Satellite: Corporate Fact Sheet. http://www.iridium.com/corp/iri_corp-story. asp?storyid=2

IS03 «Irvine Sensors Demonstrates Complete Stacked Computer,» Press Release, 22 Aug 2003, http://www.irvine-sensors.com/pdf/08-22-03%20ISC%20demonstrates%20 complete%20stacked%20computer.pdf

JA01 «How the facial recognition security system works», by Joseph Atick, CNN.com chat room, Oct 1, 2001, http://edition.cnn.com/2001/COMMUNITY/10/01/atick/

JBOO «Free, anonymous information on the anarchists' Net,» by John Borland, CNET News.com, April 26, 2000, http://news.com.com/2100-1033-239756.html

JB01 «Internet Voting Project Cost Pentagon $73,809 Per Vote,» by John Dunbar, The Public Integrity Special Report, August 9, 2001, http://www.notablesoftware.com/ Press/JDunbar.html

JD01 «Pentagon braces for a makeover,» by John Dillin, The Christian Science Monitor, February 12, 2001

JD02 «French agents probe Murdoch firm,» by Jamie Doward, The Observer, March 17, 2002, http://observer.guardian.co.uk/business/story/0,6903,669046,00.html

JD03 «500 paedophiles to be tracked by satellite tags,» by Jamie Doward, Observer, Sep 21,2003, http://observer.guardian.co.uk/uk_news/story/ 0,6903,1046614,00.html

JD97 «Networking With Spooks» by John Dillon, Covert Actions Quarterly, Winter 1997, http://mediafilter.org/caq/internic

JD99 «Are Pentagon computers compromised? Analyst charges Windows NT isn't secure,» by Jon E. Dougherty, WorldNetDaily.com, Feb 23, 1999, http:// www.worldnetdaily.conVbluesky_dougherty/19990223_xnjdo_are_pentag.sht ml

JE02 «Mob informant scandal involved highest levels of FBI, documents show,» by Jeff Donn, Associated Press, July 28, 2002, http://www.boston.com/news/daily/28/ fbi_mob.htm

JE98 «NSA Network Security Framework Forum (NSFF), Baltmore Maryland, March 2 1998,» by Jeremy Epstein, IEEE Cipher, 1998, http://www.ieee-security.org/Cipher/ ConfReports/conf-rep-NSFF.html

JG97 «Cryptanalysis of Alleged A5 Stream Cipher,» by Jovan Golic, in Proceedings of EUROCRYPT'97, LNCS 1233, Springer-Verlag 1997, http://jya.com/a5-hack.htm

JH01 «Free the Encyclopedias!» by Judy Heim, Technology Review, September 4, 2001, http://www.techreview.com/articles/print_version/heim090401. asp

JH03 «The Business of Fear,» by Jack Hitt, Business 2.0, June 2003, http://www.business2.com/subscribers/articles/mag/0,1640,49468,00.html

JK03 «Saving Private Lynch story 'flawed',» by John Kampfner, BBC News, 15 May 2003, http://news.bbc.co.Uk/2/hi/programmes/correspondent/3028585.stm

JL02 «Neuromarketing firm launched by Atlanta ad veteran,» by Jim Lovel, Atlanta Business Chronicle, June 17, 2002, http://atlanta.bizjournals.com/atlanta/stories/2002/06/ 17/story6.html

JL03 «ID cards protect civil liberties – Blair,» by John Leyden, The Register, 30 Sept 2003, http://www.theregister.co.Uk/content/6/33138.html

JM02 «Implantable chips make first run at personal Ш,» by Charles J. Murray, EE Times, February 16, 2002, http://www.eetimes.com/story/OEG20020215S0046

JM03 «13 million on terror watch list», by James Gordon Meek, NY Daily News, April 8, 2003, http://www.nydailynews.com/04-08-2003/news/wnj-eport/story/73628p-68132c.html

JM96 «The Complete, Unofficial TEMPEST Information Page,» by Joel McNamara http://www.eskimo.com/~joehn/tempest.html

JO03 «Hollywood goes paranoid,» by Joanne Ostrow, The Denver Post, May 18, 2003, http://www.denverpost.com/Stories/0,1413,36~122~1393956,OO.html

JP01 «Roosevelt's Secret War: FDR and World War Two Espionage,» by Joseph Persico, Random House, 2001

JR01 «A Cautionary Tale for a New Age of Surveillance,» By Jeffrey Rosen, New York Times Magazine, October 7, 2001, http://www.nytimes.com/2001/10/07/magazine/ 07SURVEILLANCE.html

JS01 «Thought Police Peek Into Brains,» by Julia Scheeres, Wired News, October 05, 2001, http://www.wired.com/news/business/0,1367,4722l,00.html

JS02 «Understanding the Windows EAL4 Evaluation», by Jonathan S. Shapiro, http://eros.cs.jhu.edu/~shap/NT-EAL4.html

JS03 «Three R's: Reading, Writing, RFID» by Julia Scheeres, Wired News, Oct. 24, 2003, http://www.wired.com/news/technology/0,1282,60898,00.html

JU02a «They Want Their Ш Chips Now,» by Julia Scheeres, Wired News, 06 Feb 2002, http://www.wired.com/news/privacy/0,1848,50187,00.html

JU02b «Politician Wants to 'Get Chipped',» by Julia Scheeres, Wired News, Feb. 15, 2002, http://www.wired.com/news/technology/0,1282,50435,00.html

JU02c «ID Chip's Controversial Approval,» by Julia Scheeres, Wired News, Oct. 23, 2002, http://www.wired.com/news/politics/0,1283,55952,00.html

JU03 «When Cash Is Only Skin Deep,» by Julia Scheeres, Wired News, Nov. 25, 2003, http://www.wired.com/news/technology/0,1282,61357,00.html

JWOO «Why We Spy on Our Allies,» by R. James Woolsey, The Wall Street Journal, March 17,2000, http://cryptome.org/echelon-cia2.htm

JW02 «Watching your every move,» by Jane Wakefield, BBC News Online, 1 February, 2002, http://news.bbc.co.Uk/2/hi/science/nature/1789157.stm

JW03 «GSM Association downplays mobile security concerns,» by John Walko, EETimes Germany, September 3,2003, http://www.eetimes.de/at/news/OEG20030903S0018

JW94 «The Future Direction of Intelligence», address by James Woolsey to the Center for Strategic and Internatioal Studies, Washington, D.C., 18 July

1994

JY01 «Euro bank notes to embed RFID chips by 2005,» by Junko Yoshida, EE Times, December 19,2001, http://www.eetimes.com/story/OEG20011219S0016

KA98 «Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations,» by Markus Kuhn and Ross Anderson, in Information Hiding, Second International Workshop, IH'98, Portland, Oregon, USA, April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf

KB93 «Mobile ComSec in Europe (A5),» by Klaus Brunnstein, RISKS DIGEST, Volume 14: Issue 60,12 May 1993, http://catless.ncl.ac.uk/Risks/14.60.htmltfsubj6.1

KD92 «Hiding Space. NASA's Tips for Avoiding Scrutiny,» by Kate Doyle, Columbia Journalism Review, July/August 1992, http://www.cjr.Org/year/92/4/nasa.asp

KF03 «Brave new elections,» by Mike Keefe-Feldman, Missoula Independent, Vol.14 No. 50, Dec 11,2003, http://www.missoulanews.com/News/News.asp?no=3670

KJ99 «Differential Power Analysis,» by P. Kocher, J. Jaffe, B. Jun; in Crypto 99 Proceedings, LNCS 1666, M. Wiener ed., Springer-Verlag, 1999. http://www.cryptography.com/resources/whitepapers/DPA.pdf

KK99 «Design Principles for Tamper-Resistant Smartcard Processors,» by Oliver Kom-merling, Markus G. Kuhn, USENIX Workshop on Smartcard Technology, Chicago, Illinois, USA, May 10-11,1999. http://www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf

KPOO «Echelon Reporter answers Ex-CIA Chief,» by Kevin Poulsen, SecurityFocus.com, March 23,2000, http://www.securityfocus.eom/news/6

KP01 «Electronic warfare tactics wipe out thousands of hacked smart cards,» by Kevin Poulsen, SecurityFocus, Jan 25 2001, http://www.securityfocus.com/news/143

KR02 «Iraqi Denial and Deception Far Beyond Battlefield Tactics,» by Kathleen T. Rhem, American Forces Press Service, Oct. 8, 2002, http://www.defenselink.mil/news/ Oct2002/nl0082002 200210085.html

KR03 «Iraqis Say Lynch Raid Faced No Resistance,» by Keith B. Richburg, Washington Post, April 15, 2003, http://www.washingtonpost.com/ac2/wp-dyn/A26714-2003Aprl4

LD03 «Mark of the Beast: Ш Verichip microchip called Digital Angel» by These Last Days Ministries, Revised: November 25, 2003, http://gvsregistry.4verichip.com

LG02 «Trusted Computing Platform Alliance: The Mother(board) of all Big Brothers», Lucky Green, Presentation at the 11th USENIX Security Symposium, August 2002, http://www.cypherpunks.to/TCP A_DEFCON_10.pdf

LG03 «The story behind the Lynch story,» by Lou Gelfand, Star Tribune, June 1, 2003, http://www.startribune.com/stories/782/3910734.html

LG96 «The Package» by Bernard Levine and Fred Guinther, Electronic News, Issue: 29 July 1996, http://gbop.nm.ru/lg96.htm

LG99 «More NSAKEY musings,» by Lucky Green, Crypto-Gram, September 15, 1999, http://www.schneier.com/crypto-gram-9909.html

LL03b «NIST Ignores Scientific Method for Voting Technology,» by Lynn

Landes, Voting Machine Webpage, Dec. 15,2003, http://www.ecotalk.org/NIST.htm

LL03a «Offshore Company Captures Online Military Vote», by Lynn Landes, Voting Machine Webpage, July 16, 2003, http://www.ecotalk.org/SERVEaccenture.htm

LM03 «Computer Voting Expert Ousted From Elections Conference,» by Lynn Landes, www.EcoTalk.org, Aug 1, 2003, http://www.ecotalk.org/MercuriIACREOT.htm

LNOO «Black Mass: The Irish Mob, the FBI, and a Devil's Deal,» by Dick Lehr and Gerard O'Neill, Public Affairs, 2000

LR03 «Americans give thumbs up to biometrics,» by John Leyden, The Register, Jan 8, 2003, http://www.securityfocusonline.com/news/2001

LU02 «Information Leakage from Optical Emanations,» by Joe Loughry and David A. Umphress, ACM Trans. Info. Sys. Security, Vol. 5, No. 3, pp. 262-289. http://applied-math. org/acm_optical_tempest.pdf

MA03 «Is RFK» Technology Easy to Foil?» by Mark Baard, Wired News, Nov. 18, 2003, http://www.wired.com/news/privacy/0,1848,61264,00.html

MBO3a «GCHQ arrest over Observer spying report,» by Martin Bright, The Observer, March 9,2003, http://www.observer.co.uk/iraq/story/0,12239,910648,00.html

MBO3b «Shoot-to-kill demand by US», by Martin Bright, The Observer, November 16, 2003,http://observer.guardian.co.uk/uk_news/story/0,6903,1086397,00.html

MB99 «Solving the Bible Code Puzzle,» by Brendan McKay, Dror Bar-Natan, Maya Bar-Hillel, and Gil Kalai, Statistical Science, Vol. 14 (1999) 150-173, http://cs.anu.edu.au/~bdm/dilugim/StatSci

MCO3 «Uncensored Gore (an interview with Gore Vidal),» by Marc Cooper, LA Weekly, November 14 – 20,2003, http://www.laweekly.com/ink/03/52/features-cooper.php

MDOO The 2000 Ballistic Missile Defense Applications Report, http://www.defenselink. mil/specials/missiledefense/tar02g.html

MD02 «Bible Code П: The Countdown,» by Michael Drosnin, 2002

DW02 «He's Ba-a-ack!» by Maureen Dowd, The New York Times, December 1, 2002, http://www.nytimes.com/2002/12/01/opinion/01DOWD.html

MD97 «Bible code,» by Michael Drosnin, 1997

MP97 1997 Space And Missile Defense Technologies Army Science and Technology Master Plan, http://www.fas.org/man/dod-101/army/docs/astmp/aD/D5C.htm

ME01 «Cops tap database to harass, intimidate,» by M.L.Elrick, Detroit Free Press, July 31,2001, http://www.freep.com/news/mich/lein31_20010731.htm

ME03 «Cryptographers sound warnings on Microsoft security plan,» by Rick Merritt, EE Times, April 15,2003, http://www.eetimes.com/story/OEG20030415S0013

MFOO «VeriSign buys Network Solutions in $21 billion deal» by Melanie Austria Farmer, CNETNews.com, March 7, 2000, http://news.com.com/2100-1023-237656.html

MF02 «Partnership is Critical to Preparation», Microsoft Froutlines, 2002

February, 18th Issue, http://www.microsoft.com/usa/government/Februaryl 8thlssue.pdf

MF98 «New security flap over Windows NT», by Mary Jo Foley, Sm@rt Reseller, September 23,1998, http://www.zdnet.com/zdnn/stories/news/0,4586,2140612,00.html

MK02 «Optical Time-Domain Eavesdropping Risks of CRT Displays,» by Markus Kuhn, Proceedings of the 2002 IEEE Symposium on Security and Privacy, Berkeley, California, 12-15 May 2002, http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf

ML03 «Voting Machines Gone Wild!» by Mark Lewellen-Biddle, In These Times, 11 Dec 2003, http://www.mthesetmes.cony comments.php?id=490_0_l_0_C

MM01 «Making Dead Birds The Deal of the Century,» by Michael Menduno, Wired, August 2001, http://www.wired.com/wired/archive/9.08/mustread.html?pg=8

MM03 «What's inside the government's e-voting booth?» by Susan M. Menke, GCN, 14 July 2003, http://www.gcn.com/22_18/new_products-technology/22718-l.html

MN02 «Homeland Insecurity,» by Merrell Noden, Popular Science, September 2002, http://www.popsci.com/popsci/science/article/0,12543,335438,00.html

PY03 «Peru wants Yale to give back relics,» by Associated Press, March 6, 2003, http://www.cnn.com/2003/WORLD/americas/03/06/peru.relic.ap/

MP03 «The Real 'Saving of Private Lynch',» by Mitch Potter, Toronto Star, May 4, 2003 http://www.refuseandresist. org/war/art.php?aid=769

MR02 «How to find hidden cameras», by Marc Roessler, preprint, 2002, http://www.tentacle.franken.de/papers/hiddencams.pdf

MR03 «Intel Backs Off Security Plan: LaGrande architecture will appear in only some chips, and can be disabled,» by Robert McMillan, IDG News Service, September 17, 2003,http://www.pcworld.com/resource/printable/article/0,aid,112519,00.asp

MS01 «Bruce Lee's Fantastic Comeback,» by Michael Stroud, Wired News, November 16, 2001, http://www. wired. com/news/digiwood/0,1412,48449,00.html

MZ02 «Scanning Tech a Blurry Picture,» by Declan McCullagh and Robert Zarate, Wired News, Feb 16, 2002, http://www.wired.com/news/print/0,1294,50470,00.html

ND03 «NDS Rejects EchoStar Lawsuit as Opportunistic and Baseless,» NDS Press Release, 20 June 2003, http://www.nds.com/newspdfs/EchoStar_200603.pdf

NH96 «Secret Power,» by Nicky Hager, Craig Potton Publishing, New Zealand, 1996.

N102 «Top Ten Most Stolen Vehicles in the U.S.» by the US National Insurance Crime Bureau (NICB), December 10, 2002, http://www.mymobileguardian.com/MG/ MG_topten.asp

N103 «NIST Symposium on Building Trust and Confidence in Voting Systems,» Gaithers-burg, Maryland, Dec. 10-11,2003, http://vote.nist.gov/

NN01 «NASA and NIMA Begin Joint Review Of Mars Polar Lander Search Analysis,» NASA Press Release, 26 Mar 2001,

http://sse.jpl.nasa.gov/whatsnew/pr/ 010326A.html

NP98 «Probing into C2 security claims: Is NT as secure as Microsoft has said it is?» by Nicholas Petreley, InfoWorld, July 13, 1998, http://www.infoworld.com/pageone/ opinions/petrel/980713np.htm

NR02 «GSM calls even more secure thanks to new A5/3 Algorithm,» ETSI News Release, 3 July 2002, http://www.etsi.org/pressroom/previous/2002/3algorithm.htm

NSOO «Name.Space, Inc. v. Network Solutions», US Court Of Appeals, Decided: January 21,2000, http://namespace.pgmedia.net/law/appeal/2ndcir-dec.html

NS02 NavSource Online: Aircraft Carrier Photo Archive, PCU GEORGE H.W. BUSH (CVN-77), http://www.navsource.org/archives/02/77.htm

NS03 «Stop dodging the awkward truth,» by Norman Solomon, The Observer, March 9, 2003,http://www.observer.co.uk/iraq/story/0,12239,910381,00.html

NY03 «NYC police to destroy database on protesters,» by AP, Apr 11, 2003, http://www.usatoday.com/tech/news/techpolicy/2003-04-ll-nypd-database_x.htm

OI89 Obituary: «Intrepid» – Sir William Stephenson, Time, Feb. 13,1989, page 76

OR03 «SAIC has role in cellphone changes,» The Oak Ridger, 27 November 2003, http://www.oakridger.eom/stories/l 12703/new_20031127006.shtml

PBO3 «Tampa police eliminate facial-recognition system,» by Associated Press, 08 Aug 2003, http://www.palmbeachpost.com/news/content/news/0820camera.html

PD02 «Arlington 'Bait Car' Hooks Suspect,» by By Patricia Davis, The Washington Post, 16 April 2002, http://lists.jammed.com/crime/2002/04/0099.html

PE03 «Hall Monitors or Spies? Wireless Tech to Track Building Occupants,» by By Paul Eng, ABC News, Sept. 10, 2003, http://abcnews.go.com/sections/scitech/ Fu-tureTech/smartbadges03 0910.html

PG99 «Re: Forthcoming Biryukov/Shamir result against A5/1 GSM privacy algorithm», Peter Gutmann, posting to cryptography@c2.net mailing list, 7 Dec 1999, http://www.mail-archive.eom/cryptography@c2.net/msg02546.html

PKOO «Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned,» by Ton van der Putte and Jeroen Keuning, in the Proceedings of Fourth Working Conference on Smart Card Research and Advanced Applications, pages 289-303, Kluwer Academic Publishers, 2000; http://cryptome.org/fake-prints.htm

PK03 «In the Company of Spies,» by Paul Kaihla, Business 2.0, May 01, 2003, http://www.business2.com/subscribers/articles/mag/0,1640,49068,00.html.

PK96 «Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems,» by P. Kocher, in Crypto 96 Proceedings, LNCS 1109, Springer-Verlag, 1996. http://www.cryptography.com/resources/whitepapers/TimingAttacks.pdf

PL98 «Re: Status of GSM Crypto Attacks», Paul Leyland, posting to

uk-crypto@maillist.ox.ac.uk mailing list, 21 Oct 1998, http://jya.com/gsml02898.htm

PR02 «Can a Hacker Outfox Microsoft?» by Peter Rojas, Oct. 18, 2002, Wired News, http://www.wired.com/news/technology/0,1282,55807,00.html

PR03 «Poll Examines Saddam, 9-11 Link,» Associated Press, September 06, 2003, http://wireservice.wired.com/wired/story.asp?section=BreakingstoryId=779532

PS02 «Prison Statistics On June 30, 2002,» U.S. Department of Justice, Bureau of Justice Statistics, 2002, http://www.ojp.usdoj.gov/bjs/prisons.htm

PW87 «Spycatcher – The Candid Autobiography of a Senior Intelligence Officer,» by Peter Wright, William Heinemann Australia, 1987

QA03 «QA On Facial Recognition,» ACLU Web feature on face-recognition technology, 2003,http://www.aclu.org/Privacy/Privacy.cfm?ro=13434c=130

RA03 «Trusted Computing Frequently Asked Questions – TC / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCP A» by Ross Anderson, Version 1.1 (August 2003), http://www.cl.cam.ac.uk/~rjal4/tcpa-faq.html

RA94 «Subject: A5», Ross Anderson, posting to Newsgroups: sci.crypt,alt.security; 17 Jun, 1994, http://www.ecn.org/crypto/etere/ander.htm

RA96 «The Eternity Service,» by Ross J. Anderson, in Proceedings of Pragocrypt 96, http://www.cl.cam.ac.uk/users/rjal4/eternity/eternity.html

RB98 «And there are it nevertheless, the movement profiles,» by Niklaus Ramseyer and Denis Von Burg, SonntagsZeitung Online, July 12, 1998. English translation: http://jya. com/gsm-scandal.htm

RC03 «Banned BBC film up for sale on internet,» by Rob Crilly, Glasgow Herald, 26 August 2003, http://www.theherald.co.uk/news/archive/26-8-19103-0-7-44.html

REOO «Pentagon launches 'smart card' ID – New badges will serve as passport to electronic world,» by Reuters, Oct. 11, 2000, http://www.nytimes.com/reuters/technology/tech-smartcard-pentag.html

RE02 «Microsoft says Windows 2000 passes security check, gets Level 4 Common Criteria OK», Reuters, October 30, 2002, http://www.usatoday.com/tech/news/computer-security/2002-10-30-windows-secure_x.htm

RE03 «Microsoft Large Army Software Contract», Reuters, June 25, 2003. http://www.forbes.com/technology/newswire/2003/06/25/rtrl011470.html

RF03 «Michelin Embeds RFK» Tags in Tires,» RFID Journal News, Jan 17, 2003, http://www.rfidj ournal. com/article/articleview/269/1 /1 /

RH03 «On Election Day 2004, How Will You Know If Your Vote Is Properly Counted? -Answer: You Won't». Representative Rush Holt (Democrat, New Jersey). May 22, 2003, http://holt.house.gov/issues2.cfm?id=5996%20

RJ03 «Bad publicity, clashes trigger MS Palladium name change», The Register, 27 January 2003, http://www.theregister.co.uk/content/archive/29039.html

RL03 «VeriSign tapped to secure Internet voting» by Robert Lemos, CNETNews.com, 30 Sept 2003, http://news.com.com/2100-1029-5083772.html

RM03 Rumsfeld, Myers Pentagon Briefing, April 3, 2003,

http://usinfo.state.gov/topical/ pol/terror/texts/03040408.htm

RN03 «Bush OKs Global Crossing sale to STT,» Reuters, Sep 19, 2003, http://money.cnn. com/2003/09/19/news/international/global_crossing.reut/index.htm

RO02 «U.S. Hopes to Check Computers Globally,» by Robert OHarrow Jr., The Washington Post, 12 Nov 2002, http://www.washingtonpost.com/wp-dyn/articles/ A40942-2002Novll.html

RO99 «Airborne Remotely Operated Device (1982-1988),» ROBOTICS at Space and Naval Warfare Systems Center, San Diego, 10 December 1999, http://www.spawar. navy.mil/robots/air/arod/arod.html

RP01 «Ping service can test mobile phone availability», Rick Perera, 21 November, 2001, http://www.gate5.de/english/news/coverages/view_idg20011119.html

RR02 «Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards,» by Josyula R. Rao, Pankaj Rohatgi, Helmut Scherzer, Stephane Tinguely, 2002 IEEE Symposium on Security and Privacy, May 12 – 15, 2002 Berkeley, http://www.research. ibm.com/intsec/gsm.html

RR03 «Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes (Redacted Final)», SAIC-6099-2003-261, Sep 2, 2003, http://www.dbm.maryland. gov/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf

RS01 «Rental driver finds Big Brother over shoulder,» by Richard Stenger, CNN News, 22 June 2001, http://www.cnn.com/2001/TECH/ptech/06/22/gps.airiq/index.html

RS02 «Face Scanning at Airports: Ready for Prime Time?» by Richard M. Smith, Biometrics Presentation, 2002, http://www.computerbytesman.com/biometrics/ presentation

RS98 «Radio Sweden on Mobile Phone Tapping», Feb 1999, http://www.shmoo.com/ mail/cypherpunks/feb99/msg00306.html

RWOO «U.S. spying pays off for business,» by Robert Windrem, NBC News online, 15 April 2000, http://www.dei.uc.pt/majordomo/sociedade/msg01132.html

SA02 «Optical Fault Induction Attacks,» by Sergei P. Skorobogatov, Ross J. Anderson; Cryptographic Hardware and Embedded Systems Workshop (CHES-2002), San Francisco, CA, USA, 13-15 August 2002; http://www.cl.cam.ac.uk/~sps32/ches02-optofault.pdf

SCOO «When The Best Must Do Even Better,» the text of NASA Administrator Dan Goldin's speech before JPL, March 29, 2000, http://www.space.com/news/ goldin_speech_000329.html

SC01 «Sikorsky CYPHER П UAV Conducts First Flight», Press Release, July 5, 2001, http://www.sikorsky.com/news/20010705b.html

SC03 «TIA Is Dead – Long Live TIA» by Steven M. Cherry, IEEE Spectrum Online, Nov 2003, http://www.spectrum.ieee.Org/WEBONLY/resource/nov03/l103ntia.html

SC96 «Semiconductor Cubing,» NASA Spinoff Technologies Homepage, 1996, http://www.sti.nasa.gov/tto/spinoffl996/57.html

SC98 Press release of Smartcard Developer Association, 13 Apr 1998, http://www.scard. org/gsm/

SG03 «CIA exhibits spy gadgets with Bond edge» by Reuters, October 28, 2003, http://reuters.com/newsArticle.jhtml?type=technologyNewsstoryID=3706593

SI03 «Radio tracking devices set to boom,» by Swisslnfo, September 13, 2003, http://www.swissinfo.org/sen/Swissinfo.html?siteSect=511sid=1642638

KI01 «Identifying terrorists before they strike by using computerized knowledge assessment (CKA),» by Steve Kirsch, Version 2, October 07, 2001, http://www.skirsch.com/politics/plane/ultimate.htm

SK01 «Echelon Panel Calls It a Day,» by Steve Kettmann, Wired News, June 21, 2001, http://www.wired.eom/news/politics/0,1283,44721,00.html

SL01 «Thirty countries sign cybercrime treaty,» by Sarah Left, Guardian, November 23, 2001, http://www.guardian.co.uk/internetnews/story/0,7369,604964,00.html

SL02 «Where piracy and profits converge» by Bob Sullivan, MSNBC, May 30, 2002, http://www.legal-rights.org/NDSLAWSUIT/wherepiracy.html

SL03 «She Was Fighting to the Death, Details Emerging of W. Va. Soldier's Capture and Rescue,» by Susan Schmidt and Vernon Loeb, Washington Post, April 3, 2003; http://www.washingtonpost.com/ac2/wp-dyn/A14879-2003Apr2

SM03 «A Very American Coup,» by SCOOP New Zealand, 2002-2003 http://scoop.co.nz/ mason/features/?s=usacoup

SO03 «Microsoft plans new PC fortifications,» NewScientist.com news, 9 October 2003, http://www.newscientist.com/news/news.jsp?id=ns99994258

SP03 «Divvying up the Iraq Pie,» by Stephen Pizzo, AlterNet.org, Independent Media Institute, October 7,2003, http://www.alternet.org/story.html?StoryID=16901

SQ02 «On a New Way to Read Data from Memory,» by David Samyde, Sergei Skoroboga-tov, Ross Anderson, Jean-Jacques Quisquater; First International IEEE Security in Storage Worbhop, 11 December 2002, Greenbelt Marriott, Maryland, USA. http://www.flp.cl.cam.ac.uk/ftp/users/rjal4/SISW02.pdf

SR03 «Special Report: Attack on the 507th Maintenance Company, 23 March 2003, An Nasiriyah, Iraq», U.S. Army Public Affairs Office, July 17, 2003, http://www.army.mil/features/507thMaintCmpy/

SS03 «Uncle Sam keeps SAIC on call for top tasks,» by Scott Shane, The Baltimore Sun, October 26,2003, http://www.sunspot.net/news/bal-te.saic26oct26,0,1485260.story

ST03 «IBM details Blue Gene supercomputer», by Stephen Shankland, CNETNews.com, May 8,2003, http://news.com.com/2100-1008-1000421.html

SS94 «Cryptanalysis of the GSM A5 Cipher Algorithm», by Simon J. Shepherd, IEE Colloquium on Security and Cryptography Applications to Radio Systems, Digest No. 1994/141, Savoy Place, London, 3 June 1994

ST02 «Startup Profiles: Aspex Technology,» Semiconductor Times, February 2002, Vol 7 Issue 2, http://www.pinestream.com/PDF%20files/Semiconductor.pdf

SUOO «EU pact criminalizing security research?» By Bob Sullivan, MSNBC, October 25, 2000, http://www.zdnet.com/zdnn/stories/news/0,4586,2644958,00.html

SU02 «A $1 billion, corporate-funded hack?» by Bob Sullivan, MSNBC,

April 19, 2002, http://www.msnbc. com/news/740634. asp

SV03 «The yeast and the cockroach – a spy tale», by Sue Vorenberg, Seattle Post-Intelligencer, Oct 29, 2003, http://seattlepi.nwsource.com/national/ 145921_science29.html

SZ03 «Report Raises Electronic Vote Security Issues» by John Schwartz, Sep 25, The New York Times, http://www.nytimes.com/2003/09/25/technology/25VOTE.html

TA01 «3D Stacked Neuro Processor Device – 3DANN,» NASA Technology And Applications Program, February 14, 2001, http://technology.jpl.nasa.gov/gallery/ techGal-lery/gallery/gl_pages/DANN-R_Cube.html

TC01 «Brain-scans can defeat terrorism, InfoSeek founder claims,» by Thomas C Greene, The Register, 03 Oct 2001, http://www.theregister.co.uk/content/55/ 22020.html

TE03 «TR100/2003: 100 innovators poised to make a dramatic impact on our world», Technology Review, October 2003, http://www.techreview.com/trlOO/index.asp

TG01 «US Supremes: Hi-tech surveillance is out,» by Thomas C Greene, The Register, 12 June 2001, http://www.theregister.co.Uk/content/6/19655.html

TG03 «The truth about Jessica,» The Guardian, 15 May 2003, http://www.guardian.co.uk/ Iraq/Story/0,2763,956255,OO.html

TЮ3 «Microsoft software „riddled with vulnerabilities", trade body claims,» The Inquirer, 28 August 2003, http://www.theinquirer.net/?article=l 1249

TL02 «TEMPEST timeline», the compilation of the history of TEMPEST technology, http://cryptome.org/tempest-time.htm

TM01 «Climbing Inside The Criminal Mind (TIME 100: The Next Waveflnnovators/ Security/The Brain Scientist)», by Sarah Sturman Dale, Nov. 26, 2001, http://www.brainwavescience.com/in-the-news.php

TM02 «Impact of Artificial „Gummy" Fingers on Fingerprint Systems» by Tsutomu Ma-tsumoto et al., Prepared for Proceedings ofSPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002, http://cryptome.org/ gummy.htm

TR03 «Finger, faceprints get green light for Europe's ГО standard,» by John Lettice, The Register, 03 October 2003, http://www.theregister.co.Uk/content/6/33208.html

TT96 «Wild Bill And Intrepid: Donovan, Stephenson, and the Origin of CIA», by Thomas F. Troy, 1996

TZ02 «Body Check: Biometric Access Protection Devices and their Programs Put to the Test,» by Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler, c't, nil, 2002, http://www.heise.de/ct/english/02/! 1/114/

WB03 «China Begins Effort to Replace Citizen IDs With Digital Cards,» by Andrew Bat-son, Wall Street Journal, August 12, 2003, http://cryptome.org/cn-lbn-ids.htm

WE85 «Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?» by Wim van Eck, Computers Security 4 (1985) 269-286

WF03 «What is Freenet?» The Freenet Project Website, 2003, http://freenetproject.org/ index.php?page=whatis

WG95 «alt.scientology.war» by Wendy M. Grossman, Wired Magazine,

Issue 3.12 – Dec 1995, http://www. wired, com/wired/archive/3.12/alt. scientology.war.html

WH93 «Biography of Bobby Ray Inman,» The White House Office of the Press Secretary, December 16,1993, http://www.fas.org/irp/news/1993/931216i.htm

WJ03 «The Good Book holds key to bin Laden whereabouts,» The Wall Street Journal, Feb 28,2003,http://online.wsj.com/article/0,,SB1046387440730138423,OO.html

WK02 «Drone plane kills terror suspects,» by Will Knight, NewScientist.com news, 05 November 2002, http://www.newscientist.com/news/news.jsp?id=ns99993014

WK03 «Site Lets Citizens Monitor 'Big Brother',» by Jonathan Krim, Washington Post, July 8,2003; http://www.washingtonpost.com/ac2/wp-dyn/A23552-2003Jul7e=42

WM03 «Tipsters told Americans: POW is alive,» by Tracy Wilkinson and Greg Miller, Los Angeles Times, April 3, 2003, http://www.chicagotribune.com/news/nationworld/ iraq/chi-0304030290apr03,0,2870927.story?coll=chi-news-hed

WP03 «Maryland Keeps E-Voting System, Promises Fixes», Washington Post, 25 September 2003, http://www.washingtonpost.com/wp-dyn/articles/A60825-2003Sep24.html

WP04 «Wikipedia», from Wikipedia, the free encyclopedia; last modified 3 Jan 2004, http://en.wikipedia.org/wiki/Wikipedia

WS76 «A Man Called Intrepid: The Secret War», by William Stevenson, New York and London: Macmillan, 1976

WS98 «British Security Coordination: The Secret History of British Intelligence in the Americas 1940-1945», William S. Stephenson, ed., Fromm International Publishing, 1998.

YB02 «Smart glasses mean instant refills,» by Yudhijit Bhattacharjee, New Scientist, 04 April 2002,http://www.newscientist.com/news/news.jsp?id=ns99992123