access

# СОДРУЖЕСТВО НАДЗИРАЮЩИХ ГОСУДАРСТВ: ОБ ЭКСПОРТЕ И ПЕРЕПРОДАЖЕ РОССИЙСКОЙ ТЕХНОЛОГИИ СЛЕЖЕНИЯ НА ТЕРРИТОРИИ ПОСТСОВЕТСКОЙ ЦЕНТРАЛЬНОЙ АЗИИ

АВТОР: ПИТЕР БОРГЕЛАИС

# ОСНОВНЫЕ ПОЛОЖЕНИЯ

Четыре обсуждаемые в данном документе постсоветские центрально-азиатские республики – Казахстан, Таджикистан, Туркменистан и Узбекистан – имеют запятнанную репутацию в отношении электронной слежки, если принимать во внимание международные нормы надлежащих правовых процедур, конфиденциальности и прозрачности. Можно отметить некоторые значимые победы в отношении регулирования экспорта технологий слежки западными компаниями в такие проблематичные регионы, как Средний Восток. В то же время для региона с сильным влиянием России, такого как Центральная Азия, нужен иной подход. Мы начнем с описания российской системы для оперативно-розыскных мероприятий (СОРМ), комплекса технических средств и мер для обеспечения электронной слежки, разработанного в конце 1980-х годов советским КГБ и позднее использованного на территории всей Центральной Азии. После этого мы представим читателю главный итог этой работы: серию профилей, сортированных по странам, главных российских (и двух западных) компаний, которые экспортировали оборудование для осуществления электронной слежки в регион, а также приведем некоторые ранее неизвестные региональные проблемы, связанные с безопасностью самой системы СОРМ. В завершении мы обсудим возможные ответные действия со стороны глобального движения за цифровые права, оставляя разработку более детализованного и полного плана действий за будущими работами.

# МЕТОДОЛОГИЯ

Вся представленная здесь информация была получена из трех источников: ранее опубликованные исследовательские труды по теме, собственное исследование с использованием доступных ресурсов (таких как веб-сайты компаний и вики-страницы релевантной маркетинговой литературы), а также некоторые конфиденциальные источники с опытом работы в регионе.

# ВВЕДЕНИЕ

На территории четырех из пяти постсоветских центрально-азиатских государств – Казахстана, Таджикистана, Туркменистана и Узбекистана – проживают в сумме около 55 миллионов человек, все они живут в условиях режимов, которые год за годом занимают позиции самых деспотичных в мире.[1] Их рейтинг в отношении использования технологий перехвата коммуникаций и электронного слежения не является исключением из общего вектора пренебрежения к правовым процедурам и правам человека на конфиденциальность и свободу самовыражения. Тогда как контроль экспорта и политические кампании показали хотя бы частичную эффективность против западных компаний, продающих технологии слежения подобным режимам либо напрямую, либо через вторичные рынки, некоторые поставщики технологий слежения в регионе – это российские компании, которые не так легко поддаются лоббированию или давлению, как большинство западных компаний. В этом документе мы составили профили восьми компаний, которые продавали оборудование для электронного надзора или мобильной слежки в Центральной Азии, с указанием их связей с агентствами безопасности и/или телекоммуникационными операторами в регионе, а в некоторых случаях и историю их взаимодействия с российскими службами безопасности. В то время как вариантов противодействия в этом мало освещённом в СМИ регионе немного, некоторые возможности все же существуют: «клеймить и позорить» западных инвесторов, сотрудничающих с этими компаниями; проведение международных кампаний с вовлечением Управления Верховного комиссара Организации Объединённых Наций по делам беженцев (УВКБ) и Организации по безопасности и сотрудничеству в Европе (ОБСЕ); прямые действия с фокусом на обучение по вопросам безопасности; призыв к созданию сбалансированных и законных норм в отношении перехвата коммуникаций в Таджикистане; и возбуждение судебных разбирательств в отношении некоторых компаний.

1 Например, в 2011/2012 годах в Индексе Свободы Прессы, публикуемом Репортерами Без Границ, Таджикистан занял 122 позицию, в тройке с такими странами как Алжир и Малайзия. Казахстан в этом рейтинге занял 154 место, в паре с Ливией после смещения Каддафи, Узбекистан и Туркменистан заняли соответственно 157 и 177 места. Таким образом, Туркменистан находится ниже Китая, Ирана и Сирии, превосходя лишь Северную Корею и Эритрею (источник: Различные авторы (2011). ИНДЕКС СВОБОДЫ ПРЕССЫ 2011/2012. [В СЕТИ] доступно по ссылке: http://en.rsf.org/press-freedom-index-2011-2012,1043.html. [Дата последнего доступа: 1 декабря 2012].)

ТОГДА КАК КОНТРОЛЬ ЭКСПОРТА И ПОЛИТИЧЕСКИЕ КАМПАНИИ ПОКАЗАЛИ ХОТЯ БЫ ЧАСТИЧНУЮ ЭФФЕКТИВНОСТЬ ПРОТИВ ЗАПАДНЫХ КОМПАНИЙ, ПРОДАЮЩИХ ТЕХНОЛОГИИ СЛЕЖЕНИЯ ПОДОБНЫМ РЕЖИМАМ ЛИБО НАПРЯМУЮ, ЛИБО ЧЕРЕЗ ВТОРИЧНЫЕ РЫНКИ, НЕКОТОРЫЕ ПОСТАВЩИКИ ТЕХНОЛОГИЙ СЛЕЖЕНИЯ В РЕГИОНЕ – ЭТО РОССИЙСКИЕ КОМПАНИИ, КОТОРЫЕ НЕ ТАК ЛЕГКО ПОДДАЮТСЯ ЛОББИРОВАНИЮ ИЛИ ДАВЛЕНИЮ, КАК БОЛЬШИНСТВО ЗАПАДНЫХ КОМПАНИЙ.

# ПРЕДЫСТОРИЯ

Для начала некоторая предыстория о глобальной борьбе против электронной слежки в авторитарных режимах вне данного региона может проиллюстрировать, какой опыт был успешным в аналогичных условиях. Например, Area SpA, итальянская компания, специализирующаяся на технологии электронного перехвата, была замечена за построением системы слежения, которая «дала бы режиму сирийского президента Башара аль-Асада возможность перехватывать, сканировать и каталогизировать практически каждое сообщение электронной почты, которое проходит через страну»[2].

AREA SPA, ИТАЛЬЯНСКАЯ КОМПАНИЯ, СПЕЦИАЛИЗИРУЮЩАЯСЯ НА ТЕХНОЛОГИИ ЭЛЕКТРОННОГО ПЕРЕХВАТА, БЫЛА ЗАМЕЧЕНА ЗА ПОСТРОЕНИЕМ СИСТЕМЫ СЛЕЖЕНИЯ, КОТОРАЯ «ДАЛА БЫ РЕЖИМУ СИРИЙСКОГО ПРЕЗИДЕНТА БАШАРА АЛЬ-АСАДА ВОЗМОЖНОСТЬ ПЕРЕХВАТЫВАТЬ, СКАНИРОВАТЬ И КАТАЛОГИЗИРОВАТЬ ПРАКТИЧЕСКИ КАЖДОЕ СООБЩЕНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ, КОТОРОЕ ПРОХОДИТ ЧЕРЕЗ СТРАНУ»

НЕДАВНО, В КОНЦЕ АПРЕЛЯ 2012 ГОДА, ПРЕЗИДЕНТ ОБАМА ПОДПИСАЛ ПРИКАЗ, ПРЕДУСМАТРИВАЮЩИЙ САНКЦИИ ПРОТИВ ОРГАНИЗАЦИЙ, КОТОРЫЕ ЭКСПОРТИРУЮТ ИТ ОБОРУДОВАНИЕ, ПОЗВОЛЯЮЩЕЕ, «ИСПОЛЬЗУЯ БРЕШИ В КОМПЬЮТЕРАХ ИЛИ СЕТЯХ, ОСУЩЕСТВЛЯТЬ МОНИТОРИНГ ИЛИ СЛЕЖЕНИЕ, КОТОРЫЕ МОГЛИ БЫ ПОДДЕРЖАТЬ ИЛИ ОБЕСПЕЧИТЬ СЕРЬЕЗНЫЕ НАРУШЕНИЯ ПРАВ ЧЕЛОВЕКА» ПРАВИТЕЛЬСТВАМИ СИРИИ И ИРАНА.

NOKIA SIEMENS NETWORKS И ERICSSON, УШЛИ С РЫНКА ПОСЛЕ СВЯЗАННЫХ С ВЫБОРАМИ ПРОТЕСТОВ 2009 ГОДА.

ДВУМЯ ГОДАМИ ПОЗЖЕ ИЗ-ЗА НАРАСТАЮЩЕГО БЕСПОКОЙСТВА В США И ЕВРОПЕ КАСАТЕЛЬНО СВЯЗЕЙ КОМПАНИИ HUAWEI С ИРАНОМ, КОМПАНИЯ ЗАЯВИЛА, ЧТО «ДОБРОВОЛЬНО ОГРАНИЧИТ РАЗВИТИЕ СВОЕГО БИЗНЕСА В ЭТОЙ СТРАНЕ, ОТКАЗАВШИСЬ ОТ ПОИСКА НОВЫХ КЛИЕНТОВ И ОГРАНИЧИВАЯ ДЕЯТЕЛЬНОСТЬ ОБСЛУЖИВАНИЕМ СУЩЕСТВУЮЩИХ КЛИЕНТОВ».

После того, как информация о проекте была независимо друг от друга опубликована новостным агентством Bloomberg и организацией Privacy International, а так же в связи с нарастающим давлением со стороны гражданского общества, компания Area SpA в итоге отказалась от реализации проекта. Недавно, в конце апреля 2012 года, президент Обама подписал приказ, предусматривающий санкции против организаций, которые экспортируют ИТ оборудование, позволяющее, «используя бреши в компьютерах или сетях, осуществлять мониторинг или слежение, которые могли бы поддержать или обеспечить серьезные нарушения прав человека» правительствами Сирии и Ирана. Некоторые

2 Vernon Silver (2011). Итальянская фирма заявила о выходе из Сирийского проекта по мониторингу. [В СЕТИ] доступно по ссылке: http://www.bloomberg.com/news/2011-11-28/italian-firm-exits-syrian-monitoring-project-repubblica-says.html [Дата последнего доступа: 15 июля 2012].

не западные страны тоже в разной степени снизили свою активность в регионе. Например, китайская фирма Huawei начала расширять свою и без того огромную долю в иранском телекоммуникационном секторе, после того как западные компании, такие как Nokia Siemens Networks и Ericsson, ушли с рынка после связанных с выборами протестов 2009 года. Компания начала сотрудничество с расположенной в Великобритании компанией Creativity Software, чтобы обеспечить MTN Irancell, 51% которой принадлежит государству, сервисом, позволяющим «операторам сотовой связи 'соответствовать законодательству, предусматривающему легальный перехват', что позволяет полиции получать доступ к содержимому информационных потоков и информации о местоположении пользователей».[3] Двумя годами позже из-за нарастающего беспокойства в США и Европе касательно связей компании Huawei с Ираном, компания заявила, что «добровольно ограничит развитие своего бизнеса в этой стране, отказавшись от поиска новых клиентов и ограничивая деятельность обслуживанием существующих клиентов».[4] Однако важно заметить, что компания не полностью приостановила свою деятельность в Иране, заявив, что «коммуникационные сети, переданные или передаваемые клиентам, продолжат получать необходимый сервис Huawei с тем, чтобы обеспечить связь для граждан Ирана».

Все это мало относится к группам гражданского общества в большинстве центрально-азиатских стран, где мониторинг интернет-трафика и телефонных коммуникаций осуществляется при помощи российской технологии. Более того, Россия имеет куда более развитый ИТ сектор по сравнению с большинством средне-восточных и северо-африканских стран, и российские компании экспортируют эту технологию на территории постсоветской Центральной Азии, где она используется местными службами безопасности для аналогичных целей.[5] Более того, российские технологические компании гораздо менее чувствительны по отношению к негативным публикациям в прессе. Ярким примером является Центр речевых технологий (ЦРТ), расположенная в Санкт`-Петербурге компания, специализирующаяся на экспертизе фонограмм речи и автоматизированном распознавании лиц, которая была занесена в базу данных Spy Files. Spy Files - это база данных компаний, представляющих решения для прослушивания и мониторинга, составленная совместно Wikileaks, Privacy International и Bugged Planet.[6] [7] Когда Сергею Ковалю, главному аналитику в ЦРТ, был задан вопрос о публикации Spy Files, он продемонстрировал абсолютное пренебрежение к потенциальной возможности репрессивного использования этой технологии. «Все эти разговоры о технологии поимки диссидентов – это просто бред собачий! Это типичная попытка психологического воздействия, которую американцы используют против своих конкурентов. Я считаю, что все эти аргументы касательно прав человека являются чистейшим лицемерием. Американцы просто используют их для своих собственных целей.»[8] [цитата в переводе с английского]

> АКТ ПЕРЕХВАТА ТЕЛЕФОННЫХ РАЗГОВОРОВ ОСУЩЕСТВЛЯЕТСЯ МЕСТНЫМИ СЛУЖБАМИ БЕЗОПАСНОСТИ, У КОТОРЫХ, КАК ПРАВИЛО, ЕСТЬ ОФИС В ГЛАВНЫХ ЗДАНИЯХ МЕСТНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ КОМПАНИЙ (ЧТО БЫЛО НЕОДНОКРАТНО ОТМЕЧЕНО В НИЖЕ ПРИВЕДЕННЫХ ДОКУМЕНТАХ О TELIASONERA). ЭТОТ ПЕРЕХВАТ ОСУЩЕСТВЛЯЕТСЯ ПОСРЕДСТВОМ СИСТЕМЫ ДЛЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ (СОРМ) - РОССИЙСКОЙ СИСТЕМЫ, КОТОРАЯ БЫЛА СКОПИРОВАНА ПО ВСЕЙ ЦЕНТРАЛЬНОЙ АЗИИ.

3 Steve Stecklow, Farnaz Fassihi и Loretta Chao (2011). Китайский технический гигант помогает Ирану. [В СЕТИ] доступно по ссылке: http://online.wsj.com/article/SB10001424052970204644504576651503577823210.html. [Дата последнего доступа: 1 июля 2012].

4 Loretta Chao, Steve Stecklow, и Farnaz Fassihi (2011). Huawei собирается снизить активность деятельности в Иране. [В СЕТИ] Доступно по ссылке: http://online.wsj.com/article/SB10001424052970204319004577088001900708704.html. [Дата последнего доступа: 1 июля 2012].

5 Андрей Солдатов и Ирина Бороган (2012). Только бизнес: как российская технология обеспечивает глазами и ушами Больших Братьев мира. [В СЕТИ] Доступно по ссылке: http://www.opendemocracy.net/od-russia/andrei-soldatov-irina-borogan/just-business-how-russian-technology-provides-eyes-and-ears-. [Дата последнего доступа: 1 июня 2012].

6 Оригинальная база данных поддерживается Privacy International, Bugged Planet, и Bureau of Investigative Journalism.

7 Говоря более детально, компания создала технологию, которая может «сохранять миллионы элементов биометрических данных (образцы голоса и фото изображения) и сопоставлять их с конкретными людьми, осуществляя поиск во всех коммуникационных каналах мира (включая видео файлы). Разработанная ими технология распознавания голоса может идентифицировать говорящего независимо от языка, акцента или используемого диалекта (они идентифицируют голоса только по физическим параметрам воспроизводимого звука). У них также есть средства для использования отпечатков пальцев и технологии идентификации человека по особенностям радужной оболочки его глаз).» (Источник: см. сноску 5)

8 См. сноску 5

Несмотря на отрицания со стороны ЦРТ в Москве, именно эту технологию российские службы безопасности используют против политических оппонентов.[9] Налицо наличие множества крепких связей между российским технологическим сектором и Федеральной службой безопасности (ФСБ), преемником старой советской службы КГБ. После развала Советского Союза многие исследователи, работавшие над технологией прослушивания и мониторинга внутри спецслужб перешли в частный сектор, так как «бюджет КГБ на исследования и разработки был урезан до десятой части изначального объема, а отдел Коваля был ликвидирован. И теперь, когда они не могут распределять работу между 40 разными государственными агентствами, как было раньше, у Центра есть много возможностей передавать особо сложную работу независимым подрядчикам. «У нас есть друзья во всех спец. службах, которые всегда готовы помочь», - говорит Коваль.»[10] На этих основаниях российские технологические компании не тревожатся по поводу сотрудничества с местными службами безопасности, а экономические стимулы, похоже, распространяют это равнодушие и в отношении работы в Центральной Азии.

Акт перехвата телефонных разговоров осуществляется местными службами безопасности, у которых, как правило, есть офис в главных зданиях местных телекоммуникационных компаний (что было неоднократно отмечено в ниже приведенных документах о Teliasonera). Этот перехват осуществляется посредством Системы для оперативно-розыскных мероприятий (СОРМ) - российской системы, которая была скопирована по всей Центральной Азии. Изначально разработанная в качестве исследовательского проекта КГБ в середине 1980-х для перехвата разговоров в стационарных телефонных сетях, новые версии системы способны осуществлять целевое прослушивание отдельных лиц во всех разновидностях интернет- и телефонных коммуникаций. Существует три версии системы, работающей в России:

> «СОРМ-1 ПЕРЕХВАТЫВАЕТ ТЕЛЕФОННЫЙ ТРАФИК, ВКЛЮЧАЯ МОБИЛЬНЫЕ СЕТИ, В ТО ВРЕМЯ КАК СОРМ-2 ОТВЕТСТВЕНЕН ЗА ПЕРЕХВАТ ИНТЕРНЕТ-ТРАФИКА, ВКЛЮЧАЯ GPRS. СОГЛАСНО РЕКЛАМНОЙ ИНФОРМАЦИИ, ПУБЛИКУЕМОЙ РАЗРАБОТЧИКАМИ, СОРМ-3 БУДЕТ СПОСОБЕН СОБИРАТЬ ИНФОРМАЦИЮ СО ВСЕХ СРЕДСТВ КОММУНИКАЦИИ И ОБЕСПЕЧИТ ДОЛГОВРЕМЕННОЕ ЕЕ ХРАНЕНИЕ (ТРИ ГОДА), А ТАКЖЕ ОБЕСПЕЧИТ ДОСТУП КО ВСЕМ ДАННЫМ АБОНЕНТОВ. В ДОПОЛНЕНИЕ, СИСТЕМА СОРМ ПОЗВОЛЯЕТ ИСПОЛЬЗОВАТЬ МОБИЛЬНЫЕ КОНТРОЛЬНЫЕ ПУНКТЫ, НАПРИМЕР, НОУТБУК СО СПЕЦИАЛЬНЫМ МОБИЛЬНЫМ БЛОКОМ, КОТОРЫЙ МОЖЕТ БЫТЬ ПОДКЛЮЧЕН НАПРЯМУЮ К КОММУНИКАЦИОННЫМ УЗЛАМ, И НЕМЕДЛЕННО НАЧАТЬ ЗАПИСЬ ТРАФИКА ОПЕРАТОРА. ОДИН ТАКОЙ НОУТБУК ИМЕЕТ ВОЗМОЖНОСТИ ОДНОВРЕМЕННО ПЕРЕХВАТЫВАТЬ ЛИНИИ 1024 АБОНЕНТОВ.»[11]

СОРМ-2 изначально был представлен в Центральной Азии как часть программы, ассоциированной с Министерством внутренних дел (МВД) Российской Федерации, и, согласно конфиденциальным источникам, службы безопасности в этих странах усиленно пытались найти квалифицированный персонал для работы с этим оборудованием,[12] что вызывает подозрение касательно того, кто на самом деле работает с этим оборудованием.

В дополнение к этим продолжительным связям между ФСБ и российским технологическим сектором, есть смысл назвать западные компании, которые развернули серьезную деятельность в этом регионе и частично помогли в организации надзирающего государства. Как было доказано недавно, шведско-финская компания Teliasonera посредством нескольких дочерних и акционерных компаний сотрудничала со службами безопасности в Казахстане, Узбекистане и Таджикистане и оказывала содействие в перехвате телефонных звонков различных

9 Когда openDemocracy Russia связалась с главой филиала ЦРТ в Москве Дмитрием Дырмовским, «он попросил нас не публиковать то, что сказал Коваль. «У Сергея Львовича Коваля нет права представлять компанию и у не было права разговаривать с вами, хотя я не осведомлен о том, что он сказал или не сказал вам», - сказал Дырмовский. Он наотрез отказался показать нам любой продукт ЦРТ, даже из тех коммерческих продуктов, которые открыто рекламируются на веб-сайте компании.» Из источника, указанного в сноске 5

10 См. сноску 5

11 Андрей Солдатов и Ирина Бороган (2012). ИН проекта: «Кто прослушивает российскую оппозицию?». [В СЕТИ] Доступно по ссылке: http://www.opendemocracy.net/od-russia/andrei-soldatov-irina-borogan/project-id-who%E2%80%99s-bugging-russian-opposition. [Дата последнего доступа: 1 июля 2012].

12 В некоторой степени также подтверждается профилем OpenNet Initiative о ситуации с цифровыми правами в Таджикистане. См. Различные авторы (2010). Профили стран: Таджикистан. [В СЕТИ] Доступно по ссылке: http://opennet.net/research/profiles/tajikistan. [Дата последнего доступа: 1 июня 2012].

журналистов и оппозиционных деятелей.[13] Недавно компания стала партнером Датского института по правам человека (DIHR – *Danish Institute for Human Rights*) с целью пересмотреть свои правила в отношении запросов на прослушивание в регионе.[14] Более того, компания стала одним из ведущих членов Диалога о свободе самовыражения и конфиденциальности телекоммуникационной индустрии[15] , а представитель компании даже принял участие в панельной дискуссии о правах в отношении телекоммуникационного сектора на недавнем Форуме интернет-управления в Баку, Азербайджан [16] . Однако и это не особо помогает пользователям региона, на рынке которого доминируют государственные и российские телекоммуникационные компании. В Центральной Азии эти компании постоянно боролись за милость местных авторитарных правителей, таких как Ислам Каримов в Узбекистане и Гурбангулы Бердымухамедов в Туркменистане, и, таким образом, не имеют другого выбора, кроме как сотрудничать с национальными службами безопасности.[17]

# ОБЗОР РОССИЙСКИХ КОМПАНИЙ-ПОСТАВЩИКОВ ТЕХНОЛОГИЙ НАДЗОРА И ИХ КЛИЕНТОВ

Огромное количество компаний, разрабатывающих и продающих решения СОРМ и другие средства слежения и мониторинга являются российскими. Российскими же являются несколько главных региональных телекоммуникационных компаний. Обзор этих компаний даст нам представление о том, какие разновидности технологий эти компании производят и какого типа прослушивание и мониторинг можно ожидать в регионе в ближайшие годы. Краткая таблица, расположенная в приложении к этому докладу, предлагает краткий обзор профилей представленных здесь компаний, их релевантные продукты, а также информацию о том, в каких странах они осуществляли свой бизнес

## УЗБЕКИСТАН

> УЗБЕКСКИЕ ГОСУДАРСТВЕННЫЕ СЛУЖБЫ БЕЗОПАСНОСТИ СПОСОБНЫ ПРОВОДИТЬ ПЕРЕХВАТ ТЕЛЕФОННЫХ КОММУНИКАЦИЙ, ОСУЩЕСТВЛЯЕМЫХ ПОСРЕДСТВОМ СТАЦИОНАРНЫХ ТЕЛЕФОНОВ; ПРОСМАТРИВАТЬ ИНТЕРНЕТ-ТРАФИК, СЛАБОСТРУКТУРИРОВАННЫЕ ДАННЫЕ, ТАКИЕ КАК SMS, MMS И ПОСТЫ НА ФОРУМАХ; А ТАКЖЕ ОСУЩЕСТВЛЯТЬ АВТОМАТИЗИРОВАННОЕ РАСПОЗНАВАНИЕ ГОЛОСА И ЛИЦ. У НИХ ТАКЖЕ ЕСТЬ НЕКОТОРЫЕ ВОЗМОЖНОСТИ СЛЕЖЕНИЯ ЗА МОБИЛЬНЫМИ КОММУНИКАЦИЯМИ.

Государственные службы безопасности в Узбекистане имеют доступ ко множеству компаний-источников

13 Uppdrag Granskning (2012). «Как Teliasonera продается диктатурам | Uppdrag Granskning: Черные Ящики | Расследовательная Миссия». [В СЕТИ] Доступно по ссылке: http://vimeo.com/41248885. [Дата последнего доступа: 1 июля 2012].

14 Katrina Kaiser (2012). «На этой неделе в интернет-цензуре: расширение антибогохульных законов в Саудовской Аравии, депортация активистов из ОАЭ, китайские видео сайты будут проходить предварительную цензуру и шведская TeliaSonera представит обзор прав человека». [В СЕТИ] Доступно по ссылке: https://www.eff.org/deeplinks/2012/07/week-internet-censorship-china-saudi-arabia-sweden-UAE. [Дата последнего доступа: 1 августа 2012].

15 Teliasonera (2012). «Диалог телекоммуникационной индустрии отбирает пять принимающих организаций в качестве потенциальных адресов». [В СЕТИ] Доступно по ссылке: http://www.teliasonera.com/en/newsroom/news/2012/telecommunications-industry-dialogue-selects-five-host-organisations-as-potential-addresses/.

16 Access (2012). IGF 2012 Предложение для воркшопа :: (No: 98) План для уважающих права телекоммуникационных компаний. [В СЕТИ] Доступно по ссылке: http://www.intgovforum.org/cms/mag/116-workshop-proposals/1034-igf-2012-workshop-proposal-no-98-a-plan-for-rights-respecting-telecoms. [Дата последнего доступа: 1 августа 2012].

17 Joanna Lillis (2012). «Узбекистан: Липкие пальцы Ташкента портят аппетиты иностранных инвесторов». [В СЕТИ] Доступно по ссылке: http://www.eurasianet.org/node/65735. [Дата последнего доступа: 15 августа 2012]. Мария Киселёва (2012). «ОБНОВЛЕНИЕ 1-российский мобильный оператор МТС возвращается в Туркменистан». [В СЕТИ] Доступно по ссылке: http://www.reuters.com/article/2012/07/26/mts-turkmenistan-idUSL6E8IQJSV20120726. [Дата последнего доступа: 30 июля 2012].

компонентов СОРМ, и похоже, что в республике осуществляют деятельность компании, предоставляющие программное обеспечение для перехвата и анализа звуковых сигналов и мониторинга мобильных сетей. Российская компания МФИ-Софт, имеющая офисы в Нижнем Новгороде и Москве, производит полнофункциональные пакеты всех трех версий СОРМ, включая СОРМ-2 или «СОРМович». Система СОРМович, согласно информации, указанной на сайте МФИ-Софт, разработана для неограниченного масштабирования для сетей любого размера. Несколько удаленных узлов перехвата могут быть подключены к этой системе, обеспечивая возможность предоставления информации об одной сети нескольким агентствам безопасности.[18] МФИ-Софт экспортировала это оборудование в Центральную Азию через посредника, компанию ALOE Systems,[19] передав его государственной структуре Узбекистана УЗБЕКТЕЛЕКОМ.[20] Кроме того, компания ALOE Systems продает СОРМ-3 клиентам, находящимся вне региона, под названием Netbeholder из своих офисов в Торонто, Канада.

Другой российской компанией, предлагающей аналогичное оборудование для электронного перехвата является ПРОТЕЙ, ранее подразделение Ленинградского отраслевого научно-исследовательского института связи (ЛОНИИС), позднее переданное Российскому министерству связи, а в 2002 году ставшее независимой компанией. Несмотря на отрицания со стороны менеджмента ПРОТЕЙ, аналогичные ранее упомянутым высказываниям главы ЦРТ в Москве,[21] ПРОТЕЙ реализует несколько компонентов СОРМ, а также платформу Deep Packet Inspection (DPI).[22] DPI от компании ПРОТЕЙ - это «платформа для управления трафиком с возможностью глубокой проверки пакетов, что позволяет эффективно управлять утилизацией сетевых ресурсов и предоставлять новые полезные сервисы. Главными функциями ПРОТЕЙ DPI являются: динамическое применение политики обслуживания, учет трафика и представление дополнительных услуг».[23]

На нетехническом языке, DPI платформа способна осуществлять мониторинг сетевого трафика и постоянно обновлять разновидности трафика, которые она блокирует или записывает вплоть до конкретных веб-страниц и сервисов (таких как Skype и службы обмена мгновенными сообщениями). У компании есть контракты с Узбекистаном.[24]

Системы электронного перехвата и анализа являются не единственными продуктами, предоставляемыми российскими компаниями, которые вызывают опасения. Компания Оксиджен Форенсикс и его учредитель, компания Оксиджен Софтвер так же вошли в базу данных Spy Files. Оксиджен Форенсикс продает пакеты инструментов для мобильной криминалистики, которые органы юстиции могут использовать для получения практически любой информации, сохраненной на конфискованных телефонах.[25] Один из торговых посредников Оксиджен, компания Softline, имеет представительства во всех обсуждаемых здесь странах, включая четыре офиса в одном только Казахстане.[26]

---

18 МФИ-Софт (2012). СОРМ2 | МФИ СОФТ. [В СЕТИ] Доступно по ссылке: http://www.mfisoft.ru/products/sorm/sorm2/sormovich. [Дата последнего доступа: 15 июля 2012]. И ресурс, указанный в сноске 11.

19 См. сноску 5

20 ALOE Systems (2012). Clients | ALOE Systems VoIP Softswitch Solutions. [В СЕТИ] Доступно по ссылке: http://www.aloe-systems.com/company/clients#cis. [Дата последнего доступа: 10 декабря 2012].

21 Когда генеральному директору компании ПРОТЕЙ был задан вопрос о включении его компании в базу данных Spy Files, он сказал: «Мне не важно… Мы работаем с мобильными сетями во многих странах; видимо, так они о нас узнали. Я не уделяю этому особого внимания, потому что подобные вещи меня не волнуют. На самом деле, мы не продаем такого рода технологию: прослушивающие устройства и тому подобное. Более того, мы не являемся единственной компанией, производящей такие приложения для мобильных устройств». Из источника, указанного в сноске 5. В любом случае, представители ПРОТЕЙ появились на ISS World trade show, прошедшем в Дубае в 2009 году, где они представили себя в качестве специалистов по законному перехвату (LI – Lawful Interception). В соответствии с информацией об этом событии на их вебсайте, они описали LI решение под названием “Beyond LI”, которое «позволяет системным операторам отслеживать звонки, распознавать паттерны и взаимоотношения между подозреваемыми, идентифицировать потенциальных соучастников и многое другое, все это лишь одним нажатием на кнопку». См. Протей (2012). Телекоммуникационные Решения - ПРОТЕЙ. [В СЕТИ] Доступно по ссылке: http://www.protei.com/events/past/. [Дата последнего доступа: 1 ноября 2012].

22 ПРОТЕЙ (2012). Конвертер СОРМ XSM - Оборудование СОРМ - Обзор - НТЦ ПРОТЕЙ. [В СЕТИ] Доступно по ссылке: http://www.protei.ru/products/xsm/. [Дата последнего доступа: 11 декабря 2012].

23 ПРОТЕЙ (2012). DPI Platform - Traffic Management - Overview - PROTEI. [В СЕТИ] Доступно по ссылке: http://www.protei.com/products/dpi/. [Дата последнего доступа: 11 декабря 2012].

24 См. сноску 5

25 Oxygen Software (2012). The Spy Files - Mobile forensic analysis for smartphones. [В СЕТИ] Доступно по ссылке: http://www.wikileaks.org/spyfiles/docs/oxygen/34_mobile-forensic-analysis-for-smartphones.html. [Дата последнего доступа: 1 августа 2012].

26 Softline (2012). Softline - информация о компании и корпоративная презентация. [В СЕТИ] Доступно по ссылке: http://softline.ru/about. [Дата последнего доступа: 15 июля 2012].

Компания Softline напрямую продает пакеты для судебно-технической экспертизы на сайте Allsoft.uz, узбекской версии вебсайта одной из дочерних компаний.[27] В завершение надо отметить, что согласно документам в базе данных Spy Files, Центр речевых технологий (ЦРТ) - расположенная в Санкт-Петербурге компания, специализирующаяся на экспертизе фонограмм речи, которая была обсуждена в предыдущей части этого документа, также осуществляла деятельность в Узбекистане.[28]

Одним из двух примеров западных компаний, которые, как минимум, пытались экспортировать технологии перехвата и цифровой криминалистики в Центральную Азию, является AccessData – компания, расположенная в городе Линдон, штат Юта. Компания AccessData разработала ряд платформ для цифровой криминалистики, включая линию сетевого мониторинга SilentRunner. Система SilentRunner Mobile, например, «позволяет вам осуществлять мониторинг, записывать, анализировать и графически визуализировать сетевой трафик, чтобы точно видеть, что происходит в вашей сети во время профилактического аудита или киберрасследования.»[29]

Компания AccessData указывает как Softline, так и расположенную в Москве фирму Ester Solutions в качестве своих торговых представителей для России; и в то время как она не предлагает их на январь 2013 года, архивная версия той же страницы показывает, что дочка компании Softline компания Axoft указывает три продукта AccessData – включая SilentRunner – на своем русскоязычном вебсайте.[30] Сайт axoft.uz не поддерживает свой собственный список программных продуктов, переадресовывая запрос в каталог своего российского аналога.[31] Что касается компании Ester Solutions, список её торговых представителей включает несколько региональных телекоммуникационных компаний, с которыми она осуществляла сотрудничество, в том числе МТС и Мегафон.[32] Однако исходя из описаний на сайте Ester Solutions, эти сервисы не имеют отношения к прослушиванию и/или цифровой криминалистике. Никакой информации касательно продажи мобильного криминалистического оборудования в настоящее время не имеется.

Узбекские государственные службы безопасности способны осуществлять перехват телефонных коммуникаций, осуществляемых посредством стационарных телефонов, просматривать интернет-трафик, слабоструктурированные данные, такие как SMS, MMS и посты на форумах, а также осуществлять автоматизированное распознавание голоса и лиц. У них также есть некоторые возможности слежения за мобильными коммуникациями.

## КАЗАХСТАН

ГОСУДАРСТВЕННЫЕ СЛУЖБЫ БЕЗОПАСНОСТИ КАЗАХСТАНА СПОСОБНЫ ОСУЩЕСТВЛЯТЬ ПЕРЕХВАТ ТЕЛЕФОННЫХ КОММУНИКАЦИЙ, ОСУЩЕСТВЛЯЕМЫХ ПОСРЕДСТВОМ СТАЦИОНАРНЫХ ТЕЛЕФОНОВ, ПРОСМАТРИВАТЬ ИНТЕРНЕТ-ТРАФИК, СЛАБОСТРУКТУРИРОВАННЫЕ ДАННЫЕ, ТАКИЕ КАК SMS, MMS И ПОСТЫ НА ФОРУМАХ, А ТАКЖЕ ОСУЩЕСТВЛЯТЬ АВТОМАТИЗИРОВАННОЕ РАСПОЗНАВАНИЕ ГОЛОСА И ЛИЦ. У НИХ ЕСТЬ НЕКОТОРЫЕ ВОЗМОЖНОСТИ СЛЕЖЕНИЯ ЗА МОБИЛЬНЫМИ КОММУНИКАЦИЯМИ, А ТАКЖЕ ПЕРЕДОВЫЕ ПРОГРАММНЫЕ ПРОДУКТЫ ДЛЯ АНАЛИЗА ДАННЫХ.

27 Allsoft (2012). Allsoft - интернет магазин лицензионного софта. [В СЕТИ] Доступно по ссылке: http://allsoft.uz/search_result.php?words=oxygen&p=2. [Дата последнего доступа: 1 декабря 2012]. И Allsoft.kz (2012). Allsoft - интернет магазин лицензионного софта. [В СЕТИ] Доступно по ссылке: http://allsoft.kz/search_result.php?words=oxygen&p=2. [Дата последнего доступа: 1 декабря 2012].

28 Ilya Oparin (2009). Complex Identification Decision Based on Several Independent Speaker Recognition Methods. [В СЕТИ] Доступно по ссылке: http://www.wikileaks.org/spyfiles/files/0/52_200906-ISS-PRG-STC.pdf. [Дата последнего доступа: 1 декабря 2012].

29 AccessData (2012). SilentRunner Mobile Network Forensics Software. [В СЕТИ] Доступно по ссылке: http://accessdata.com/products/digital-forensics/silentrunner-mobile. [Дата последнего доступа: 1 декабря 2012].

30 AccessData (2012). Partners | AccessData. [В СЕТИ] Доступно по ссылке: http://www.accessdata.com/partners/partners. [Дата последнего доступа: 1 декабря 2012]. И европейская секция его списка торговых представителей, а также Axoff (2012). AccessData: обзор. [В сети] Доступно по ссылке: http://web.archive.org/web/20120701144310/http://axoft.ru/software/AccessData/. [Дата последнего доступа: 1 декабря 2012].

31 Axoff.uz (2012). Главная | «Аксофт» — дистрибуция программного обеспечения. [В СЕТИ] Доступно по ссылке: http://axoft.uz/. [Дата последнего доступа: 1 декабря 2012].

32 Ester Solutions (2012). Клиенты. Эстер Солюшнс (Ester Solutions) - Разработка программного обеспечения, управление SIM-картами, системная интеграция, сервисные приложения для мобильных операторов. [В СЕТИ] Доступно по ссылке: http://www.estersolutions.ru/ru/clients/. [Дата последнего доступа 1 декабря 2012].

В Казахстане власти имеют аналогичные возможности СОРМ, что и в Узбекистане. МФИ-Софт через своего посредника ALOE Systems, указывает казахские телекоммуникационные компании Astel OJSC, JSC Nursat, а также на 51% принадлежащий государству КАЗАХТЕЛЕКОМ в числе своих клиентов.[33] ЦРТ, специализирующаяся на экспертизе фонограмм речи и расположенная в Санкт-Петербурге компания, обсуждаемая в разделе «Предыстория», также осуществляла свою деятельность в Казахстане.[34] Оксиджен Софтвер, работающая в области мобильной криминологической экспертизы компания, обсуждаемая в подразделе об Узбекистане, через своего торгового представителя Softline напрямую реализует программный пакет «Мобильный криминалист» через сайт Allsoft.kz, казахская версия вебсайта одной из её дочерних компаний.[35]

СОРМ-3, который покрывает еще более широкий спектр коммуникаций, включая SMS, MMS, форумы, блоги и социальные медиа, также требует серьезных возможностей сохранения и анализа данных.[36] Система «Semantic Archive», разработанная расположенной в Москве компанией Аналитические Бизнес Решения (АБР) используется именно для этого.[37] Системы, аналогичные Semantic Archive, разрабатываются для того, чтобы собирать информацию с различных источников в одну базу данных с оптимизированным поиском. Как ФСБ так и КАЗАХТЕЛЕКОМ пользуются этой системой. Рекламная литература АБР также упоминает несколько важных телекоммуникационных компаний в регионе, таких как МТС и бренд ВымпелКома «Билайн».[38] К аналогичным продуктам можно отнести систему «Xfiles», разработанную российской компанией i-Teco, которая указывает Министерство юстиции Казахстана, а также несколько региональных телекоммуникационных компаний в качестве своих партнеров.[39]

Государственные службы безопасности Казахстана способны осуществлять перехват телефонных коммуникаций, осуществляемых посредством стационарных телефонов, просматривать интернет-трафик, слабоструктурированные данные, такие как SMS, MMS и посты на форумах, а также осуществлять автоматизированное распознавание голоса и лиц. У них есть некоторые возможности слежения за мобильными коммуникациями, а также передовые программные продукты для анализа данных.

## ТАДЖИКИСТАН

> ГОСУДАРСТВЕННЫЕ СЛУЖБЫ БЕЗОПАСНОСТИ ТАДЖИКИСТАНА СПОСОБНЫ ОСУЩЕСТВЛЯТЬ ПЕРЕХВАТ ТЕЛЕФОННЫХ КОММУНИКАЦИЙ, ОСУЩЕСТВЛЯЕМЫХ ПОСРЕДСТВОМ СТАЦИОНАРНЫХ ТЕЛЕФОНОВ, ПРОСМАТРИВАТЬ ИНТЕРНЕТ-ТРАФИК, И, ВОЗМОЖНО, СЛАБОСТРУКТУРИРОВАННЫЕ ДАННЫЕ, ТАКИЕ КАК SMS, MMS И ПОСТЫ НА ФОРУМАХ.

Гораздо меньшее число компаний предоставляет компоненты СОРМ в Таджикистане. МФИ-Софт и ПРОТЕЙ (обе компании уже были описаны выше в разделе «Узбекистан») осуществляли свою деятельность в этой стране. ALOE Systems, посредник компании МФИ-Софт, указывает таджикскую дочку мультинациональной телекоммуникационной компании Билайн в числе своих клиентов.[40] ПРОТЕЙ также указывает таджикскую дочку российской телекоммуникационной компании Мегафон в числе своих клиентов.[41]

33 См. сноску 20

34 См. сноску 28

35 См. сноску 27

36 МФИ-Софт (2012). СОРМ3 | МФИ Софт. [В СЕТИ] Доступно по ссылке: http://www.mfisoft.ru/products/sorm/sorm3/yanvar. [Дата последнего доступа: 1 декабря 2012].

37 См. сноску 8, а также Андрей Солдатов и Ирина Бороган (2012). Технология прослушивания российского государства. [В СЕТИ] Доступно по ссылке: http://www.opendemocracy.net/od-russia/andrei-soldatov-irina-borogan/russian-state-and-surveillance-technology. [Дата последнего доступа: 1 ноября 2012].

38 Денис Шатров, Виталий Кузин и Евгений Чубров (2011). Например, Тренинг и сертификация. [В СЕТИ] Доступно по ссылке: http://www.slideshare.net/lp1009/abs-invest. [Дата последнего доступа: 1 декабря 2012].

39 i-Teco (2012). “i-Teco”. [В СЕТИ] Доступно по ссылке: http://www.i-teco.ru/company_eng.html. [Дата последнего доступа: 1 августа 2012].

40 См. сноску 20

41 ПРОТЕИ (2012). Телекоммуникационные Решения - ПРОТЕИ. [В СЕТИ] Доступно по ссылке: http://www.protei.com/company/customers/. [Дата последнего доступа:15 августа 2012].

## ТУРКМЕНИСТАН

ГОСУДАРСТВЕННЫЕ СЛУЖБЫ БЕЗОПАСНОСТИ ТУРКМЕНИСТАНА ИМЕЮТ ВОЗМОЖНОСТЬ ОСУЩЕСТВЛЯТЬ АВТОМАТИЗИРОВАННОЕ РАСПОЗНАВАНИЕ ГОЛОСА И ЛИЦ, А ТАКЖЕ ПРИОБРЕЛИ КАК МИНИМУМ ДЕМО-ВЕРСИЮ МОБИЛЬНОЙ ПЛАТФОРМЫ ДЛЯ ПЕРЕХВАТА И МОНИТОРИНГА КОМПАНИИ GAMMA INTERNATIONAL.

Центр речевых технологий (ЦРТ) - специализирующаяся на экспертизе фонограмм речи и расположенная в Санкт-Петербурге компания, обсуждаемая в разделе «Предыстория», также осуществляла свою деятельность в Туркменистане [42]Кроме того, британо-германская компания Gamma International экспортировала как минимум демо-версию своего мобильного программного обеспечения в Туркменистан. В соответствии с документами, полученными немецкой новостной программой ZAPP,[43] компания Gamma в сотрудничестве со швейцарской компанией Dreamlab AG пыталась заключить контракт с туркменскими властями. FinSpy Mobile – это система перехвата, разработанная компанией Gamma, которая позволяет отслеживать деятельность отдельных пользователей посредством методов, аналогичных используемым традиционными вредоносными программами. С помощью специального оборудования, установленного в серверной Интернет провайдера, к которому подключен пользователь, ему предлагается установить якобы стандартное обновление на часто используемое мобильное или компьютерное приложение (например, iTunes), но это «обновление» на самом деле является программой, которая передает все разновидности внешней коммуникации, включая данные с установленного микрофона и камеры, на сервер управления и контроля, принадлежащий осуществляющему перехват агентству. Эта система обходит абсолютно все средства обеспечения безопасности, включая все разновидности шифрования. Когда образцы мобильного шпионского программного обеспечения были проанализированы экспертами в области безопасности из Гражданской лаборатории университета Торонто, сканирование публичного Интернета на наличие серверов управления и контроля выявило систему на IP-адресе, ассоциированном с Министерством связи Туркменистана.[44]

Реакция гражданского общества на это открытие была благотворной, но это лишь один случай из широкого спектра проблем, связанного с контролем западного экспорта в Центральную Азию. Юридический отдел Казначейства Великобритании (*Treasury Solicitor*) опубликовал заявление, в котором FinSpy рассматривается в качестве «технологии двойного применения» и, таким образом, является предметом экспортного контроля Европейского Союза. В результате компания Gamma должна подать прошение на выдачу лицензии для продажи FinSpy вне Европейского Союза. Время покажет, как это решение будет приведено в исполнение, будет ли требование лицензии иметь обратную силу, и подавала ли изначально компания Gamma прошение на выдачу лицензии для экспорта FinSpy в Туркменистан. Также непонятно, как Gamma может попробовать обойти эти ограничения.[45]

## ОБЩИЕ ТЕНДЕНЦИИ

Помимо картографического упорядочивания компаний по конкретным странам, на территории всего региона наблюдаются более общие тенденции, которые заслуживают дальнейшего обсуждения, в особенности это касается связей между российскими компаниями-экспортерами технологий перехвата и российскими спецслужбами, а также проблем отслеживания поставок компаний через посредников до конечных клиентов.

Например, компания МФИ-Софт имеет тесные связи с российскими службами безопасности. Президент компании Александр Иванов был заместителем министра связи, ответственным за спутниковую и радио связь в Советском Союзе с 1989 до 1992 года, и впоследствии несколько лет служил в Вооруженных Силах России.[46] После основания компании

42 См. сноску 28

43 ZAPP (2012). Немецкие шпионские программы для диктаторов. [В СЕТИ] Доступно по ссылке: http://www.ndr.de/fernsehen/sendungen/zapp/media/zapp4923.html. [Дата последнего доступа: 1 декабря 2012].

44 Morgan Marquis-Boire, Bill Marczak и Claudio Guarnieri (2012). Смартфон любивший меня: FinFisher становится мобильным?. [В СЕТИ] Доступно по ссылке: https://citizenlab.org/wp-content/uploads/2012/08/11-2012-thesmartphonewholovedme.pdf. [Дата последнего доступа: 1 сентября 2012].

45 Privacy International (2012). Британское правительство признает, что начинает контролировать экспорт FinSpy от Gamma International. [В СЕТИ] Доступно по ссылке: https://www.privacyinternational.org/press-releases/british-government-admits-it-has-already-started-controlling-exports-of-gamma. [Дата последнего доступа: 1 октября 2012].

46 МФИ-Софт (2012). Руководство | МФИ Софт. [В СЕТИ] Доступно по ссылке: http://www.mfisoft.ru/about/managment. [Дата последнего доступа: 1 декабря 2012].

в 2007 году Иванов заявил, что «мы не отрицаем и не видим ничего плохого в использовании административных ресурсов, [и] связях с федеральными агентствами и организациями», упомянув при этом ФСБ.[47]

> В СВЯЗИ С НАЛИЧИЕМ ЭТИХ КРЕПКИХ СВЯЗЕЙ, НЕКОТОРЫЕ ОБСУЖДЕННЫЕ ЗДЕСЬ СТРАНЫ НЕ СПЕШИЛИ ПОЛАГАТЬСЯ ИСКЛЮЧИТЕЛЬНО НА РОССИЙСКУЮ ТЕХНОЛОГИЮ. НАПРИМЕР, СОГЛАСНО КОНФИДЕНЦИАЛЬНЫМ ИСТОЧНИКАМ, ОПРОШЕННЫМ В РАМКАХ ДАННОГО ИССЛЕДОВАНИЯ, СЛУЖБА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ КАЗАХСТАНА НЕ ИСПОЛЬЗУЕТ КОМПОНЕНТ СЕМАНТИЧЕСКОЙ БАЗЫ ДАННЫХ СИСТЕМЫ СОРМ-3, А ВМЕСТО ЭТОГО, ПОДОЗРЕВАЯ НАЛИЧИЕ В СИСТЕМЕ РОССИЙСКИХ ЧЕРНЫХ ХОДОВ, РАЗРАБОТАЛА СОБСТВЕННЫЕ АНАЛОГИ ЭТОГО КОМПОНЕНТА. СТОИТ ТАКЖЕ ОТМЕТИТЬ, ЧТО ГРУППЫ ГРАЖДАНСКОГО ОБЩЕСТВА В КИРГИЗСТАНЕ ВЫРАЖАЛИ АНАЛОГИЧНЫЕ ОПАСЕНИЯ КАСАТЕЛЬНО ИСПОЛЬЗОВАНИЯ ЭТОЙ СИСТЕМЫ В ИХ СТРАНЕ.[48]

В завершении хочется отметить, что это все, что нам удалось узнать о глобальной индустрии перехвата из вики-сайтов таких компаний-поставщиков данной технологии, как BuggedPlanet, Blue Cabinet и Spy Files. По причине громадности глобальной сети дистрибьюторов и посредников, занимающихся продажей программного обеспечения, незначительную часть которой удалось осветить в этом отчете, а также из-за мультинациональной природы телекоммуникационных компаний иногда, полагаясь только на такие вики-сайты, совершенно не ясно, куда экспортируются продукты отдельно взятой компании. Находить связи между компаниями разработчиками и посредниками, которые распространяют продукты до конечных пользователей, независимо от того, являются они телекоммуникационными компаниями, устанавливающими оборудование электронного перехвата, или службами безопасности, покупающими программное обеспечение для цифровой криминалистики, это всегда сложная задача, даже при наличии огромного количества открытых источников, доступных в настоящее время.

# В НАПРАВЛЕНИИ ПЛАНА ДЕЙСТВИЙ

Постсоветская Центральная Азия является одним из наиболее запущенных регионов в глобальном движении за свободный, безопасный и открытый Интернет, где право на конфиденциальность общепринято. Кажущийся недостаток возможностей и союзников в отношении технологии перехвата в регионе – это симптом более широкой проблемы, которая выходит за рамки одного этого вопроса: недостаточное участие международного сообщества за свободный Интернет в том, что несколько групп гражданского общества независимо осуществляют деятельность в регионе. Однако есть несколько общих стратегий, которые группы гражданского общества в регионе и вне его границ могут реализовывать, чтобы противостоять использованию технологий перехвата для слежения за диссидентами и журналистами. *В то же время автор хотел бы отметить, что простых решений для этой проблемы не существует. Автор оставляет конкретизацию обсуждаемой здесь темы за будущими работами.*

## 1. ЗАПАДНОЕ «КЛЕЙМИТЬ И ПОЗОРИТЬ

Мультинациональный характер нескольких из называемых компаний может определить выгодный пункт оказания давления для активистов за цифровые права посредством лоббирования через акционеров и инвесторов или через публичные кампании и правительственные санкции. Нет никакой пользы в том, что ЦРТ имеет полностью принадлежащие ему дочерние компании в США, Германии и Мексике. С другой стороны российское правительство предпринимало попытки привлечь иностранные инвестиции в технологический сектор. В то время как инвестиции в поддерживаемый правительством технологический парк Сколково, расположенный вне Москвы, были сконцентрированы на не относящихся к данному вопросу компаниях, таких как Яндекс и Mail.ru, более глубокая исследовательская работа необходима с целью определения западных инвесторов, являющихся партнерами каких-либо из компаний, упомянутых

47 Инна Ерохина и Александр Малахов (2007). Экс-глава Госкомсвязи решил торговать коммутаторами. [В СЕТИ] Доступно по ссылке: http://www.kommersant.ru/doc/751197. [Дата последнего доступа: 10 октября 2012].

48 Не доступен (2012). Киргизстан: Бишкек следит, используя российское программное обеспечение. [В СЕТИ] Доступно по ссылке: http://www.eurasianet.org/node/66150. [Дата последнего доступа: 8 ноября 2012].

в этом документе.[49] МФИ-Софт имеет офис в Сколково,[50] также как и ответвление ЦРТ.[51] Некоторые сообщения в прессе вокруг Сколково и иностранных инвестиций в российский ИТ сектор в целом информируют о том, что инвесторы уже сейчас имеют опасения, связанные с коррупцией в экономике России. Негативные отзывы в прессе касательно компаний, с которыми они сотрудничают, могут быть особенно эффективным стимулом для ухода инвесторов. Конечно, эта стратегия представляет собой потенциальную проблему ответной реакции. Если западная инвестиционная фирма закончит свое партнерство с российским разработчиком технологий перехвата, российская фирма может занять её место.

## 2. МЕЖДУНАРОДНЫЕ КАМПАНИИ.

Есть ограниченное число возможностей в том, что касается обращения внимания на нарушения прав человека в этой сфере на международном уровне. Франк Ла Ру, Специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их свободное выражение, уже делал заявления на тему угроз свободе слова в Интернете. В его докладе речь идет непосредственно об угрозах конфиденциальности со ссылкой на 12 Статью Всеобщей декларации прав человека (ВДПЧ) и 17 Статью Международного пакта о гражданских и политических правах (МПГПП).[52] Процедура оформления жалоб через офис Докладчика может в некоторых случаях оказаться полезной. Во время последних визитов (требующих приглашения со стороны правительства, которому наносится визит) он тоже упоминал свободу слова в сети (лучшим примером является визит в Южную Корею два года назад), но ни одна из рассматриваемых стран не входила в список его последних визитов. Как Access уже рекомендовал ранее, если анализ прав на свободу самовыражения и частной жизни в сети будет включен в процесс универсального периодического обзора Совета по правам человека ООН, повышение осведомленности может занять долгое время, так как страны подлежат оценке в ближайшие годы.[53] Представитель ОБСЕ по свободе СМИ, Дуня Миятович, тоже делала много заявлений касательно цифровых прав, особенно в Центральной Азии.[54]

## 3. ПРЯМОЕ ДЕЙСТВИЕ И ТЕОРЕТИЧЕСКИЕ ИССЛЕДОВАНИЯ.

Широкий спектр технической работы необходим, чтобы принять меры по решению проблемы технологии перехвата в Центральной Азии и за её пределами. Можно обнаружить присутствие и работу многих из этих систем перехвата информации с использованием системы Layer8, разработкой которой в настоящее время занимается Freedom House, но больше исследований и разработок необходимо, чтобы эти системы могли быть применены в отношении перехвата информации в необходимом масштабе.

Есть и другие возможности прямого действия, в которые Access никогда не был и не будет напрямую задействован. Например, Коллин Андерсон, независимый исследователь, специализирующийся на вопросах цифровых прав на Среднем Востоке, описал 50Гб лог-файл, полученный группой активистов Telecomix от файлового сервера с плохим уровнем безопасности, принадлежащего Syria Telecom, который позволил получить ценную информацию об использовании систем обеспечения цензуры и мониторинга, разработанной Blue Coat Systems, фирмой специализирующейся на веб-безопасности и расположенной в Силиконовой долине.[55] Автор спешит добавить, что ни он, ни Access не поддерживают попытки компрометации служб безопасности в любой центрально-азиатской стране, но это не одобрение подобных действий сказать, что полученная от аналогичных агентств информация была полезна для групп гражданского общества.

---

49 The Economist (2012). Россия пытается создать новую Силиконовую Долину. [В СЕТИ] Доступно по ссылке: http://afr.com/p/technology/russia_aims_to_create_new_silicon_A8ANhJkb1zBaV2Aiu16jbP. [Дата последнего доступа: 1 августа 2012].

50 sk.ru (2012). ООО “МФИ Софт”. [В СЕТИ] Доступно по ссылке: http://community.sk.ru/net/1110043/. [Дата последнего доступа: 1 декабря 2012].

51 См. сноску 5

52 UNHRC (2011). Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение, Франк Ла Руе*. [В СЕТИ] Доступно по ссылке: https://s3.amazonaws.com/access.3cdn.net/61561d24e3a5fd6e47_yzm6bno8i.pdf. [Дата последнего доступа: 1 декабря 2012].

53 Peter Micek (2012). Совет по Правам Человека ООН принимает резолюцию, признающую право человека на Интернет. [В СЕТИ] Доступно по ссылке: https://www.accessnow.org/blog/un-human-rights-council-adopts-resolution-affirming-human-rights-on-interne/. [Дата последнего доступа: 1 декабря 2012].

54 OSCE (2012). Представитель ОБСЕ по свободе СМИ призывает Таджикистан разблокировать YouTube и обеспечить свободный поток информации. [В СЕТИ] Доступно по ссылке: http://www.osce.org/fom/92477. [Дата последнего доступа: 1 августа 2012].

55 Collin Anderson (2012). BlueCoat и Сирия: Индикаторы и вина. [В СЕТИ] Доступно по ссылке: http://b.averysmallbird.com/entries/bluecoat-and-syria-indicators-and-culpability. [Дата последнего доступа: 1 декабря 2012].

## 4. ПОВЫШЕНИЕ ПОТЕНЦИАЛА И ОБУЧЕНИЕ В ОБЛАСТИ БЕЗОПАСНОСТИ.

Из дискуссий с организациями гражданского общества, представляющих собой пользователей с самым большим уровнем риска в мире, организации Access стало известно, что есть общая потребность в повышении потенциала и обучении использованию инструментов для обеспечения безопасных и конфиденциальных коммуникаций (например, шифрование коммуникаций по телефону и текстовых сообщений, а также безопасные клиенты служб мгновенного обмена сообщениями). Пользователи должны понимать угрозы и риски в условиях, где существует всеобъемлющий перехват электронных коммуникаций, и знать о том, как снизить эти риски.

## 5. ДАЛЬНЕЙШАЯ ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА.

Одной из главных причин, по которой предметом данного документа являются российские компании – это огромное количество открытых источников об их работе в регионе. Согласно конфиденциальным источникам информации, роль западных, израильских и китайских компаний может быть такой же или даже еще более важной. Обратите внимание на тот факт, что опубликованная Wikileaks секретная информация посольства США в Ашхабаде, Туркменистан, датированная июлем 2009 года, описывает Siemens AG как «как сообщается… главный поставщик оборудования для перехвата для туркменских спецслужб». Эта информация была обнародована спустя четыре месяца после того, как Siemens зарегистрировала Trovicor GmbH, дочернее подразделение, специализирующееся на мониторинге и легальном перехвате.[56] Возможно Trovicor продолжает обслуживание этого оборудования, но по сведениям автора это еще не было открыто доказано. Что касается китайских компаний, и Huawei, и ZTE осуществляли серьезную деятельность в Таджикистане, Туркменистане и Узбекистане. Принимая во внимание случай с Huawei в Иране, коротко описанный в начале этого документа, велика вероятность того, что эти компании также продавали технологии двойного применения в этом регионе. Однако нам не удалось найти какие-нибудь публичные или конфиденциальные источники, предоставляющие убедительные доказательства связи между этими компаниями и технологиями перехвата в данном регионе.[57]

## 6. СБАЛАНСИРОВАННАЯ ЗАКОННАЯ ПОЛИТИКА ПЕРЕХВАТА.

Важно отметить, что у всех технологий, обсуждаемых здесь, есть абсолютно легальное применение. Ничего в этом документе не должно истолковываться в качестве осуждения общей практики легального перехвата до тех пор, пока этот перехват действительно легальный и осуществляется в соответствии с международными нормами, обеспечивающими базовые права человека на конфиденциальность и надлежащую правовую процедуру. Однако, принимая во внимание хронически плохую историю в отношении обеспечения прав человека в трех из четырех описанных здесь стран и господство исполнительной власти, любая реальная реформа их правовой и регуляторной системы в ближайшем будущем вряд ли принесет положительные изменения. Единственное возможное исключение это Таджикистан, имеющий не только наиболее жизнеспособное гражданское общество из всех этих четырех стран, но и Гражданскую инициативу политики Интернет - местную группу по защите цифровых прав, расположенную в Душанбе. Серьезная попытка создания политики легитимного перехвата в этой стране может быть практической возможностью, и, возможно, она наиболее необходима, принимая во внимание нарастающую сложность ситуации, с которой сталкиваются местные НПО.[58] Актуальный черновой вариант Международных принципов по перехвату и мониторингу коммуникаций и правам человека, являющийся развивающейся основой для сбалансированной законной политики перехвата, может быть хорошим началом в данной ситуации.[59]

56 Vernon Silver и Ben Elgin (2011). Пытки в Бахрейне становятся рутиной с помощью Nokia Siemens. [В СЕТИ] Доступно по ссылке: http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html. [Дата последнего доступа: 1 Ноября 2012].

57 Deirdre Tynan (2012). Центральная Азия: Китайские телекоммуникационные компании выполняют роль ушей для центрально-азиатских деспотов?. [В СЕТИ] Доступно по ссылке: http://www.eurasianet.org/node/65008. [Дата последнего доступа: 1 Сентября 2012].

58 Eurasianet.org (2012). Таджикистан: НПО становится жарко зимой. [В СЕТИ] Доступно по ссылке: http://www.eurasianet.org/node/66177. [Дата последнего доступа: 15 Ноября 2012].

59 См. http://necessaryandproportionate.net и Raegan MacDonald (2012). Тенденции: рост запросов на «законный доступ» создает вызовы для прав пользователей. [В СЕТИ] Доступно по ссылке: https://www.accessnow.org/blog/2012/11/28/lawful-access-challenge-for-rights. [Дата последнего доступа: 1 декабря 2012].

## 7. ЗАМЕТКА О САНКЦИЯХ, КОНТРОЛЕ ЭКСПОРТА И ОТЧЕТНОСТИ.

Случай с FinSpy в Туркменистане – это позитивный пример использования экспортного контроля по отношению к оборудованию перехвата в Центральной Азии. Более того, есть движение, отчасти направляемое членом Европейского Парламента от Нидерландов Мариетӧттой Шааке, требующее от Европейской Комиссии «предоставлять регулярно обновляемый список продуктов ограниченного экспорта и стран, куда они экспортируются».[60] Однако аналогичные попытки в США, скорее всего, оказались бы гораздо менее эффективными, принимая во внимание тот факт, что Казахстан, Узбекистан и Таджикистан находятся на Северной сети поставок (ССП), важнейшем пути поставок для обеспечения операций в Афганистане, в дополнение в Ашхабаде находится важная станция дозаправки.[61] В любом случае любые западные санкции могут потенциально сместить спрос в сторону российских, описанных здесь, или китайских компаний, которые могли в прошлом или могут в будущем осуществлять деятельность в регионе. Важно отметить, что Китай не подписал Вассенарское соглашение, одно из немногих международных соглашений, связанных с экспортом так называемых технологий «двойного применения». И все же некоторые люди утверждают, что группы в поддержку цифровых прав имеют моральный императив для призыва к более серьезным санкциям.

## 8. ЛЕГАЛЬНЫЕ МЕРЫ ПРОТИВ КОМПАНИЙ РАЗРАБОТЧИКОВ ТЕХНОЛОГИЙ ПЕРЕХВАТА.

Все эти компании имеют как минимум некоторое понимание того, куда продают свои продукты, что относится и к компании AccessData. Возбуждение уголовных дел по отношению к этим компаниям обсуждается редко, но в потенциале может оказаться очень полезным средством привлечения общественного внимания к тому, где такие технологии применяются и на кого они влияют.

ОДНАКО, ПРИНИМАЯ ВО ВНИМАНИЕ ХРОНИЧЕСКИ ПЛОХУЮ ИСТОРИЮ В ОТНОШЕНИИ ОБЕСПЕЧЕНИЯ ПРАВ ЧЕЛОВЕКА В ТРЕХ ИЗ ЧЕТЫРЕХ ОПИСАННЫХ ЗДЕСЬ СТРАН И ГОСПОДСТВО ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ, ЛЮБАЯ РЕАЛЬНАЯ РЕФОРМА ИХ ПРАВОВОЙ И РЕГУЛЯТОРНОЙ СИСТЕМЫ В БЛИЖАЙШЕМ БУДУЩЕМ ВРЯД ЛИ ПРИНЕСЕТ ПОЛОЖИТЕЛЬНЫЕ ИЗМЕНЕНИЯ. ЕДИНСТВЕННОЕ ВОЗМОЖНОЕ ИСКЛЮЧЕНИЕ ЭТО ТАДЖИКИСТАН, ИМЕЮЩИЙ НЕ ТОЛЬКО НАИБОЛЕЕ ЖИЗНЕСПОСОБНОЕ ГРАЖДАНСКОЕ ОБЩЕСТВО ИЗ ВСЕХ ЭТИХ ЧЕТЫРЕХ СТРАН, НО И ГРАЖДАНСКУЮ ИНИЦИАТИВУ ПОЛИТИКИ ИНТЕРНЕТ - МЕСТНУЮ ГРУППУ ПО ЗАЩИТЕ ЦИФРОВЫХ ПРАВ, РАСПОЛОЖЕННУЮ В ДУШАНБЕ.

60 Leila Nachawati (2012). ЕС ужесточает правила для экспорта технологии перехвата. [В СЕТИ] Доступно по ссылке: http://advocacy.globalvoicesonline.org/2012/11/01/eu-to-tighten-the-rules-on-surveillance-technology-exports/. [Дата последнего доступа: 1 декабря 2012].

61 Ben Piven (2012). Карта: базы США окружают Иран. [В СЕТИ] Доступно по ссылке: http://www.aljazeera.com/indepth/interactive/2012/04/201241713124276729 8.html. [Дата последнего доступа: 1 сентября 2012].

# ЗАКЛЮЧЕНИЕ

Борьба за цифровые права в постсоветской Центральной Азии сильно затруднена тем фактом, что множество необходимых технологий, используемых для перехвата онлайн-коммуникаций, доступны от российских компаний, что позволяет обойти широкий спектр успешных тактик, применяемых против западных компаний, экспортирующих аналогичные технологии репрессивным режимам. Разновидности потенциального перехвата в регионе – это широкий спектр от традиционного прослушивания аналоговых коммуникаций до сложных систем мониторинга, поддерживаемых массивными базам данных, разработанными для обработки данных с блогов и социальных сетей. И хотя простых решений нет, есть некоторые потенциальные пути публичной защиты, включая способ «клеймить и позорить» на уровне западных иностранных инвестиций, привлечение внимания к этим нарушениям на международной уровне и, что наиболее важно, сотрудничество на местах с локальными группами гражданского общества. Если недавние победы в области интернет-цензуры могут предоставить какой-то пример, самые успешные кампании в этой области это те, где местные группы находятся «на месте водителя». Когда эти группы в достаточной степени поддержаны словом и делом глобальным цифровым сообществом, мы можем начинать противодействие этой угрозе гражданского общества в слишком игнорируемом регионе бывшего Советского Союза.

# ВЫРАЖЕНИЕ БЛАГОДАРНОСТИ

Автор хотел бы поблагодарить Бретта Соломона и Джохаи Бен-Ави за неоценимый вклад в написание этого документа. Он также благодарит Рафаля Рогожински, Машу Фейгуинову, Эрика Джонсона, Эрика Кинга, Артема Горяинова и Коллин Андерсон за их вклад.

## ПРИЛОЖЕНИЕ: ТАБЛИЦА ПРОФИЛЬНЫХ КОМПАНИЙ

| Название компании | Продукт | Краткое описание | Местоположение | KZ | UZ | TJ | TM |
|---|---|---|---|---|---|---|---|
| МФИ-Софт | Компоненты СОРМ (СОРМ 1, 2 и 3) | Перехват стационарных линий телефонных связи (СОРМ 1), интернет-трафика (СОРМ 2) и слабоструктурированных данных, таких как SMS, MMS и постов на форумах, с долгосрочным хранением, а также оборудование для удаленного управления (СОРМ 3) | Нижний Новгород / Москва, Российская Федерация | X | X | X | |
| Центр речевых технологий (ЦРТ) | Аудио криминология / Биометрическое распознавание | Распознавание голоса и лица, автоматизированное распознавание, основанное на других биометрических данных (таких как отпечатки пальцев) | Санкт-Петербург, Российская Федерация | X | X | | X |
| ПРОТЕЙ | Компоненты СОРМ | См. МФИ-Софт | Санкт-Петербург, Российская Федерация (Средний Восток /Северо-Африканское отделение в Аммане, Иордания) | | X | X | |
| Аналитические бизнес решения (АБР) | Компоненты баз данных для СОРМ-3 | Анализ различных источников информации (посты на форумах, MMS, социальные сети) с целью получения данных и осуществления анализа | Москва, Российская Федерация | X | | | |
| iTeco | Компоненты баз данных для СОРМ-3 | См. АБР | | X | | | |
| AccessData | Технология сетевого мониторинга двойного использования | Может перехватывать сетевой трафик, потенциальное использование в СОРМ 2 или 3 | Линдон, Юта, США | | X | | |
| Gamma International | Шпионское программное обеспечение | Получение данных (включая данные с микрофона и камеры в реальном времени) с используемых целевыми пользователями мобильных телефонов посредством традиционных способов троянского вредоносного программного обеспечения | Андовер, Великобритания | | | | X |
| Оксиджен Софтвер | Мобильная криминалистика | Получение всех данных с конфискованных мобильных телефонов | Москва, Российская Федерация | X | X | | |

*Access - это глобальное движение, в основе которого лежит убеждение в том, что политическая вовлеченность и реализация прав человека в 21-ом веке все больше зависит от доступа к интернету и от других форм технологии.*

*Для получения дополнительной информации, пожалуйста, посетите www.accessnow.org или по электронной почте info@accessnow.org.*