3.

СЪБИРАЙТЕ ВСИЧКО!

Архивът от документи, събран от Едуард Сноудън, беше зашеметяващ и по размер, и по обхват. Дори и като човек, който години беше писал за опасностите от тайното наблюдение, извършвано от САЩ, аз все пак бях искрено смаян от необятността на системата за шпионаж, още повече че всичко очевидно беше извършвано без всякакъв контрол, прозрачност или ограничения.

Хилядите програми за наблюдение, описани от архива, не са били предназначени от прилагащите ги хора изобщо да станат обществено достояние. Много от програмите бяха насочени към американското население, но и десетки страни по целия свят – включително демократични държави, които обикновено се смятат за американски съюзници, като Франция, Бразилия, Индия и Германия – също бяха мишени на безразборното масово шпиониране.

Архивът на Сноудън бе елегантно организиран, но размерът и неговата сложност го правеха изключително труден за обработка. Десетките хиляди документи на АНС в него бяха създадени от почти всяко звено и подразделение в огромната агенция, а също така съдържаше и някои файлове, които бяха тясно свързани с чужди разузнавателни агенции. Документите бяха учудващо актуални: най-вече от 2011 г. и 2012 г., както и много от 2013 г. Имаше дори такива от март

и април на тази година, само няколко месеца преди да се срещнем със Сноудън в Хонконг.

По-голямата част от файловете в архива бяха с гриф „строго секретно“. Повечето от тях бяха маркирани FVEY, което означаваше, че са одобрени за разпространение само за четирите най-близки съюзници в шпионирането на АНС, англоговорящия алианс на „Петте очи“, съставен от Великобритания, Канада, Австралия и Нова Зеландия. Други бяха предназначени само за САЩ и с гриф NOFORN, тоест *no foreign distribution* (да не се разпространяват извън страната). Някои документи – като например съдебната заповед по FISA, която позволяваше събирането на телефонни записи, и президентската директива на Обама за подготвяне на офанзивни кибератаки, бяха сред най-внимателно пазените тайни на правителството на САЩ.

Дешифрирането на архива и научаването на жаргона, използван в АНС, ми отне много дни на усилено проучване. Агенцията комуникира със себе си и своите партньори на един особен език, жаргон, който е едновременно бюрократичен и високопарен и все пак от време на време звучи като хвалба и обида едновременно. Повечето от документите освен това бяха доста технически, пълни с неразбираеми акроними и кодови имена, а понякога се изискваше първо да се върна и да прочета други документи, за да ми стане ясно какво пише в този, който съм отворил в момента.

Но Сноудън беше предвидил проблема и ми беше направил полезен глосар със съкращения и имена на програми, както и вътрешните речници на агенцията за специализирани термини. И въпреки това някои от документите бяха неразбираеми при първи, втори или дори трети прочит. Тяхното значение ми стана ясно едва след като бях събрал на едно място различни части от други документи и се бях консултирал с някои от най-изтъкнатите експерти в света по шпионаж, криптография, хакерски атаки, история на АНС, както и по правната рамка, уреждаща американския шпионаж.

Трудността ставаше още по-голяма заради факта, че планините от документи често бяха организирани не по тема, а по клона на агенцията, където са били създадени; драма-

тични разкрития бяха поставени в една папка с огромни количества банални или строго технически материали, които не представляваха особен интерес. Въпреки че „Гардиън“ разработи програма за търсене по ключова дума във файловете, която се оказа от голяма полза, тази програма далеч не беше перфектна. Процесът на „смилане“ на архива беше ужасяващо бавен – много месеци след като за първи път получих документите, някои термини и програми все още изискваха допълнителна работа, за да могат да бъдат публикувани безопасно и разбираемо.

Въпреки тези проблеми обаче файловете на Сноудън безспорно разкриваха сложна мрежа на подслушване и шпионаж, обхващаща както американци (които са изрично извън мандата на АНС), така и не-американци. Архивът разкриваше техническите средства, използвани за прихващане на комуникациите: подслушване на интернет сървъри, сателити, подводни оптични кабели, местни и чуждестранни телефонни системи и дори персонални компютри. В документите се посочваха хората, срещу които са насочени тези изключително агресивни форми на шпионаж: списъкът включваше от предполагаеми терористи и заподозрени в престъпления до демократично избрани лидери на съюзнически държави и дори обикновени американски граждани. Освен това те хвърляха светлина върху общите стратегии и цели на АНС.

Сноудън беше поставил най-критичните, най-всеобхватни документи на видно място в архива и ги беше маркирал като особено важни. Тези файлове показваха в какъв мащаб е работила агенцията, както и измамата и дори престъпните похвати, с които е действала. Програмата BOUNDLESS INFORMANT беше едно от първите разкрития. Тя показваше, че АНС с математическа точност „брои“ всички телефонни разговори и имейли, събирани всеки ден от цял свят. Сноудън беше поставил тези файлове на видно място не само защото те показваха в количествено изражение разговорите и имейлите, събрани и съхранявани от АНС – буквално милиарди всеки ден, – но също и защото те доказваха, че шефът на АНС Кийт Александър и други служители са лъгали пред Конгреса. Нееднократно служители на АНС

твърдяха, че не могат да предоставят конкретни цифри – точно данните, които BOUNDLESS INFORMANT беше създадена да събира.

За периода от един месец, започващ на 8 март 2013 г. например, слайд от презентацията за BOUNDLESS INFORMANT показва, че едно-единствено звено от АНС – „Операции за глобален достъп“, е събрало данни за повече от 3 милиарда телефонни обаждания и имейли, които са преминали през американската телекомуникационна система. (DNR, или *Dialed Number Recognition* – „разпознаване на набрания номер“, се отнася до телефонни разговори; DNI, или *Digital Network Intelligence* – „разузнаване в цифровите мрежи, се отнася до интернет базирани комуникации, например имейли.) Това надхвърляше събирането на данни от системите в Русия, Мексико и почти всички страни в Европа и беше приблизително равно на събирането на данни от Китай.

Като цяло само за трийсет дни звеното беше събрало данни за над 97 милиарда имейли и 124 милиарда телефонни обаждания от цял свят. Друг документ от BOUNDLESS INFORMANT показваше данните от международно шпиониране, събрани в един период от трийсет дни от Германия (500 милиона), Бразилия (2,3 милиарда) и Индия (13,5 милиарда). Други файлове съдържаха колекция от метаданни, събрани в сътрудничество с правителствата на Франция (70 милиона), Испания (60 милиона), Италия (47 милиона), Нидерландия (1,8 милиона), Норвегия (33 милиона) и Дания (23 милиона).

Слайд от презентация за програмата BOUNDLESS INFORMANT

Въпреки законово определените права на АНС да се занимава с „чуждо разузнаване“, документите потвърждаваха, че американското общество е било съвсем равностойна мишена на тайно наблюдение. Това ставаше още по-ясно след прочитане на свръхсекретната заповед, издадена на 25 април 2013 г. от съда по FISA, която задължаваше *Verizon* да предаде на АНС цялата информация за телефонните разговори на американските си клиенти“, „метаданните за телефония“, както бяха наречени. С гриф NOFORN текстът на заповедта бе колкото ясен, толкова и нетърпящ възражение:

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.

Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.

📎* С НАСТОЯЩОТО РАЗПОРЕЖДАМ Отговорникът за записите да представи на Агенцията за национална сигурност (АНС), при връчване на настоящата заповед, и да продължи да предоставя на текущи ежедневни начала след това, за времето, за което настоящата заповед е в сила, освен ако не бъде разпоредено друго от съда, електронни копия от следните материални обекти: всички записи с

*Този символ обозначава превода на предхождащ оригинален документ. – Б. р.

подробни данни за обажданията или „метаданни за телефония“, създадена от *Verizon* за комуникации между (i) Съединените щати и чужбина; или (ii) изцяло в рамките на Съединените щати, включително местни метаданни за телефония, включващи подробна информация за комуникационните маршрути , включително, но не ограничено: идентифициращa информация за сесията (напр. телефонен номер, от който е осъществено набирането, и предназначението на обаждането, номер *International Mobile Subscriber Identity*, или IMSI – международен идентификационен номер на мобилен абонат; номер *International Mobile Equipment Identity*, или IMEI – международен идентификационен номер на мобилно оборудване, и т.н.), идентификатор на магистралата, номер на картата за телефонни разговори, час и продължителност на разговора.

Програмата за масово събиране на телефонни данни е едно от най-значителните разкрития в архива; от нея ставаше ясно съществуването на най-различни тайни програми за шпиониране – от мащабната PRISM (включваща събиране на данни директно от сървърите на най-големите световни интернет компании) и PROJECT BULLRUN, съвместен проект между АНС и британския ѝ аналог – Централа за правителствени комуникации (*Government Communications Headquarters*, GCHQ) за разбиване на най-често използваните форми на криптиране, използвани за предпазване на извършваните онлайн трансакции, до по-малки по мащаб начинания с имена, които отразяват презрителното и склонно към самохвалство чувство за надмощие: EGOTISTICAL GIRAFFE („егоистичен жираф“), чиято цел е браузърът *Tor*, предназначен да осигури анонимност при онлайн сърфиране; MUSCULAR („мускулест“) – средство за влизане в частните мрежи на *Google* и *Yahoo!*; и OLYMPIA, канадската програма за шпиониране на Министерството на мините и енергетиката на Бразилия.

Част от шпионажа поне на пръв поглед бе наистина насочена срещу заподозрени в терористични действия. Но огромни части от програмите очевидно нямаха нищо общо с националната сигурност. Документите не оставяха никакво съмнение, че АНС е била не по-малко заета да извършва икономически шпионаж, дипломатически шпионаж и

всеобщо подслушване без определени подозрения, насочено към цялото население.

Разгледан в своята цялост, в крайна сметка архивът на Сноудън водеше до едно просто заключение: американското правителство е изградило система, която има за цел пълното премахване на личната неприкосновеност в електронната мрежа по целия свят. Това не е хиперболизирано твърдение, а буквалната, изрично посочена цел на шпионската държава: да събира, съхранява, наблюдава и анализира цялата електронна комуникация на всички хора по целия свят. Агенцията има една всеобхватна мисия: да не допусне и един байт електронна комуникация да избегне цедката, създадена от системата.

Този самоналожен „мандат“ изисква на практика безкрайно разширяване на обсега на АНС. Всеки ден АНС полага усилия да идентифицира електронните комуникации, които в момента не се събират и съхраняват, а след това разработва нови технологии и методи да отстрани тази „слабост“. Агенцията не счита, че се нуждае от конкретна обосновка, за да събира определени електронни комуникации, нито поне от подозрения по отношение на своите обекти. Нейната цел е нещо, което АНС нарича „SIGINT“ – разузнаване, обхващащо всички канали. Накрая става така: самият факт, че агенцията има капацитет да събира тези комуникации, се превръща в причина за събирането.