
ВІЙНА
Шейн Гарріс
БИТВИ В КІБЕРПРОСТОРІ

Шейн Гарріс

ВІЙН@
битви в кіберпросторі

Книгу видано за сприяння
Відділу преси, освіти і культури Посольства США в Україні

Shane Harris

@WAR

the rise of the military-Internet complex

Шейн Гарріс

ВІЙН@
битви в кіберпросторі

Переклад з англійської
Олени Замойської

Київ
Ніка-Центр
Львів
Видавництво Анетти Антоненко
2019

УДК 007:316.77:341.326
Г20

Переклад з англійської Олени Замойської

Гарріс Ш.
Г20 ВІЙН@: битви в кіберпросторі / Шейн Гарріс ; пер. з англ. О. Замойської. – Київ : Ніка-Центр ; Львів : Видавництво Анетти Антоненко, 2019. – 296 с.
ISBN 978-966-521-738-1 (Ніка-Центр)
ISBN 978-617-7654-25-3 (Видавництво Анетти Антоненко)

Наші мрії донедавна були пов'язані з міжгалактичними мандрівками та підкоренням космосу, квітами на Марсі й корисними копалинами на Юпітері… А поруч тривала розробка стратегій війн, армії шпигунів (або розвідників) наполегливо полювали на надсекретні дослідження.

Інформаційна революція кінця тисячоліття змінила майже все. Сьогодні шпигунам не потрібно викрадати паперові документи з офісів чи підслуховувати розмови інженерів у кабінетах. Вони навчилися цупити інформацію віддалено, за допомогою комп'ютерних мереж.

Відомий американський журналіст Шейн Гарріс ретельно дослідив етапи розвитку військово-мережевого комплексу США, питання кібершпигунства та стратегій кібервійн – війн майбутнього. Ця книжка стала підсумком його багаторічної роботи.

Новітні технології тепер є буденністю в житті майже кожного з нас. Не варто їх недооцінювати. Інтернет приховує чимало несподіванок, загроз і пасток. Будьте пильними та обережними!

УДК 007:316.77:341.326

ISBN 978-966-521-738-1 (Ніка-Центр)
ISBN 978-617-7654-25-3 (Видавництво Анетти Антоненко)

ЗМІСТ

ВІЙНИ НОВОГО ПОКОЛІННЯ

Науковий прогрес, дедалі розширюючи рамки пізнаваного простору, ставить перед людством складне гносеологічне завдання: звичайної, неспеціальної освіти вже замало, щоб зрозуміти, що відбувається на передньому краї майже будь-якої науки. Епоха енциклопедистів назавжди відійшла у минуле. Люди, чия місія – розширювати горизонт людського пізнання всесвіту, та й будь-якої нової царини науки, вимушено стають «вузькими» спеціалістами: вони вживають спеціальні терміни, користуються інструментарієм, притаманним лише певному роду діяльності. Журналісти, що мають за мету популяризувати досягнення в нових сферах людського життя, модерні ідеї та технології, вимушені перебрати на себе складну, майже нездійсненну функцію: за умов сучасних викликів розповісти загалові ті таємниці, що їх «вузькі» спеціалісти навмисно намагаються якнайретельніше приховати.

На цьому тлі журналістське розслідування, яке провів Шейн Гарріс, а відтак виклав його результати у книжці «Війн@», цікаве, власне, не лише тими фактами, які спромігся зібрати автор, а й солідним забезпеченням їх висновками й доказами, взятими з різних джерел, копіткою роботою з відкритими джерелами інформації, вмінням добути таємні знання – і в прямому, і в переносному розумінні цього слова. Понад десять років Гарріс писав на теми кібербезпеки й електронного шпигунства. Матеріал для цієї книжки – це більше тисячі інтерв'ю, які він збирав роками, розмовляючи з нинішніми і колишніми урядовцями, військовими, керівниками та працівниками корпорацій, експертами, дослідниками й активістами. Перелік посилань, що міститься наприкінці книжки, красномовно свідчить, що робота була проведена титанічна. Але чи не намарно? Чи така вже важлива тема, що так захопила автора й змусила будь-що дошукуватися правди, попри важку працю?

Читаємо у Вікіпедії: «Комп'ютерний вірус (*англ.* computer virus) – комп'ютерна програма, яка має здатність до прихованого самопоши-

рення. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера». Ще в далекому 1988 році 6 тисяч комп'ютерів, підключених до ARPANET, постраждали від «хробака» Морріса. Збитки від цієї вірусної атаки становили 96,5 мільйонів доларів. Утім це були незаплановані наслідки експерименту, над яким утратили контроль, а не якихось зловмисних дій. За тридцять років, що минули від тієї події, змінилися не лише віруси, а й середовище їхнього існування. Автоматизувавши більшість виробничих процесів у промисловості, людство також переклало на комп'ютери керування у більшості інфраструктурних мереж. Захопивши владу над комп'ютером, вірус сьогодні може вивести з ладу не тільки сам комп'ютер, а й керовані ним механізми та мережі. Віруси почали загрожувати найрізноманітнішим галузям, ба навіть цілим країнам.

На наших очах протягом життя одного покоління використання ресурсів мережі для обміну й зберігання надважливих даних як державними установами, так і корпораціями досягло таких обсягів, що проблеми, пов'язані зі втручанням у мережу, здатні привести людство на межу катастрофи. Тож слушно, що на захист кіберпростору постала кіберармія.

Армія – це взагалі особлива царина. Війна і мир, якщо й не зовсім протилежні за своїми принципами, але ніколи не протікають одночасно. Навіть сучасні «гібридні» війни не змушують суспільство перебувати водночас в обох станах, а ділять загал на дві світоглядні страти, які живуть у різних умовах (війни і миру відповідно). Ці частини суспільства в моральній площині жодним чином не пересікаються і навіть не здатні зрозуміти одна одну. Інша річ – армія, професійні військові, яких готовлять діяти зовсім по-різному в мирний і воєнний час. Усі ці особливості притаманні й новоствореній кіберармії. Але поки що оголошувати стан війни в мережі ніхто не квапиться. Тож ми маємо справжню «гібридну» війну у віртуальному світі. Деякі битви цієї війни, досліджені у книжці, дають змогу зрозуміти: це не дитячі забавки – все набагато складніше і небезпечніше. Багато уваги автор приділив юридичним аспектам створення кіберармії в США. Із зрозумілих причин історія створення протидійних армій не ввійшла до книжки, залишивши таку собі інтригу й гарячий інтерес для майбутніх дослідників.

Шейн Гарріс замислив свою книжку не як посібник для фахівців із кібербезпеки, а як захоплюючий шпигунський роман. Доступною пересічній людині мовою він описав перебіг подій в епізодах, зі зрозумілих причин зазвичай прихованих від громадськості. Але й спеціалістам не завадить подивитися на свою діяльність трохи збоку, усвідомити масштаб проблеми й ті критерії, за яким будуть міряти їхню діяльність прийдешні покоління. Врешті-решт, визначити, на чиєму боці вони перебувають у цій війні.

Власне, майже всі головні висновки автор виклав у останньому розділі. Але допитливий і уважний читач, опанувавши один по одному всі розділи книжки, пройшовши за автором всіма звивами його досліджень, напевне, дізнається чимало нового про методи розслідування в такій тонкій і втаємниченій сфері та збагатить своє розуміння кіберпростору. Імовірно, хтось не погодиться з висновками автора, а може, хто зна, піде далі у власних передбаченнях, адже тема війни в кіберпросторі геть зовсім не вичерпана, ця війна розгортається, видозмінюючись і вдосконалюючись, безпосередньо на наших очах.

С. П. Попович, фахівець з інформаційної безпеки

Присвячую моєму чоловікові, Джо де Фео

ЗАУВАГИ ЩОДО ДЖЕРЕЛ

Як журналіст, я понад десять років писав на теми кібербезпеки і електронного шпигунства. Матеріал для цієї книжки – це понад тисяча інтерв'ю, які я збирав роками, розмовляючи з нинішніми і колишніми урядовцями, військовими, керівниками та працівниками корпорацій, експертами, дослідниками й активістами. Протягом двох років праці над цим проектом я провів повторні інтерв'ю з багатьма із цих людей, яких вважаю своїми найнадійнішими і вартими довіри джерелами. З деким я розмовляв уперше. Збираючи матеріали для книжки, я здебільшого покладався на розмови з держслужбовцями і військовими, які й нині працюють у сфері кібербезпеки або політики. Усі вони працюють в окопах цієї мінливої лінії фронту, а не в тилу. Я вдячний їм за те, що знайшли час для розмов зі мною на тему, яку багато хто в уряді й надалі відмовляється обговорювати публічно, позаяк ідеться здебільшого про таємні матеріали й операції.

Чимало людей, з якими я мав бесіди, дозволили їх цитувати, і в цих випадках я подаю їхні імена в тексті або в примітках. Інші жадали, щоб я не згадував їхніх прізвищ, а в деяких випадках навіть уникав назв агенцій і компаній, в яких вони працюють. Прикро, але доволі часто, пишучи про таємні матеріали зі сфери національної безпеки, журналісти не можуть відкрити джерел інформації. Не думаю, що бодай одна людина, з якою я спілкувався, збираючи матеріали для цієї книжки, поділилася зі мною інформацією, яка загрожує національній безпеці або піддає ризику чиєсь життя. Але я задовольнив прохання цих людей із двох причин.

Передусім тому, що інформація, надана ними, була важливою для розповіді й не могла бути отримана в інший спосіб, або ж тому, що її було неможливо отримати з інших джерел або ж вона підтверджувала інформацію з офіційних джерел чи документів у вільному доступі. (Хоч як це дивно, але чимало викривальної інформації щодо кібервійн і шпигунства оприлюднено або вона взагалі ніколи не була секретною.) По-друге, ці люди, розмовляючи зі мною, сильно ризикували своєю професійною кар'єрою і, можливо, свободою.

Обговорюючи кібервійни й шпигунство, інформатори часто й самі не знають, розкривають вони таємну інформацію або ж лишень підбираються до межі. Якщо б інформаторів, які обговорювали зі мною ці питання, ідентифікували за іменами, вони б позбулися допуску до надсекретних матеріалів і через це могли втратити працю за обраним фахом у сфері національної безпеки.

Крім того, через розкриття певної інформації ці джерела також могли зазнати кримінального переслідування. В адміністрації президента вкрай вороже ставляться до держслужбовців, які діляться інформацією з журналістами. Міністерство юстиції відкрило кримінальні провадження за розголошення таємних відомостей на більшу кількість осіб, ніж за усіх попередніх адміністрацій разом. Простіше кажучи, у наші часи з журналістами говорити надто відверто небезпечно. Найбільше ризикують колишні державні службовці та військові. Кілька колишніх керівників служби розвідки розповіли мені, що протягом останнього року їм неодноразово прямо заявляли: якщо вони й надалі бажають працювати на уряд за контрактами, журналістів їм краще оминати. У тих випадках, коли я посилаюся на інформацію з анонімних джерел, я намагаюся якнайдокладніше пояснити, чому слова цих людей варті довіри, водночас дотримуючись слова не розкривати інформацію, за якою їх можуть ідентифікувати.

Значна частина цієї книжки ґрунтується на документах із відкритих джерел, як-от урядові звіти і презентації, свідчення в Конгресі, виступи високопосадовців, а також аналітичні звіти приватних дослідників національної безпеки – ці документи щораз докладніші і їх щораз більше. Коли я починав збирати матеріали для книжки, багато колег запитували, як я зможу писати щось на таку оповиту державними таємницями тему, як кібербезпека. Однак, на мій подив, з'ясувалося, що величезна кількість викривальних й інформативних матеріалів є у відкритому доступі. Саме там я здобув значну кількість даних, які перекреслюють заяви багатьох держслужбовців про те, що ця тема надто тонка й уразлива, щоб обговорювати її публічно. Упродовж кількох останніх років дедалі більше держслужбовців і військових керівників почали говорити про кібервійни і шпигунство відкритіше, і це обнадіює. Суспільство не зможе усвідомити важливість проблеми, а влада – ухвалювати адекватні закони і вести виважену політику без чесного й відкритого обговорення цих питань.

ВСТУП

Шпигуни з'явилися без попередження. Вони тихенько займалися своїм ремеслом, викрадаючи секрети у найпотужнішої в світі військової структури. Вони пропрацювали декілька місяців, аж поки їхню присутність почали зауважувати. А коли злодіїв виявила американська влада, було надто пізно. Вони заподіяли неабияку шкоду.

Зловмисники викрали величезну кількість технічної та конструкторської інформації, що стосувалася найважливішого новітнього озброєння Сполучених Штатів – ударних літаків нового покоління під назвою «Єдиний ударний винищувач» (Joint Strike Fighter, JSF). Розробники сподівалися, що цей винищувач перевершить усі інші ударні літаки, буде використовуватись усіма видами війська і забезпечить панування Збройних сил США у повітрі на років десять. Винищувач F-35 був найскладнішим із будь-коли розроблених військовими озброєнням і, зважаючи на оціночну вартість у $337 млрд, іще й найдорожчим.

Усе вказувало на збройні сили Китаю як на винуватця серії зухвалих зламувальних операцій, які почалися наприкінці 2006 року. У цієї країни був мотив і можливості вкрасти секретну інформацію щодо F-35, особливо ту, що стосувалася системи уникнення ворожих радарів. Протягом десятиліть Китай провадив агресивну шпигунську кампанію проти Збройних сил США, свого найсерйознішого противника. З кінця 1970-х китайські шпигуни частенько працювали в американських університетах, а також у державних дослідних лабораторіях і компаніях, що виконували замовлення оборони, або ж проникали в них, викрадаючи конструкторську документацію, пов'язану з системами озброєння, зокрема з ядерними боєголовками.

Однак в цьому випадку крадії поводилися незвично. Шпигуни не викрадали паперових документів з офісів і не підслуховували розмови інженерів у кімнаті відпочинку. Вони цупили інформацію віддалено, за допомогою комп'ютерних мереж. Програму «Єдиний ударний винищувач» хакнули.

Фахівці у сфері інформаційної криміналістики військово-повітряних сил (ВПС), відповідальні за розробку F-35, почали шукати злочинців. Щоб зрозуміти, як саме хакери проникли в систему, їм довелося почати думати так, як думають злочинці. Отож вони взяли до команди хакера. Це був колишній військовий офіцер і ветеран таємних військових кібероперацій. Він з'їв усі зуби на тих перших військово-інформаційних операціях середини 1990-х, коли доводилося влазити радше в голову ворога, аніж у його бази даних. Ішлося про різновиди класичних пропагандистських кампаній комп'ютерної епохи; військовим хакерам було потрібно знати, як проникнути у комунікаційні системи ворога й передати повідомлення так, щоб вони здавалися надісланими з надійних джерел. Потому колишнього офіцера залучили до стеження за повстанцями та терористами в зоні бойових дій у Іраку, де він відстежував їх за мобільними телефонами та інтернет-повідомленнями. Йому було трохи за сорок, однак за стандартами професії він був старожилом.

Про витік інформації з програми «Єдиний ударний винищувач» збройні сили знали таке: інформація була вкрадена не з військових комп'ютерів. Очевидно, витік стався в компанії, яка допомагала проектувати та будувати літак. Шпигуни схитрували, націлившись на підрядників Міністерства оборони, у комп'ютерах яких було вдосталь надсекретної інформації, зокрема деякі креслення F-35, які, вірогідно, можна було виявити в комп'ютерах Міністерства оборони. І це була підступна тактика. Американські збройні сили не можуть існувати без підрядних компаній: без них не літають літаки, не їздять танки, не будуються і не ремонтуються кораблі. Але комп'ютерні системи приватних компаній зазвичай захищені гірше, ніж надсекретні військові мережі, найважливіші з яких навіть не під'єднані до інтернету. Хакери просто знайшли інший спосіб проникнення, націлившись на підприємства, яким військові доручили так багато важливих операцій.

Військові слідчі не були впевнені, в якій компанії стався витік. Це могла бути фірма Lockheed Martin, провідний підрядник у програмі створення F-35, або один із двох її головних субпідрядників – компанія Northrop Grumman чи BAE Systems, або будь-яка інша компанія з понад тисячі фірм і постачальників, які працювали за контрактом над багатьма механічними системами або ж розробляли електроніку. Близько 7,5 млн рядків програмного коду допомагали керувати літаком – це втричі більше, ніж містить програма управління най-

сучасніших винищувачів. Іще 15 млн рядків коду управляють логістикою, навчальною програмою та іншими системами підтримки. Для шпигуна така ситуація була, як кажуть військові, «обстановкою з багатьма мішенями». Він міг завиграшки знайти секрети систем навігації літака, бортових датчиків, систем контролю та озброєння будь-де.

Логічно було почати розслідування з компанії Lockheed Martin, провідного підрядника. В її комп'ютерах містилася вкрай важлива інформація щодо літака, але, що найважливіше, саме ця компанія керувала працею численних субпідрядників, яким передавали розмаїті дані з різних етапів розробки F-35. Однак коли військовий хакер з'явився в офісі фірми, щоб розпочати розслідування, зустріли його аж ніяк не технарі і не військові офіцери, які наглядали за розробкою F-35. Його привітали юристи компанії.

Хакер попросив ноутбук. «Навіщо він вам?» – запитали юристи. Він пояснив, що для початку йому потрібно дослідити схему внутрішніх комп'ютерних мереж. Він також хотів довідатись, яким програмним забезпеченням і якими додатками зазвичай користуються працівники компанії. Ці програми могли містити помилки у системних кодах або «бекдори»*, мати вразливості або лазівки в системі захисту, що дозволяють користувачеві (зокрема авторизованому, як-от системний адміністратор) обійти звичні заходи безпеки, наприклад введення логіна і пароля користувача, і отримати доступ до комп'ютера. Зламувач міг використати ці шляхи доступу, щоб укріпитися на позиції в електронній мережі компанії. Все, що потребував шпигун, – це вхід і цифровий плацдарм для проведення операцій.

Юристи видали хакеру новесенький, щойно з коробки ноутбук, який жодного разу не під'єднували до корпоративної мережі. Жоден працівник компанії, крім юриста, не торкався його. Хакер обурився. Це було наче його просили з'ясувати, як пограбували будинок, не дозволивши оглянути місце злочину.

Чому ж компанія Lockheed, яка заробляла мільярди на створенні «Єдиного ударного винищувача», не зробила всього можливого, щоб допомогти викрити шпигунів? Можливо, тому, що ретельне розслі-

---

* Бекдор (від англ. back door – чорний хід) – метод обходу стандартних процедур автентифікації, що дозволяє здійснити несанкціонований віддалений доступ до комп'ютера. – *Тут і далі примітки перекладача.*

дування виявило б незадовільний захист комп'ютерних мереж компанії? Слідчі могли відстежити витоки інформації, що стосувалася інших військових розробок. Навряд чи компанію могло виправдати те, що мережу зламали шпигуни, ноги яких не було на підприємстві. Компанія Lockheed була найбільшим постачальником товарів і послуг для американського уряду. У 2006 році вона уклала контрактів на $33,5 млрд, понад 80 % з яких припадало на Міністерство оборони. Однак ці цифри не охоплюють вартості секретних завдань для управління розвідки, яких, напевно, було ще на кілька мільярдів. Зрозуміло, компанія Lockheed не могла дозволити, щоб її вважали поганим охоронцем найцінніших державних таємниць – насправді, жоден з оборонних підрядників не може такого собі дозволити. А ще Lockheed – це відкрита акціонерна компанія. Тому радше за все акціонери негативно відреагували б на новини про те, що компанія не здатна захистити інформацію, надважливу для цього багатомільярдного бізнесу.

Не дивно, що хакер не знайшов у комп'ютері нічого цінного. Вище керівництво військово-повітряних сил, яке хотіло бачити єдиний ударний винищувач готовим, було розлючене через витік інформації і вимагало, щоб компанія Lockheed, так само як усі інші підрядні організації, сприяла розслідуванню уповні. На їхню думку, ці компанії не просто працювали на уряд, а й були його частиною, утримуваною на кошти платників податків, яким довірили надважливі державні таємниці. Командування військово-повітряних сил поглибило розслідування, і протягом кількох наступних місяців хакер і його колеги здійснили ретельну перевірку комп'ютерних мереж Lockheed, а також інших компаній, які працювали над програмою.

Слідчі виявили, що злам був не один. Витоки з мережі компанії Lockheed здійснювалися регулярно. Важко сказати, скільки саме разів це відбувалося, але спричинені збитки були вельми серйозними, зважаючи на кількість вкраденої інформації й безперешкодний доступ зламувачів до мережі. Під час останньої шпигунської кампанії, мішенями якої стали й інші підприємства, шпигуни викрали кілька терабайтів інформації, яка стосувалася конструкції винищувача, що згрубша дорівнює 2 % колекції бібліотеки Конгресу.

Раніше впровадження шпигуна в американську корпорацію і встановлення ним підслуху вважали ознакою героїчної майстерності у шпигунстві. Не було потреби заражати комп'ютер шкідливим про-

грамним забезпеченням, перехоплювати спілкування в інтернеті та підслуховувати з іншої частини світу.

Що більше прочісували слідчі інтернет-блоги і драйвери, то більше жертв виявляли. Шпигуни проникли у мережі субпідрядників у кількох країнах. Технарі простежили інтернет-протокольні адреси й проаналізували методи, якими послуговувалися шпигуни. Був невеличкий сумнів, чи це справді китайці, але, ймовірно, саме ця група була причетна до спроб зламу мереж оборонного відомства і великих американських компаній, зокрема тих, що працюють у галузях технологій і енергетики. Керівники військових структур і розвідки щойно почали усвідомлювати розмах, наполегливість і хитромудрість китайського кібершпигунства. Можливо, через збентеження, або в остраху перед висміюванням, або ж не бажаючи повідомляти китайцям, що їх викрили, уряд США не оприлюднив факту крадіжки.

Шпигуни полювали за деталями конструкції винищувача й інформацією щодо його здатності витримувати навантаження під час польоту й повітряного бою. Можна було припустити, що вони хотіли довідатися про недоліки літака, а також збудувати власний винищувач. Наслідки цього лякали. Якщо припустити, що шпигуни працювали на китайські збройні сили, одного дня американські винищувачі могли вступити в бій із власними клонами. А американським льотчикам довелося б мати справу з ворогом, який знає вразливі місця F-35.

На той момент інформація про сенсори й систему управління польотом, що дозволяють винищувачу виявляти противника або виконувати складні маневри, здавалася захищеною, позаяк відповідні креслення зберігалися на комп'ютерах, не під'єднаних до інтернету. Але навіть через рік слідчі надалі виявляли витоки інформації, які раніше проґавили. Можна було припустити, що шпигунська кампанія триває і під приціл потрапляють навіть не під'єднані до інтернету комп'ютери. Сам факт відсутнього під'єднання до мережі дозволяв припустити, що ці комп'ютери містять важливу інформацію.

Зрештою слідчі виснували, що спочатку шпигуни зовсім не шукали інформацію про F-35, а цілилися на іншу секретну програму. Імовірно, проект винищувача виявився для них легкою здобиччю, зважаючи на те, скільки незахищеної інформації зберігалось у мережі компанії. Ця зміна планів на півдорозі свідчить про неабияку зухвалість шпигунів. Деяких представників влади просто спантеличило те, що зламувачі майже не переймалися замітанням слідів. Здавалося, їм

було байдуже, що їх виявлять. Вони наче підбурювали американців вистежити їх, зухвало вважаючи, що цього не станеться.

Шпигуни викрали інформацію, потенційно корисну для розвідки, а також затримали розробку винищувача F-35. Згодом представники влади США заявили, що через нахабне проникнення в комп'ютери субпідрядників програмісти були вимушені переписати програмні коди для систем літака, що призвело до річної затримки у реалізації програми і 50-відсоткового збільшення її вартості. Китайцям не доведеться зіткнутися в бою з винищувачем, який не злетить. Натомість ця країна значно просунулася в проектуванні власного літака. У вересні 2012 року, під час візиту міністра оборони США Леона Панетти, китайська влада проґавила витік фотографій найновішого винищувача, що стояв на аеродромі. Він був дуже схожим на F-35, що не могло бути звичайним збігом, визнала американська влада. Конструкція китайського винищувача почасти базувалася на інформації, викраденій шпигунами в американських компаній шість років тому.

Керівники компаній докладно не знали, навіщо їх викликали до Пентаґону і навіщо їм видали тимчасові допуски до державної таємниці. Роззираючись довкола, вони бачили чимало знайомих облич. Генеральні директори або їхні представники працювали в дванадцяти найбільших американських корпораціях, які виконували оборонні замовлення: Lockheed Martin, Raytheon, General Dynamics, Boeing, Northrop Grumman та інші. Це були стабільні, впливові компанії, які десятиліттями будували американську військову машину. Навряд чи те, заради чого їх швидкоруч зібрали в штаб-квартирі Міністерства оборони того літнього дня 2007 року, було хорошою новиною.

Керівників компаній запросили до режимного приміщення для роботи з конфіденційною інформацією – кімнати, недосяжної для підслухувальних пристроїв. Розмова почалася з інструктажу щодо загроз, і в цьому не було нічого незвичного, позаяк військові регулярно обговорювали з керівниками оборонних підприємств можливі загрози національній безпеці. Однак цей інструктаж був присвячений корпоративній безпеці. Зокрема, безпеці корпорацій, якими керували зібрані директори.

Військові, які розслідували витоки інформації про F-35, розповіли все, що з'ясували. Масована шпигунська кампанія була націле-

на на комп'ютерні мережі всіх компаній. Шпигуни не обмежились інформацією про F-35; вони викрали стільки військових таємниць, скільки змогли знайти. Крадії обійшли слабкий електронний захист корпоративних мереж і скопіювали секретну інформацію на власні сервери. Вони надсилали працівникам, залученим до секретних проектів, невинні на перший погляд електронні листи, які виглядали так, ніби прийшли з надійних джерел усередині компанії. Коли ж адресат відкривав такий лист, на його комп'ютері інсталювався «бекдор», який дозволяв китайцям відстежувати кожне натискання клавіші на клавіатурі, кожен відвіданий сайт, кожен завантажений, створений або надісланий файл. Мережі компаній ставали проникними, а їхні комп'ютери – контрольованими і відстежуваними. Американський військово-промисловий комплекс, якщо використовувати сленг, хакнули.

Шпигуни надалі перебували в мережах цих компаній, полюючи за секретами і перехоплюючи повідомлення працівників. Можливо, саме зараз вони читають приватні електронні листи керівників компаній. «Чимало людей, які увійшли до цієї кімнати темноволосими, вийшли з неї сивими», – розповів Джеймс Льюїс, провідний експерт у галузі інформаційної безпеки і науковий співробітник Центру стратегічних і міжнародних досліджень – «мозкового центру» у Вашинґтоні, якому відомі подробиці тієї зустрічі.

Підрядні компанії виявилися слабкою ланкою у ланцюгу держбезпеки. Представники Пентаґону повідомили керівникам, що відповідь на крадіжку військових секретів – невідкладне питання національної безпеки, а для компаній – питання життя або смерті, адже їхній бізнес здебільшого залежить від коштів, зароблених із продажу літаків, танків, супутників, кораблів, підводних човнів, комп'ютерних систем і розмаїтих технічних і адміністративних послуг, наданих федеральному уряду.

Військові чітко заявили: якщо підрядники хочуть продовжити нинішні контракти, їм доведеться приділити пильнішу увагу інформаційній безпеці.

Однак вони не робитимуть цього самотужки.

Після тієї зустрічі Міністерство оборони почало надавати компаніям інформацію про кібершпигунів і небезпечних хакерів, вистежених американською розвідкою. На той час Пентаґон відстежував

близько десятка шпигунських операцій, здійснюваних різними групами інтернет-злочинців, які можна було класифікувати за цікавістю до певних військових технологій, структури військових операцій чи організацій або до оборонних підрядників. Ця інформація про іноземних шпигунів була результатом праці американської розвідки й збиралася за допомогою стеження та аналізу спроб проникнення в комп'ютерні мережі військових організацій, а також зламу комп'ютерів і комп'ютерних мереж ворогів Америки. У пошуках вірусів, комп'ютерних «хробаків» та інших шкідливих комп'ютерних програм контррозвідка США проаналізувала величезний обсяг трафіку в глобальних телекомунікаційних мережах. Ніколи раніше влада США не ділилася з приватними особами такою кількістю секретної інформації. Турбота про безпеку нації історично була прерогативою уряду. Однак зараз уряд та індустрія утворили союз, щоб протистояти спільній загрозі. Пентаґон надав компаніям інформацію про IP-адреси комп'ютерів і серверів, на які, як вважали, іноземні агенти пересилали викрадену інформацію, а також адреси електронної пошти, з яких, як було відомо, розсилалися на перший погляд невинні листи, що насправді містили віруси або шпигунське програмне забезпечення (ПЗ). Державні аналітики поділилися інформацією про найостанніші розробки і методи, якими послуговувалися для зламу іноземні хакери. І вони попереджали компанії про різновиди шкідливого програмного забезпечення, за допомогою якого хакери прокрадались у комп'ютери й викрадали файли. Озброєні основною інформацією (так званими ідентифікаторами загрози), компанії повинні були посилити захист мереж і зосередитися на протидії хакерам, запобігаючи проникненню їх у мережі. Ідентифікатори загрози розробили фахівці Агентства національної безпеки (АНБ) – найбільшої урядової розвідувальної служби. Його глобальна мережа стеження збирає дані з десятків тисяч комп'ютерів, зламаних і нашпигованих шпигунським програмним забезпеченням – абсолютно так само, як чинили китайські шпигуни, зламуючи комп'ютери оборонних компаній. Інформація, зібрана агентством, якнайповніше розкриває можливості, плани та наміри ворогів Америки, а тому є надсекретною. І ось уряд поділився цією інформацією з компаніями за умови дотримання суворої секретності. Отримувачам інформації було заборонено оприлюднювати будь-які матеріали щодо ідентифікаторів загрози й наказано повідомляти Пентаґон про будь-які спроби проникнення в комп'ютерні мережі.

«Ініціатива оборонної промисловості» (Defense Industrial Base Initiative), як назвали програму передачі розвідданих, спочатку охоплювала 20 компаній, керівників яких збирали у режимному приміщенні в Пентаґоні. Однак протягом року програма охопила вже 30 учасників. Сьогодні їх близько 100. Пентаґон планує додавати до цього секретного клубу, відомого його учасникам як DIB, 250 нових членів щороку.

Влада хоче захистити не лише військових підрядників. Вона розглядає DIB як модель захисту всіх промислових галузей – від телекомунікацій і енергетики до охорони здоров'я та банківської сфери, – будь-якого бізнесу, системи або функції, де використовуються комп'ютерні мережі. Нині це означає – майже все. Ця програма стала першим кроком до союзу влади й промисловості, який щораз міцнішає і розвивається.

Керівники розвідувальних служб, вищі військові чини й навіть президент наголошують, що наслідки чергової масштабної терористичної атаки на американців тьмяніють, якщо порівняти їх із хаосом і панікою, що їх може спричинити рішуча й зловмисна група хакерів. Замість того щоб украсти інформацію з комп'ютера, вони можуть знищити сам комп'ютер, зруйнувати комунікаційні мережі або вимкнути системи управління повітряним рухом. Вони можуть зламати під'єднані до інтернету пристрої, які регулюють постачання струму, і занурити міста у пітьму. Або ж можуть атакувати саму інформацію, знищивши або пошкодивши дані щодо фінансових рахунків, викликавши паніку в країні.

У жовтні 2012 року міністр оборони США Леон Панетта попереджав: «Сполучені Штати стоять на межі "електронного Перл-Гарбору": атаки, що призведе до фізичних руйнувань і смертей, паралізує й шокує країну, викликавши абсолютно нове розуміння вразливості». За п'ять місяців до того президент Барак Обама написав у газетній передовиці, що війни майбутнього відбуватимуться онлайн, коли «ворог, не здатний зрівнятися військовою міццю на поле битви, шукатиме вразливі місця у наших комп'ютерах». Обама змалював зловісну й, можливо, дещо гіперболізовану картину. Однак його вибір образних засобів віддзеркалює стурбованість державних високопосадовців і бізнесу тим, що кіберпростір, який, здавалося б, несе безмежні надії для країни, водночас є нашим найуразливішим місцем. «Зламування

життєво важливих банківських систем може спричинити фінансову кризу, – писав Обама. – Брак питної води або збій у функціонуванні лікарень здатні підірвати національну систему охорони здоров'я. І, як ми бачили під час минулих аварійних вимкнень електростанцій, припинення постачання електроенергії може призвести до зупинки підприємств, обмеження життєдіяльності міст і цілих регіонів». Директор ФБР Джеймс Комі заявляв, що загроза кібератак і зростання кіберзлочинності (зокрема шпигунства та фінансового шахрайства) стануть найбільшими загрозами національній безпеці в наступному десятилітті. Протягом останніх двох років можливість руйнівних кібератак очолила перелік «глобальних загроз», складений усіма сімнадцятьма американськими службами розвідки для звіту перед Конгресом. Для уряду США захист кіберпростору став головним пріоритетом національної безпеки, адже онлайн-атаки можуть мати згубні офлайнові наслідки.

Однак уряд не каже всієї правди. Можновладці квапляться змалювати країну жертвою, що потерпає від постійних підступів невидимих ворогів. Однак військові та розвідувальні органи США, часто у співпраці з американськими корпораціями, є одними з найагресивніших бійців у кіберпросторі. Сполучені Штати – одна з кількох країн, державна політика яких трактує кіберпростір як поле битви й має всі можливості вчинити це. Понад десятиліття кібершпіонаж був найефективнішим методом збору інформації про ворогів країни – за кордоном і вдома. Агресивні дії, до яких вдаються у кіберпросторі Сполучені Штати, докорінно змінюють інтернет, і не завжди на краще. А завзяті спроби захисту кіберпростору, до яких вдається уряд у співпраці з корпораціями, робить всесвітню мережу вразливішою.

Історія про те, як захист кіберпростору став для Сполучених Штатів таким важливим, починається зі спроб державного контролю над ним і використання кіберпростору як зброї та території шпигунства. Нині військові називають кіберпростір «п'ятим театром» бойових дій і вважають досягнуті тут перемоги такими ж важливими, як і в чотирьох інших просторах: на суші, у морі, в повітрі та космосі. Сполучені Штати ввели поняття кібератак у традиційний перелік методів бойових дій і почали застосовувати їх для виведення з ладу інфраструктури в інших країнах, тобто робити все те, чого бояться у власній країні так, що для запобігання кібератак ладні вдаватися до

найекстраординарніших заходів. Зі всього спектра військових дій у кіберпросторі США обрали агресію.

Американські армія та розвідслужби вирощують нове покоління кібервоїнів, навчених відстежувати комп'ютерні системи іноземних супротивників, зламувати їх, а якщо потрібно, виводити з ладу й знищувати. Поняття «кібервійна», як і «кіберпростір», – доволі розпливчасте. Однак воно описує цілий спектр наступальних операцій. Так само як звичайне шпигунство є невід'ємною частиною традиційної війни, так і кібершпигунство передує атаці на комп'ютерну систему. Про це свідчить той факт, що США витрачають значно більше часу та коштів на комп'ютерне шпигунство й викрадення інформації, ніж на виведення з ладу важливих об'єктів інфраструктури та знищення фізичного обладнання за допомогою комп'ютерних мереж. І подібні атаки повторюватимуться частіше й стануть ефективнішими. І справді, саме кібервійна – поєднання шпигунства й атак – стала інструментом досягнення військової перемоги Америки в Іраку в 2007 році, хоча методи її ведення до кінця не з'ясовані й належно не оцінені. У співпраці з американськими розвідслужбами військові застосовували кібертехніки наступу (хакінґ), щоб вистежувати людей у реальному світі, а потім захоплювати або вбивати їх.

Однак, так само як захист кіберпростору не є прерогативою влади, ведення війни в кіберпросторі також стає приватною справою. Індустрія торгівлі кіберзброєю та приватні служби безпеки розвиваються стрімко – вони пропонують товари і послуги як урядовим структурам, так і корпораціям, які більше не можуть протистояти невпинному шпигунству самостійно й не хочуть наражатися на ризик кібератак. Армії різних держав неминуче зіткнуться колись на кібернетичному полі бою. І там само зустрінуться армії корпорацій.

У кіберпросторі оперує не лише влада. Для захисту комп'ютерних мереж і проведення кібератак у них потрібне залучення приватного сектора, хоч і не завжди добровільне. Більшість комп'ютерних мереж США мають приватних власників. Влада не може захистити всі ці мережі або наглядати за ними. Але більшість світових цифрових комунікацій проходить через обладнання, розташоване саме в Сполучених Штатах. І влада має певні привілеї, використовуючи їх, тому вкрай потребує їхнього захисту. З цією метою і виник військово-мережевий комплекс.

Так само як і військово-промисловий комплекс, це нове об'єднання охоплює виробників танків і літаків, ракет і супутників. Але в нього також входять технологічні гіганти, фінансові організації та телекомунікаційні компанії. Влада Сполучених Штатів наполягала, переконувала, спокушала, а інколи навіть примушувала компанії надавати допомогу в запобіганні несанкціонованому доступу іноземних і місцевих недоброзичливців у американські електромережі та інші критично важливі об'єкти інфраструктури в пошуках уразливих місць. АНБ уклало таємні домовленості з провідними технологічними компаніями, зокрема з Google, щодо моніторинґу приватних мереж для відстежування загроз. АНБ передавало секретну інформацію провідним банкам і фінансовим організаціям задля уникнення катастрофічної кібератаки на Волл-стріт.

Але влада також намагалася змусити деякі компанії дозволити АНБ розмістити пристрої стеження у мережах. Агентство платило технологічним компаніям за встановлення бекдорів у їхні продукти, за допомогою яких можна було стежити за іноземними розвідслужбами й контролювати дії їхніх армій. Ці секретні точки доступу також дозволяють військовим проводити кібератаки в іноземних державах. Без співпраці з компаніями Сполучені Штати не змогли б брати участь у кібервійні. У цьому сенсі новий військово-мережевий комплекс відіграє ту саму роль, яку раніше відігравав військово-промисловий. Уряд держави не йде на війну наодинці. Він покладається на компанії, які створюють зброю, перевозять і годують військо, будують і ремонтують літаки, кораблі та супутники. Сполучені Штати стали найпотужнішою військовою державою в історії світу саме завдяки взаємовигідній співпраці з корпораціями. І прагнули повторити цей успіх у кіберпросторі.

Сполучені Штати швидко нарощують свої можливості для домінування у кіберпросторі. У 2014 році уряд витратив понад $13 млрд на програми кібербезпеки – здебільшого на захист комп'ютерів і мереж у державних установах, а також для обміну з приватними компаніями інформацією про загрози, отриманою під час розвідувальних операцій. Зауважу, що того ж року витрати на боротьбу зі зміною клімату, яку президент Обама назвав «сучасною глобальною загрозою», становили $11,6 млрд. Протягом наступних п'яти років лише Міністерство оборони планувало витратити $26 млрд на технології кібернетичного

захисту й нападу. Інформація про те, скільки коштів Сполучені Штати планують витрачати на операції наступу, – засекречена. Однак межа між обороною та нападом у кіберпросторі вкрай розмита й мінлива. Інфраструктуру, створену для захисту мереж, можна використати для атак. Зі стратегічних і цинічних міркувань офіційні особи воліють говорити публічно лише про оборону: значно легше отримати кошти та політичну підтримку на відбиття агресії, ніж на створення кіберармії для проведення атак і шпигунської активності за кордоном. Однак саме цим і займаються США, витрачаючи на операції наступу чималу частину мільярдів, наданих на «оборону».

Бізнес у сфері кібербезпеки процвітає. Компанії та приватні особи в усьому світі витрачають близько $67 млрд на рік на захист своїх комп'ютерів і мереж. Чимало експертів, що працюють у цій сфері, навчилися свого ремесла у військових або розвідувальних організаціях. Справді, Пентаґон став навчальною базою для приватних кіберцерберів, які можуть подвоїти або навіть потроїти свої прибутки, перейшовши на роботу в приватну компанію зі сфери безпеки. Оборонні підрядники, які опинялися під прицілом кібершпигунів, почали надавати експертні послуги із захисту мереж і ведення війни в них клієнтам, зокрема енергетичним підприємствам і банкам – тим самим компаніям, захистом яких так занепокоєна влада.

Боротьба за контроль у кіберпросторі визначає стратегію американської нацбезпеки у XXI столітті. Однак відповідь на кіберзагрози може змінити кіберпростір більше, ніж зміни, викликані цими загрозами. Рішення, які нині ухвалюють представники влади та бізнесу, матимуть серйозні наслідки не лише для американців, а й для людей у всьому світі, об'єднаних довірою до широкого, вільного і часто важкого для опису простору, який не є загальнодоступним, але й не належить одній корпорації або уряду. Існування загроз у кіберпросторі – незаперечний факт. Подолання цих загроз – непроста й зазвичай ризикована справа, однак ми всі у ній зацікавлені.

ЧАСТИНА І

1
ПЕРША КІБЕРНЕТИЧНА ВІЙНА

Боб Стасіо ніколи не планував ставати кіберсолдатом. Після закінчення школи Стасіо вступив до Університету Буффало, де навчався за програмою підготовки офіцерів резерву. Він спеціалізувався у фізико-математичних науках, вивчав головоломні теорії квантової механіки й диференціальних рівнянь. Університет, зацікавлений у випуску студентів, що спеціалізуються в точних науках, дозволив нехтувати певними складовими навчальної програми, наприклад, вивченням англійської мови. Протягом усього навчання Стасіо не написав жодного твору.

У 2004 році 22-річний Стасіо прибув до Форт-Льюїса (штат Вашинґтон). Штабний офіцер розвідки мигцем поглянув на резюме молодшого лейтенанта, зауважив, що той має серйозну підготовку з математики та фізики, і сказав: «Служитимеш в роті радіотехнічної розвідки (SIGINT)». Радіотехнічна розвідка займається перехопленням і аналізом сигналів електронних засобів зв'язку. Як у всіх інших галузях розвідки, тут йдеться про поєднання науки і мистецтва, хоча головний акцент зроблено таки на науці. Штабний офіцер розвідки працював у АНБ і зрозумів, що знання Стасіо з фізики виявляться вельми корисними, оскільки велика частина роботи в радіотехнічній розвідці пов'язана з прийомом радіосигналів, оптико-волоконним зв'язком та інтернет-пакетами.

Військова підготовка Стасіо в коледжі полягала в навчанні використовувати гвинтівку й керувати загоном. Протягом шести місяців він вивчав основи збирання й аналізу розвідданих у школі армійської розвідки в Форт-Хуачука (штат Арізона). Після прибуття до Форт-Льюїса Стасіо скерували в загін Stryker – механізовану бригаду швидкого реагування, створену для швидкого – протягом кількох днів – розгортання сил і вступу в бій. Завдання Стасіо полягало у визначенні місця розташування противника на полі бою за допомогою стеження за телекомунікаційними сигналами. Також він мав перед-

бачати наміри ворога, перехоплюючи накази ворожого командування або прослуховуючи запити командирів загонів, які перебували в тилу, на нанесення авіаударів. Було заплановано, що Стасіо приєднається до четвертої бригади другої стрілецької дивізії Raiders, яку мали відрядити до Іраку, і працюватиме разом із командою лінгвістів, що було дуже важливо, позаяк Стасіо не знав арабської. Однак, зустрівшись із цими лінгвістами, Стасіо занепокоївся: майже всі вони розмовляли лише англійською і корейською.

Армія створила підрозділи радіотехнічної розвідки для ведення холодної війни. Тисячі військових продовжують служити на Корейському півострові. Вони володіють знаннями з ведення сухопутних боїв зі збройними силами Північної Кореї, під час яких радіорозвідка – визначення розташування танків і військових формувань противника – повинна відігравати центральну роль в операції. Проте дивізія Raiders не надавалася для боротьби з комп'ютерними мережами іракських повстанців, добровільних джихадистів і терористів. Ці парубки не їздили на танках. Вони не організовувалися в загони за правилами військової ієрархії. Ну і, звісно, вони не розмовляли корейською.

Стасіо вирішив, що його підготовка розвідника не придасться в Іраку, американська окупація якого поступово розклеювалася. Армійські втрати нечувано зросли внаслідок успішної кампанії повстанців із мінування доріг. Солдати, що вижили після цих вибухів, поверталися додому без кінцівок або з серйозними черепно-мозковими травмами, від яких фізично й емоційно потерпатимуть решту життя. Підрозділ радіотехнічної розвідки не запобігав цим атакам, насправді до його послуг практично не вдавалися. У жовтні 2004 року один керівник служби радіотехнічної розвідки заявив, що майже 90 % усієї інформації в Іраку було отримано завдяки мережі розвідників та інформаторів, але це не допомогло американцям зменшити кількість вибухів і нападів повстанців.

Стасіо прочитав про повстанців усе, що міг, передусім зосереджуючись на способах їхньої організації – мережі з багатьох незалежних груп людей, які працювали в командах, поза централізованим управлінням. Ця схема організації діаметрально відрізнялася від вертикалі військової бюрократії, в якій накази віддають донизу згори через кілька рівнів командирів. Назагал, методи розвідки, які вивчав Стасіо, повинні були спрацювати. Від нього очікували визначення

розташування ворогів за допомогою аналізу електронних сигналів і передбачення їхніх наступних кроків. Однак військова техніка, призначена для цих операцій, була зовсім не пристосована для ведення радіорозвідки в складних міських умовах. Група Raiders використовувала систему перехоплення сигналів, відому під назвою Prophet, – масивну вантажівку з довгою радіоантеною заввишки з вуличний ліхтар на даху. Старшим офіцерам бригади система була до вподоби, бо дозволяла виявити розташування ворогів у межах найближчої зони проведення операції. Це був тактичний пристрій, і вони направляли його туди, де потрібно було зібрати розвіддані.

Проте Prophet був створений для перехоплення радіохвиль і лише на відкритій і відносно рівній місцевості ведення бойових дій. Стасіо знав, що іракські повстанці спілкуються за допомогою стільникових телефонів і електронної пошти, а також розміщують відеозаписи в інтернеті. А пересувалися вони невеликими групами в щільній бетонній забудові Баґдада та інших густонаселених міст країни. У таких умовах користі із системи Prophet було мало. Тож коли Стасіо потрапив до Іраку, він побачив, що загони військової розвідки, які прибули раніше, використовували систему Prophet не для перехоплення радіосигналів, а для перевезення їжі та інших запасів.

Була ще одна причина, чому ветерани любили Prophet, – він їм належав. Вони могли їхати ним куди завгодно і контролювали збір і аналіз розвідданих. Стасіо подумав, що старші офіцери зазвичай не довіряють розумникам, що прилітають зі Штатів, найчастіше із Вашинґтона, а також державним розвідувальним агентствам, таким як ЦРУ і АНБ, які звідси, з поля битви, здавалися громіздкими й незграбними бюрократичними машинами з тлумами програмістів і комп'ютерних диваків, надто далеких від приземлених, тактичних потреб збройних сил у Іраку.

Але Стасіо знав, що в державних агентств, зокрема в АНБ, є дещо йому потрібне: дані. А саме сервери, переповнені електронною інформацією і перехопленими сигналами, зібраними прослуховувальними пристроями агентства в усьому світі. Стасіо подумав, що якщо зможе під'єднатися до мереж радіотехнічної розвідки з Іраку, то зможе дізнатися щось про розміри й форму ворожих мереж, зібравши докупи записи щодо їхніх сеансів зв'язку. Це була кропітка праця, яка вимагала багатогодинного просиджування за комп'ютером в якому-небудь трейлері з кондиціонером, замість кружляння запорошеними

вулицями у вантажівці з системою Prophet. Стасіо був фанатом серіалу «Дроти» (The Wire) на каналі HBO, зокрема захоплювався одним із героїв цього фільму, Лестером, який розкрив мережу наркодилерів у Балтиморі, відстеживши їхні дзвінки через мобільний зв'язок. Те саме Стасіо хотів зробити в Іраку.

Він звернувся до свого бригадного офіцера розвідки у Форт-Льюїсі з проханням не відправляти його на полігон для піхотної підготовки й вивчення неповороткої системи Prophet, а дозволити йому та ще кільком офіцерам розвідки залишитися на базі для освоєння нового програмного забезпечення для побудови мережевих схем і систематизації трафіку. Підрозділи тактичної військової розвідки даремно нехтують цими інструментами, переконував Стасіо. Проте ті напевно придадуться в Іраку.

І офіцер погодився.

Стасіо і його колега-лейтенант розробили власну систему підготовки, яка опиралася на принцип зворотного зв'язку. Ідея полягала в тому, щоб невеликі підрозділи розвідки встановлювали в польових умовах власні комп'ютери, об'єднані в локальні мережі, з яких могли мати доступ до величезних баз даних АНБ та інших служб, що збирають корисну інформацію щодо всіх військових і розвідувальних операцій, зокрема супутникові фотографії, покази інформаторів, протоколи допитів полонених бойовиків і навіть політичні прогнози аналітиків ЦРУ. Стасіо вважав важливим будь-які фрагментарні дані чи неповну інформацію. Проте лише від фрагментів користі було мало. З цієї інформації потрібно було скласти повну картину.

Для людини, яка звикла з дитинства до різних способів зв'язку – телефону, електронної пошти, текстових повідомлень, – найрізноманітніших пристроїв, описаний метод аналізу інформації здається зрозумілим на інтуїтивному рівні. Стасіо і військові з його загону готувалися до відправки в Ірак протягом двох із половиною років. Він узяв до загону чотирьох корейських лінгвістів і відіслав їх на річний пришвидшений курс вивчення арабської мови. Не йшлося про вільне знання мови, досить було знати арабську на рівні, який дозволив би їм працювати з місцевими перекладачами й складати звіти для розвідки. Решту лінгвістів він відрядив вивчати методи аналізу інформації.

Стасіо прибув до Іраку в квітні 2007 року – без навантаження системою Prophet – у складі нової хвилі американських військово-

службовців. Він замислився, чи не запізно вони приїхали? Стасіо і члени його команди побачили, що повстанці невпинно атакують американських військових, мінують дороги й обстрілюють їх із мінометів. Ескалація громадянської війни руйнувала Ірак. Іноземні бойовики просочувалися в країну із сусідніх Сирії та Ірану, а нещадна терористична мережа, відома в Іраку як «Аль-Каїда», вела жорстокі атаки на американські та коаліційні війська, членів іракського уряду й на іракських шиїтів – також місцевих мусульман і мирних громадян. Терористичне угруповання прагнуло зламати хребет молодому урядові, замінивши його релігійною диктатурою. «Можливо, – подумав Стасіо, – таки варто було більше тренуватися стрільбі з рушниці».

Проте він не знав – не міг знати, – що його ідеї щодо інформаційної підтримки бойових дій доведеться випробувати масштабно. Американські збройні сили збиралися атакувати ворога способом, яким раніше навіть не намагалися діяти. І Стасіо мав опинитися на передовій.

Майк МакКоннелл мав лише годину, щоб захистити свій план.

У травні 2007 року, коли лейтенант Стасіо опинився у небезпечній ситуації в Іраку, нещодавно призначений директор національної розвідки спілкувався в Овальному кабінеті з президентом Бушем і кількома високопосадовцями з Ради національної безпеки США. МакКоннелл звертався не лише до президента, а й до віце-президента Діка Чейні, міністра оборони Роберта Ґейтса, міністра фінансів Генрі Полсона і радника президента з питань національної безпеки Стівена Гедлі. Політики такого рівня рідко збиралися всі разом у одній кімнаті. Проте їхня присутність була необхідна для здійснення плану, який визрів у голові МакКоннелла.

Остання з п'яти додаткових бригад, відправлених Бушем на боротьбу з повстанцями в Іраку того місяця, облаштовувалася на позиціях на південному сході від Баґдада. Разом із цими бригадами загальна чисельність додаткових підрозділів становила 30 тисяч осіб. МакКоннелл хотів дати їм нову зброю. Він розповів президентові про деякі можливості ЦРУ, які дозволять команді досвідчених хакерів проникати в телекомунікаційні системи, використовувані іракськими бойовиками для координації атак і мінування шляхів. Після проникнення у ці мережі американські хакери зможуть використати потужне ПЗ для стеження за ворогами й здобуття життєво важливої інформа-

ції: наприклад, про командирів окремих терористичних груп та їхні плани. Ця інформація могла допомогти військам вистежувати цілі, визначати місце розташування об'єктів стеження і, ймовірно, перешкоджати ворогові закладати бомби або влаштовувати засідки.

Але хакери також могли маніпулювати повстанцями, контролювати їхні стільникові телефони, надсилати фальшиві текстові повідомлення або робити телефонні дзвінки, які здавалися б справою рук інших повстанців. Хакери могли б збивати повстанців із цілей, ба навіть скеровувати їх у засідки, влаштовані американськими військовими. Якщо б удалося проникнути в комп'ютери повстанців, можна було б з'ясувати, хто завантажує в мережу жахливі відео страт, що стали дешевим і ефективним способом залучення прибічників і залякування іракських громадян. Американські хакери планували встановити шпигунське ПЗ на ворожих комп'ютерах і скопіювати адреси електронної пошти та номери мобільних телефонів, що ними послуговувалися бойовики. Вони могли відстежити кожне слово, набране ворогом на клавіатурі комп'ютера, кожен відвіданий сайт, кожен надісланий електронний лист. Також вони могли розшифрувати паролі, які бойовики використовували для входу на форуми, на яких планували атаки.

МакКоннелл пропонував підривати діяльність повстанців зсередини, використовуючи проти них їхні власні ресурси. Загалом, усі запропоновані заходи здавалися звичайними шпигунськими операціями з тих, що не вимагали дозволу президента. Проте успіх тієї місії цілком залежав від спритності хакерів і використаних ними інструментів, зокрема від комп'ютерних вірусів, які мали стати одним із найінноваційніших і найнепередбачуваніших озброєнь в американському арсеналі. Після встановлення шкідливого програмного забезпечення на комп'ютер завжди є ризик його поширення. Мережеві «хробаки» – це програми, що самовідтворюються, створені для того, щоб проникати в інші комп'ютери, з'єднані мережею із зараженим пристроєм. А віруси, як підказує назва, здатні дуже швидко поширюватися від комп'ютера до комп'ютера. За кілька місяців до вторгнення 2003 року армійське командування відмінило заплановану кібератаку на банківську систему Іраку, не без підстав вважаючи, що шкідливі програми можуть поширитися через іракські комп'ютерні мережі у мережі французьких банків. Через специфіку структури інтернету фінансові системи обох країн були пов'язані. Американські можно-

владці уявили заголовки передовиць, у яких ішлося про вихід із ладу банкоматів у Франції внаслідок невдалої американської операції.

Ризик супутніх утрат під час використання кіберзброї був значним. А, згідно з планом МакКоннелла, АНБ мусило заразити шкідливим ПЗ не лише телефони і комп'ютери повстанців, а й безліч пристроїв мирних іракців. Для здійснення плану потрібно було повне інформаційне покриття на полі битви, а це означало, що шпигунське ПЗ потрібно поширити максимально, інфікувавши якнайбільше іракських засобів комунікації, бо лише так можна визначити, з ким спілкуються терористи і повстанці. Таке масштабне поширення шкідливого ПЗ було небезпечним іще й тому, що могло інфікувати навіть системи збройних сил США.

Хоча кіберзброя не смертельна в тому ж сенсі, що й традиційна зброя, проте може бути дуже небезпечною і руйнівною, виходячи за межі атакованих цілей. У цьому сенсі кіберзброя подібна до ядерної. Саме тому застосування кіберзброї, як і ядерної, вимагає президентської санкції. МакКоннелл сподівався отримати цей дозвіл під час годинної зустрічі з Бушем і членами Ради національної безпеки. Прохання було дуже важливим і політично чутливим. Півтора року тому, в грудні 2005-го, агентство привселюдно зганьбили за прослуховування американських громадян у телекомунікаційних мережах без судового дозволу. І ось АНБ знову збирається проникати в мережі зв'язку й збирати інформацію, що стосується не лише повстанців, а й десятків мільйонів мирних громадян. Деякі з цих мереж належали приватним компаніям, і АНБ не збиралося просити дозволу в цих компаній на перехоплення даних. Агентство мало намір шпигувати за цілою країною, націливши кіберзброю проти американських громадян. Президент мав знати про це і дозволити такі дії.

МакКоннелл знав, що Буш не розуміється на технічних аспектах справи; він якось сказав, що користується «ґуґлом» зрідка, здебільшого щоб поглянути на супутникові фото свого ранчо в Техасі. Попередник Буша також не був технофілом. Протягом восьми років роботи в Білому домі, що припали на час народження сучасного інтернету і телекомунікаційну революцію, Білл Клінтон надіслав лише два листи електронною поштою.

Але МакКоннелл знав, що найважливіші особи у цій кімнаті йому довіряють. Шість місяців тому Чейні запросив МакКоннелла до свого особистого кабінету в офісній будівлі державного підрядчика, компа-

нії Booz Allen Hamilton, щоб повідомити їхнє спільне з президентом прохання до МакКоннелла – очолити службу розвідки. Цю посаду відкрили лише два роки тому, платня становила лише частину від цифри з семи нулями, що їх тоді отримував МакКоннелл, повноваження були розпливчастими, та й сама посада не мала ваги у бюрократичній машині. МакКоннелл звернувся за порадою до свого давнього товариша й союзника Ґейтса, який пообіцяв особисту та політичну підтримку будь-яким ініціативам майбутнього майстра шпигунства. Також МакКоннелл мав важливого союзника в особі генерала Кіта Александера, директора АНБ. Саме йому належало реалізувати запропонований план в Іраку.

Александера зацікавила така можливість. Він вибудовував розвідувальну імперію в АНБ – найбільшій шпигунській організації країни, 35 000 співробітників якої працювали в різних куточках Сполучених Штатів і в союзних країнах усього світу. Александер зібрав неперевершений колектив фахівців зі збору розвідданих, озброївши їх приголомшливою технікою для відстежування дзвінків стільниковим зв'язком, текстових повідомлень, електронних листів, інтернет-трафіку в телекомунікаційних мережах усього світу. АНБ було єдиним і найбільшим постачальником інформації для щоденних, політично важливих брифінґів у адміністрації президента з питань національної безпеки. Саме АНБ постійно надавало надійну інформацію про місцерозташування розшукуваних терористів. Натомість ЦРУ практично не мало людського ресурсу, здатного здобувати інформацію зі внутрішнього кола «Аль-Каїди». Війну з терором вела переважно розвідка. Операція в Іраку стала шансом для АНБ показати силу кібернетичної війни, нерозривно пов'язаною з методами електронного шпигунства. Щоб маніпулювати комп'ютером або телефоном чи то вивести їх із ладу, хтось повинен насамперед визначити їхнє розташування в мережі, а вже потім проникнути всередину пристрою. Протягом двох років Александер вибудовував військо шпигунів. І нарешті, їх можна було спустити з повідця й дозволити їм атакувати.

Буш був метикуватим. Попри поверхневе знання технологій, здавалося, що він миттєво збагнув зв'язок між комп'ютерами й людьми і те, що методи стеження допоможуть контролювати не лише техніку, а й людей, які цю техніку використовують, а також те, що завдяки стеженню в мережі можна визначати розташування людей, брати їх у полон або знищувати фізично. Президент уже схвалив інший се-

кретний проект, який передбачав зараження комп'ютерних систем, використовуваних для контролю іранських атомних станцій, мережевим «хробаком», який виводив із ладу центрифуги. Проаналізувавши кілька варіантів призупинення іранської програми зі створення ядерної зброї, радники Буша і деякі високопоставлені армійські генерали запропонували ще одну ідею. Чом би не позбавити Іран можливості збагачувати уран – головний компонент ядерної зброї, – саботуючи механічний процес? Вони визначили ціль – збагачувальний завод у місті Нетенз. І запропонували зброю – комплексну комп'ютерну програму, яка перебирає контроль над електронним обладнанням, що регулює роботу тисяч центрифуг – високих циліндричних пристроїв, які обертають газоподібний уран з високою швидкістю, перетворюючи його на зброю. Центрифуги становили ядро іранської ядерної програми. Без них іранці не змогли б збагатити ядерний матеріал для використання в бомбах чи боєголовках.

Буш схвалив операцію, і найкращі американські хакери й фахівці з безпеки почали роботу зі створення першої кібернетичної зброї такого штибу, яка отримала назву Stuxnet, за якою ховалися тисячі рядків програмних кодів. Проте операція, що почалася того року, мала обдурити противника, а не знищити його. Американці, які співпрацювали з Ізраїлем, хотіли поступово зірвати плани Ірану зі створення ядерної зброї, приховуючи той факт, що причиною зриву ядерної програми стала кіберзброя. Завдання Stuxnet полягало в тому, щоб перекрити вентилі, які регулюють потік газу всередині центрифуг. Що вище тиск газу, то максимальніше навантаження центрифуг, які починають працювати на межі. Цей збій можна пояснити низкою причин, зокрема несправним устаткуванням або некомпетентністю інженерів і робітників заводу, яких можуть звинуватити в неправильній установці й експлуатації центрифуг. Комп'ютерні системи контролю центрифуг не були під'єднані до інтернету, тому для впровадження Stuxnet потрібно було залучити агента або придумати віддалений спосіб інфікування. Це мусила бути непомітна й акуратна операція.

МакКоннелл запропонував інший план для Іраку – з широким використанням вірусів, шпигунського програмного забезпечення і методів комп'ютерного зламу. І кінцевою ціллю цього плану було фізичне знищення людей, а не збій технологічних процесів. Упро-

вадження «хробака» Stuxnet було актом саботажу. Натомість МакКоннелл пропонував війну.

Довіра Буша до плану МакКоннелла зросла так, що він попросив його проводити щоденні брифінґи в Овальному кабінеті – завдання, яке у минулому керівники шпигунських агенцій доручали лише своїм найближчим підлеглим. Ці двоє швидко порозумілися під час зустрічі на ранчо Буша ще до того, як президент оголосив про призначення МакКоннелла. Колишньому шпигуну й адміралові ВМС у відставці простацька манера спілкування президента, властива всім південцям, здавалася доброзичливою та звичною. МакКоннелл також зростав у Південній Каролініі й досі не втратив шарму безпосередності. Сидячи на веранді ранчо, двоє чоловіків спостерігали за грозовими хмарами, що купчилися на горизонті. «Поганий знак», – сміячись, говорили вони.

А зараз МакКоннелл попросив про годинну зустріч із президентом, щоб отримати дозвіл на кібервійну в Іраку. Буш дав «зелене світло» через 15 хвилин.

Стасіо прибув до Іраку на базу передового розгортання Таджі, запорошену рівнину в сільській місцевості на північ від Баґдада, колишню базу Республіканської гвардії, а ще раніше фабрику з виробництва хімічної зброї. Таджі розташований у спекотному сунітському трикутнику – епіцентрі опору американським збройним силам. Саму базу та її окремі підрозділи обстрілювали з мінометів і підривали за допомогою саморобних вибухових пристроїв близько 150 разів на день. Щоразу, коли загони виходили на патрулювання, на них очікували засідки або закладені на дорогах міни. І Таджі не був єдиним таким місцем. Ситуація в Іраку була вкрай напружена. Минулий рік став для коаліції одним із найкривавіших – загинуло майже 900 осіб, а 2007 рік міг навіть побити цей рекорд. Місяць прибуття Стасіо ознаменувала найбільша кількість жертв із січня 2005 року. Майже всі загиблі були американцями. Кількість загиблих іракських цивільних порахувати важче, але вона також була високою і, за достовірною інформацією, наближалася до 30 nbczx осіб протягом 2006–2007 років, що удвічі більше, ніж на початку війни.

Нова хвиля військових повинна була забезпечити безпеку в Баґдаді й найнебезпечніших околицях міста, вивільняючи додаткові сили для переслідування бойовиків і захисту цивільного населення.

Генерал Дейвід Петреус, людина, якій Буш доручив зробити останню відчайдушну спробу зупинити опір, бачив два варіанти боротьби: укласти союз із тими повстанцями, яких можна переконати перейти на бік американців або принаймні скласти зброю, а решту захопити в полон чи знищити. Останніх Петреус називав «непримиренними».

Спочатку новоприбулі сповільнили процес і додали збентеження. Здавалося, командири Стасіо в Таджі не знали, що робити з раптовим напливом нових солдатів. Проте Стасіо та його знайомий аналітик із Форт-Льюїса повернулися до «навчання». Вони організували місце праці на старому складі боєприпасів і вийшли на зв'язок із підрозділами, які вже повернулися додому і тепер працювали в інформаційному центрі у Форт-Льюїсі. Ці підрозділи стали одними з точок зворотного зв'язку. Стасіо контактував із ними за допомогою захищеної комп'ютерної мережі, а потім під'єднався до урядових інформаційних баз даних, які просто тонули в нових розвідданих. Масштабна мережа стеження на всій території Іраку постачала новими сигналами, новими даними. Нарешті Стасіо міг відчути себе Лестером з «Дротів».

Стасіо почав вибудовувати діаграми мереж бойовиків, аналізуючи сигнали їхніх стільникових телефонів для визначення зв'язку між ними й місця їхнього розташування. Він відсилав ці звіти назад до Форт-Льюїса, а відтак витягував іще більше інформації з урядових баз. У той самий час команда у Форт-Льюїсі почала працювати над складанням повної картини для звіту. Якою є племінна структура регіону, в якому розташований Таджі? Хто й до кого лояльний? На які важелі можуть натиснути американці, щоб зруйнувати союзи, підбурити одну групу проти іншої або переконати третю групу перейти на свій бік?

Мобільна мережа Іраку стала для розвідки золотою жилою. Після усунення від влади Саддама Гусейна послуги контрактного мобільного зв'язку стали популярним бізнесом. Безпровідний зв'язок був дешевшим за традиційний, тому мобільні телефони набули неабиякого поширення. До вересня 2004 року, лише через 18 місяців після початку американської окупації, АНБ розробило секретну методику, яку американські спецпідрозділи називали «знахідкою», позаяк вона дозволяла визначати місце розташування навіть вимкненого стільникового телефону. Кілька років потому військові підрахували, що ця

методика дозволила їм виявити близько тисячі нових цілей, зокрема й багатьох членів іракського підрозділу «Аль-Каїди».

АНБ мало доступ до іноземних телекомунікаційних мереж за угодою з американськими операторами зв'язку. Цим компаніям щедро платили: за словами одного з колишніх керівників, за право доступу агентів до приватних мереж і даних кожна компанія отримувала десятки мільйонів доларів щороку. Деякі компанії операторів зв'язку частково належали іноземним інвесторам. Щоб отримати від федерального уряду ліцензію на роботу в Сполучених Штатах, їм доводилося підписувати контракт, який гарантував американським розвідслужбам безперервний доступ до мереж, що дозволяв реєструвати телефонні дзвінки й записувати розмови. Наприклад, угода, укладена з компанією Level 3 Communications, навіть дозволяла скористатися «рубильником», тобто за наказом американського уряду компанія мусила розірвати всі сеанси зв'язку за допомогою телекомунікаційних кабелів, що йдуть морським дном до США. Це був захисний захід, покликаний блокувати мережу від зараження шкідливим програмним забезпеченням або зупинити передання даних у разі кібератаки.

У деяких випадках інформацію з іноземних мереж зв'язку можна було перехопити навіть з території Сполучених Штатів. Цей спосіб перехоплення даних зазвичай застосовували для аналізу трафіку електронної пошти, велика частина якого проходить кабелями й роутерами, розташованими в США. Якщо АНБ не мало дозволу під'єднатися до лінії зв'язку, воно потай проникало в комунікаційну мережу. У 2005 році у викривальній статті для одного галузевого журналу колишній морський піхотинець, який працював на розвідку за контрактом, зауважив, що мобільний зв'язок і безпровідна технологія передачі даних стали основним методом виходу в інтернет для сотень мільйонів осіб у всьому світі. «Ця тенденція дає силам союзників безпрецедентні можливості, дозволяючи збирати інформацію за допомогою перехоплення пакетів даних у безпровідних мережах, – писав він. – Західні розвідслужби здатні моніторити трафік, установлюючи неавторизовані точки доступу, проводячи цілеспрямоване перехоплення трафіку безпровідних мереж і аналізуючи зібрані дані. Збір інформації за допомогою безпровідних мереж дає унікальну можливість проводити операції в різних країнах без співпраці з місцевою владою».

Переклад: безпровідні телекомунікаційні мережі були мрією шпигунів. І ця мрія втілилася в життя в Іраку.

Стасіо не знав нічого ані про доленосну зустріч в Овальному кабінеті, ані про рішення президента Буша. Проте незабаром він побачить їхні плоди. Завдяки доступу до вхідних і вихідних телекомунікаційних мереж АНБ почало перехоплювати й зберігати інформацію про кожен телефонний дзвінок, про кожне текстове повідомлення або електронний лист, що перетинав кордон країни. Це стало наріжним каменем нової стратегії: збирання всіх даних і виявлення завдяки їм мереж терористів і повстанців.

Телефони ворогів перетворилися на пристрої для стеження. За сигналами з мобільного телефону можна визначити його місце розташування на карті. В Іраку було кілька місць, в яких точна тактична розвідка була такою ж необхідною, як в Таджі – місці дислокації військової бази, до якої належав Стасіо. Головний шлях постачання, шосе Тампа, пролягав через базу й тягнувся на північ у напрямку міста Балада у сунітському трикутнику. Шосе Тампа було найважливішою артерією, яку американські військові використовували для доставки вантажів і палива, тому й становило головну мішень повстанців. Американські солдати прозвали цю дорогу «Алеєю саморобних вибухових пристроїв» (IED).

Стасіо намалював схему шосе Тампа, розділивши його на сектори, спираючись на звіти про активність повстанців. Він створив мережеві діаграми, які завдяки додатковим звітам агентів і американських військових патрулів показали, на яких ділянках території підкладали найбільше вибухових пристроїв. Стасіо позначив певні зони як особливо небезпечні, а також спробував передбачити, ґрунтуючись на інформації про попередні атаки, де саме повстанці найімовірніше спробують атакувати наступного разу. Він класифікував вибухи за видом використаного пристрою. Був це пристрій з таймером чи з дистанційним детонатором, який умикав бойовик, що перебував поблизу? В останньому випадку бойовик переважно залишався у тій самій зоні після спрацьовування пристрою. Стасіо зберігав інформацію про типи вибухової речовини, використаної в деяких вибухових пристроях, сподіваючись вистежити постачальника матеріалів для виробників бомб.

Стасіо систематично складав карту формувань підривників. А потім інші солдати систематично їх знищували. Озброєні новою тактичною інформацією, американські патрулі тепер могли знищити за одну ніч цілі мережі підривників. Вони цілили не лише у керівника терористичної групи, а й у його заступника, а також підпорядкованих їм членів третього і четвертого рівня. Послуговуючись інформацією, наданою Стасіо і його колегами, три американських підрозділи здійснювали ліквідацію мереж підривників. Група Raiders відтепер займалася полюванням на людей.

Стасіо і члени його команди могли також відстежити джерела фінансування ворогів і виявити тих представників суспільства, які підтримували бойовиків. (Деякі колишні можновладці розповідали, що гроші поступали навіть від корумпованих представників іракської влади.) Протягом наступних 15 місяців група усунула з поля битви 450 повстанців. Убили лише двох, які стріляли у відповідь. Усіх решту взяли в полон і допитали. Отриману від них інформацію передали співробітникам розвідслужб у країні. Коли Стасіо поступив наказ покинути Таджі та вирушити на нове завдання, кількість вибухів у цій місцевості скоротилася на 90 %. Шосе Тампа стало безпечним.

Такий раптовий і яскравий успіх не міг залишатися незауваженим. Дейвід Петреус, голова командування американськими силами в Іраку, відвідав Таджі та повідомив бригаді, що її потребують на півночі на базі передового розгортання Warhorse у місті Баакуба, розташованому в неспокійній провінції Діяла. Бригада прибула туди у жовтні 2007 року. Баакуба – це багатонаціональне місто середнього розміру. Стасіо, який місяць тому отримав звання капітана, знав, що місто стало сценою жорстоких боїв у тісних житлових кварталах. Вистеження повстанців і терористів, що ховалися серед цивільних, було значно складнішим завданням, ніж пошук виробників бомб уздовж однієї-єдиної ділянки дороги.

Проте нова розвідувальна машина була створена саме для такої роботи. А в Баакубі їй довелося працювати на повних обертах.

Стасіо і його команда почали зі знищення окремих груп терористів і закінчили ліквідацією терористичних формувань. Вони знайшли чоловіка, який виготовив безліч поясів смертників, використовуваних терористами, і простежили за ним до самої його майстерні. Коли солдати спецназу вибили двері, вони виявили там жінку, що саме

вдягала на себе смертоносну одіж. Виробника бомби й майбутню смертницю заарештували.

Команда також знайшла сховок із кількома тисячами кумулятивних зарядів. Це був найбільший таємний склад, який їм доводилося бачити в Іраку. Ця зброя створена для ураження з відстані та здатна пробивати броньовані транспортні засоби, які повинні захищати солдатів од традиційних дорожніх мін. Заряди були сховані у підвалі звичайного житлового будинку. Стасіо і його аналітики виявили, що ці смертоносні пристрої вчить робити іракців такий собі іноземний громадянин. Його теж заарештували.

Стасіо був лише молодим офіцером. Проте в своїй новій ролі аналітика йому потрібно було з'ясовувати, де зберігалися міни, хто їх виготовляв і хто фінансував виробництво. Перед кожною зустріччю свого керівника з шейхом або місцевим очільником Стасіо мусив робити стислий виклад політичної передісторії, розповідати про заплутані та мінливі місцеві союзи, які американські джерела сподівалися використати задля завоювання «сердець і розумів» іракців.

Іще ніколи у воєнній практиці, наскільки він знав, від офіцера такого низького звання не вимагали володіння такими масивами тактичної й стратегічної інформації, розуміння не лише особливостей поля битви, а й геополітичних реалій війни. Зазвичай подібний аналіз проводили люди із зірками на погонах.

Друзі-офіцери підсміювалися над ним: «Бобе, ти вже відзвітував перед президентом?»

Він сприймав це як комплімент.

Стасіо був лишень одним із багатьох членів розлогої хакерської організації, авангарду нової кібернетичної війни. Після того як Буш віддав відповідний наказ, гібридні підрозділи солдатів і розвідників із бойових і розвідувальних загонів почали проводити в Іраку щоденні атаки. Оперативний центр розташовувався в залізобетонному ангарі на військово-повітряній базі в Баладі на північ від Баґдада, на якій колись перебували іракські винищувачі. Нині тут залишалися здебільшого безпілотні літальні апарати. Їхні оператори працювали спільно з хакерами АНБ, слідчими з ФБР і елітними загонами спецназу. Усі вони були поділені на кластери, але працювали як єдиний, майже живий організм. Хакери викрадали інформацію з електронних пристроїв противника і передавали її аналітикам, які складали для

загонів списки цілей. Коли вони вирушали у рейд, оператори дронів спостерігали за територією за допомогою складних камер і сенсорів, розроблених у ЦРУ, попереджуючи загони про небезпеки. Інколи оператори безпілотних пристроїв самостійно знищували цілі за допомогою ракет.

Після закінчення атаки загони відбирали у захоплених на місці проведення операції бойовиків мобільні телефони, ноутбуки, флешки, списки контактів і паперові записки, так зване кишенькове сміття, на якому могло бути лише ім'я і номер телефону, поштова або електронна адреса. Все це приносили аналітикам, які завантажували інформацію в бази даних і за допомогою програм інтелектуального аналізу шукали зв'язки з іншими бойовиками, зокрема і з ув'язненими. Особливу увагу приділяли пошукові джерел фінансування операцій бойовиків, зокрема від іноземних спонсорів із Сирії, Ірану та Саудівської Аравії.

Співробітники підрозділу викривали від 10 до 20 нових бойовиків щодня. Таким чином виявляли цілі терористичні формування, позаяк представники американських збройних сил почали думати й діяти так само, як ворог. Вони змінили вертикальну ієрархію на вузлові групи відповідно до місцевих умов. Ця структура формувалася під час просування вперед з урахуванням нових методів ведення бою.

АНБ уже вибудувало інфраструктуру для проникнення в телекомунікаційні мережі. Після терактів 11 вересня агентство встановило нові пункти прослуховування і збору інформації для відстежування в кіберпросторі телефонних дзвінків терористів, їхньої електронної пошти та інших засобів цифрового зв'язку. Чимало цих пунктів доступу були розташовані всередині офісів і комутаційних станцій найбільших операторів зв'язку США. Аналітики, які відстежували конкретного терориста, могли бачити, коли він реєструвався у мережі. Вони передавали цю інформацію оперативникам, і ті перехоплювали сигнал у бездротовій мережі. (Якщо наземні загони були дуже далеко, для перехоплення сигналу використовувалися літаки і супутники.) Усі отримані дані швидко зіставляли, щоб визначити розташування цілі аж до конкретної вулиці, будівлі та навіть квартири, з якої робили виклик або надсилали повідомлення.

Звичайному відвідувачеві об'єднаний розвідувальний центр у Баґдаді здавався домівкою різнорідної команди. Аналітики, що працювали за контрактом, із волоссям, зібраним на потилиці в нефор-

мальний хвіст, працювали пліч-о-пліч із солдатами й офіцерами у бойових мундирах. Але якщо цей відвідувач дивився на величезні монітори, підвішені під стелею ангара, на яких демонструвалося зображення з дронів, а потім на роботу команди цивільних і військових, що не відводили очей від екранів ноутбуків і розмовляли один із одним власним жаргоном, він розумів, що опинився в епіцентрі воєнних дій.

У нової стратегії розвідки був іще один наріжний камінь. Окрім збору інформації зі всіх телекомунікаційних мереж у Іраку і використання її для визначення розташування бойовиків та їхніх спонсорів, АНБ почало маніпулювати методами комунікацій, використовуючи мобільні телефони і комп'ютери повстанців – згідно зі сценарієм, викладеним Майком МакКоннеллом президентові Бушу.

Американські хакери надсилали фальшиві текстові повідомлення бойовикам і підривникам. Отримувач такого повідомлення, наприклад, читав: «Зустрінемося на розі вулиці, щоб спланувати наступний удар» або «Вирушай на ось це місце на дорозі та встанови свій пристрій». Коли бойовик приходив на зазначене місце, його зустрічали американські спецназівці або ракета Hellfire, запущена з безпілотного літального апарату з висоти в декілька сотень метрів.

Хакери й аналітики АНБ, працюючи разом із військовими в Іраку, проникли в мережу сайтів і серверів «Аль-Каїди», яку американці назвали Obelisk. Це була корпоративна внутрішня мережа «Аль-Каїди». Терористи публікували в мережі пропагандистські відеоролики, накази щодо наступу й планів ведення «священної війни». Вони навіть оприлюднювали поточні адміністративні матеріали, зокрема інформацію про витрати та особовий склад. Мережа Obelisk була оперативною системою управління повстанців. Проникнувши в неї, хакери АНБ заразили шкідливим програмним забезпеченням форуми джихадистів, вимушуючи читачів натискати на лінки, за якими на їхніх комп'ютерах встановлювалися шпигунські програми. Мережа Obelisk дала шпигунам доступ до секретів «Аль-Каїди» і можливість проникнення в їхні лави.

У вересні 2007 року внаслідок американського рейду в селі Сінджарі, розташованому за 16 кілометрів од іракsько-сирійского кордону, військові отримали масив розвідувальної інформації, зокрема імена агентів «Аль-Каїди», їхні електронні адреси, номери телефонів,

а також адреси сайтів і паролі до секретних чатів членів «Аль-Каїди». Ці дані допомогли розвідці вистежити багатьох бойовиків, захопити їх у полон або знищити. Увійшовши до чатів, аналітики змогли дослідити риторику й образи, які використовувала «Аль-Каїда» для вербування нових бойовиків. Озброєні цією інформацією, аналітики розробили контрпропаганду. Вони залишали повідомлення у різних гілках форумів, запитуючи, чи не порушує «Аль-Каїда» засади ісламу, вбиваючи інших мусульман.

Американські шпигуни почали стежити за окремими пропагандистами. Жахливі відеозаписи, на яких бойовики обезголовлювали своїх полонених – інколи американських контрактників, – були потужним засобом вербування. Відеозаписи знищення американської броньованої техніки вибуховими пристроями стали візитною карткою джихадистів. Американські хакери могли заблокувати пропагандистам доступ до інтернету. Проте це зупинило б ворога ненадовго. Тому вони просто визначали місце розташування комп'ютерів, з яких завантажувалися відеоролики, за інтернет-адресами. А потім спецназ вирушав у те місце, щоб взяти в полон або знищити відеооператора.

Це було вкрай складне завдання – значно складніше, ніж визначення розташування бойовика за сигналом його стільникового телефону. У мережі інтернет можна діяти анонімно. Будь-яка людина може зареєструвати електронну поштову скриньку на вигадане ім'я, за допомогою поштових служб Google або Hotmail, послугами яких користуються мільйони клієнтів, дані яких зберігаються на серверах, розташованих у різних куточках світу. І цих людей досить складно знайти. А просунуті користувачі знають, як скерувати трафік через ланцюжок серверів, розташованих у різних країнах, що зробить визначення їх справжнього місця розташування практично неможливим.

У роки, що передували інтернет-буму, АНБ зосереджувалося на розробці та придбанні програмного забезпечення, яке могло визначати розташування користувачів за інтернет-адресами їхніх комп'ютерів. У ті часи агентство було зацікавлене не в пошуку бойовиків, а в виявленні хакерів, які викрадали секретну інформацію з урядових і корпоративних комп'ютерів, загрожуючи роботі критично важливих об'єктів інфраструктури (наприклад, електричних станцій і фінансових систем). До початку інтернет-буму агентство вдосконалило методи пошуку людей у тумані кіберпростору. Інструменти так

званої мережевої криміналістики допомогли трохи підняти завісу анонімності та демаскувати ворога. Проте аналітикам доводилося застосовувати також старомодні методи розслідування. У АНБ почали досліджувати улюблені методики хакерів, за якими їх можна розпізнати: яке шкідливе програмне забезпечення найчастіше використовують, якими поширеними інструментами користуються для зламування комп'ютерних систем. АНБ придбало програмне забезпечення для криміналістики в технологічній компанії Computer Associates з Нью-Йорка, а також у нового гравця на цьому ринку – компанії NetWitness, розташованої не в технологічних центрах Кремнієвої долини, а в місті Рестоні (штат Вірджинія), ближче до Пентаґону й американських розвідувальних служб, в околиці Вашинґтона. За допомогою цих та інших програм, кілька з яких розробили програмісти розвідуправління, агентство протягом кількох років енергійно займалося питанням ідентифікації користувачів мереж, щоб навчитися визначати розташування людини у реальному світі, ґрунтуючись на її активності в інтернеті. Нишпорки з АНБ вдосконалили ці методи в Іраку й упродовж наступних років застосовували їх для глобального полювання на хакерів.

Кібервоїни в Іраку звернули також увагу на нові мережі, розгорнуті в цій країні. Повстанців магнітом тягнуло в інтернет-кафе, що їх вдосталь з'явилося після падіння режиму Саддама Гусейна, під час якого доступ до іноземних медіа був помітно обмежений. Кібервоїни за підтримки військово-повітряних сил проникали в комп'ютери цих закладів і стежили за тим, яку інформацію оприлюднюють повстанці та з ким спілкуються. Відвідування інтернет-кафе робило бунтівників уразливими, адже там їм доводилося діяти відкрито, а комп'ютери не перебували під їхнім постійним спостереженням і контролем. Щоразу, коли вони виходили в мережу через комп'ютер загального користування, вони піддавали себе ризику бути вистеженими.

Фахівці АНБ розробили операцію під назвою «Полярний бриз» (Polarbreeze) для проникнення у розташовані поблизу комп'ютери за допомогою безпровідного зв'язку. Офіцер американської розвідки міг сидіти в кафе й удавати, що перевіряє електронну пошту, або розмовляє по телефону, або надсилає повідомлення, а насправді за допомогою особливого пристрою викачував дані з комп'ютерів, розташованих за кілька метрів од нього у тому ж приміщенні.

Інколи було простіше вимкнути сервер, ніж відстежити когось крізь нього. Було декілька випадків, коли американські хакери виводили з ладу мережеву інфраструктуру, яку використовували бойовики для відправки електронної пошти або інтернет-спілкування, вимушуючи їх користуватися телефонною мережею, де їх було легше відстежити.

Операція почала набирати обертів і приносити результати, тому АНБ залучало до роботи найталановитіших кібервоїнів. Усі вони працювали в підрозділі під назвою «Відділ операцій з особливим доступом» (Tailored Access Operations – TAO). Із назви зрозуміло, що цей відділ розробляв інструменти і методи зламування комп'ютерів. Усі ці найнепомітніші з американських хакерів були винятковими фахівцями – у TAO працювало лише кількасот осіб, більшість з яких пройшла багаторічну підготовку за розробленою АНБ програмою, інколи ще в коледжах і університетах, яким агентство допомогло складати навчальний план.

У ході однієї успішної операції хакери з TAO звернули погляд на «Ісламську державу Іраку» – терористичне угруповання, створене 2004 року, яке присягнуло на вірність «Аль-Каїді», а згодом встало під її знамено. Ця група воювала з американськими солдатами, але також тероризувала й убивала цивільних мешканців. Лише протягом 2007 року цей підрозділ «Аль-Каїди» убив 2 тисячі іракців і захопив контроль над передмістям Дора у південній частині Баґдада, де спробував установити закони ісламу й заснувати новий «емірат» для контролю мешканців. Місцеві християни, які жили в Дорі протягом десятиліть, були вимушені залишити свої оселі, щоб не опинитися під владою суворого релігійного диктату. Представник нового емірату постукав у двері будинку одного християнина і заявив: якщо він хоче залишитися, то повинен сплачувати податок або прийняти іслам. Або ж покинути свій будинок; представники «Аль-Каїди» запропонували допомогти винести меблі.

Хакери TAO почали вистежувати лідерів цього підрозділу «Аль-Каїди». Зосередившись на операціях у Баґдаді, вони проглядали чернетки всіх електронних листів, які терористи залишали для своїх поплічників в особистих електронних скриньках, але не відправляли через інтернет, щоб не бути виявленими. Але TAO вже кілька років була відома ця хитрість.

Хакери ТАО ввійшли до складу наземних підрозділів під час наступальної операції під назвою «Розривне вістря» (Arrowhead Ripper), яка ставила собі за мету вибити підрозділ «Аль-Каїди» з опорної бази в передмісті Баакуби. В операції, що розпочалась у червні 2007 року, брали участь близько 10 тисяч солдатів, переважно з бази передового розгортання Warhorse, бригада іракської армії, а також близько 500 поліцейських. Операція почалася з наземної та повітряної атаки на Баакубу. Передові загони США знищили близько двадцяти бойовиків лише у перший день. У той самий час у провінції Анбар військові оточили шістьох терористів, підозрюваних у зв'язках із вищими керівниками «Аль-Каїди». У Фаллуджі заарештували трьох потенційних «смертників», а в місті Тармії – трьох підозрюваних у тероризмі.

Американська розвідка добре проявила себе у розшуку цих бойовиків, виявленні їхніх зв'язків із «Аль-Каїдою», розкритті механізмів вербування нових членів і підготовки нападів.

Хакерство у телекомунікаційних мережах, якими користувалися лідери «Аль-Каїди» в Іраку, допомогло ТАО звільнити передмістя Баґдада від терористичної влади, а американським військам – захопити або знищити принаймні десятьох чільників «Аль-Каїди» на полі бою. У середині серпня операція «Розривне вістря» добігла кінця, у Баакубі відновилася законна влада, та й активність повстанців на цій території значно зменшилася. До листопада «Аль-Каїда» залишила район Дори.

Розвідувальна машина продовжила перемагати. За перші шість місяців 2008 року «Аль-Каїда» влаштувала лише 28 вибухів або інших терористичних актів, хоча рік тому подібних атак було близько 300. Кількість жертв терористів серед цивільного населення також скоротилася – від 1500 осіб у 2007 році до 125 в першій половині 2008-го. Один колишній офіцер розвідки порівняв кібератаку на вищі ешелони «Аль-Каїди» з «відрубуванням зміїної голови».

«Ми провели низку операцій із проникнення в комунікаційні системи й структури оперативного управління, які дозволяли терористам і бунтівникам координувати атаки на збройні сили США, – зауважив він. – У цьому полягав ключ до успіху *будь-якої* операції».

Уперше в історії чотирилітньої війни в Іраку Сполучені Штати змогли виробити по-справжньому ефективну стратегію. Загальний успіх заходів, який дозволив американським військовим нарешті залишити Ірак, на думку істориків, військових командирів і солдатів,

можна пояснити трьома основними чинниками. По-перше, додатковий контингент сухопутних військ допоміг взяти під контроль найнебезпечніші райони, знищити або заарештувати «непримиренних» (як називав їх Петреус) і захистити мирне населення Іраку. Рівень насильства в містах знизився, люди відчули, що вони в безпеці, та почали більше співпрацювати з американськими військами. По-друге, групи повстанців, шоковані жорстокими, невблаганними методами «Аль-Каїди» і впровадженням релігійного диктату, виступили проти терористів або почали боротися на боці США на платній основі. Рух так званого Сунітського пробудження об'єднав 80 тисяч бійців, лідери яких публічно засуджували «Аль-Каїду» і підтримували спроби американських військових поліпшити життя іракських громадян.

Проте третя і, ймовірно, найголовніша складова успіху була пов'язана з низкою розвідувальних операцій, проведених АНБ і такими вояками, як Стасіо, санкціонованих Бушем на тій доленосній зустрічі в Овальному кабінеті. Колишні аналітики розвідки, військові офіцери й представники адміністрації Буша стверджують, що санкціоновані президентом кібероперації прочинили двері новим способам здобуття розвідінформації та її використання для наземних операцій. Інформація про пересування й плани противника, витягнута американськими шпигунами з комп'ютерів і телефонів бойовиків, дозволила військовим скласти план дій для пошуку бойовиків, інколи вказуючи дорогу прямо до дверей їхніх будинків. Це була найскладніша з будь-коли створених глобальна система стеження, і працювала вона зі смертельною ефективністю.

Петреус вважав, що ця нова кіберзброя «була головною причиною значного прогресу американського війська» під час наступу влітку 2008 року, яка «надала пряму можливість усунення майже 4 тисяч повстанців із поля битви». Поступ війни в Іраку обернувся на користь Сполученим Штатам. Методи розвідувальних операцій, згодом експортовані до Афганістану, «врятували життя американців і їхніх союзників, допомагаючи виявляти й нейтралізувати екстремістів у обох зонах збройного конфлікту». Пізніше АНБ інтегрувало розроблені в бойових умовах методики до операцій з вистежування терористів, шпигунів і хакерів у всьому світі. Альянс між розвідкою та військовими, викуваний в Іраку, назавжди змінив американські методи ведення війни.

2
RTRG

Під час наступу 2007 року збройні сили США і розвідувальні служби вперше випробували теорію ведення кібервійни на полі битви. Однак смертоносна тактика, випробувана в Іраку, насправді народилася раніше, в один із найпохмуріших періодів у історії АНБ.

Одинадцятого вересня 2001 року генерал-лейтенант Майкл Гейден, тодішній чільник АНБ, за дві години після початку робочого дня отримав телефонний дзвінок, яким його повідомили, що в одну з веж-близнюків у Нью-Йорку врізався літак. Кілька хвилин потому інший літак поцілив у другий хмарочос. Гейден зателефонував дружині Жанін, попросив її простежити за їхніми трьома дітьми, а відтак почав готуватися до закриття штаб-квартири агентства площею 141 га у містечку Форт-Мід (штат Меріленд), розташованому десь за 40 кілометрів од Вашинґтона.

Гейден наказав евакуювати весь допоміжний персонал. Озброєні охоронці з натренованими на пошук вибухівки собаками прочісували територію. Працівники антитерористичного центру, розташованого на вищих поверхах, почали опускати світлонепроникні гардини. Штаб-квартира АНБ переїхала до цього містечка із Вашинґтона ще 1957 року, тому що звідси було досить далеко до міста, щоб пережити ядерний вибух. Нікому й на гадку не спадало, що терористи можуть атакувати за допомогою комерційних літаків.

Насамперед Гейден вирушив до антитерористичного центру, працівники якого не приховували сліз. Усі розуміли, що АНБ проґавило якісь дуже важливі сигнали в «балачках» терористів, які так чудово перехоплювала розлога мережа збору глобальних даних. Електронні «вуха» агентства прослуховували терористів, але не зрозуміли їхніх справжніх намірів. Згодом слідчі виявили, що 10 вересня 2001 року АНБ перехопило телефонну розмову відомого терориста, який по-

переджав арабською: «завтра – час Ч*». Цей запис залишався в архіві агентства неперекладеним англійською до 12 вересня.

Гейден зосередився насамперед на стримуванні будь-яких наступних атак. 14 вересня він дозволив «цілеспрямований пошук», тобто електронний моніторинг комунікаційних зв'язків між Сполученими Штатами та іноземними державами, в яких, як було відомо, діяли терористи, – насамперед Афганістаном, головним осередком «Аль-Каїди» завдяки теократичному режимові «Талібану». АНБ почало відслідковувати номери телефонів, пов'язані з терористами. На практиці це означало, що будь-який телефонний номер в Афганістані, з якого телефонували до США, міг зацікавити іноземну розвідку, а тому його могли прослуховувати. Однак, коли дійшло до прослуховування номерів у Сполучених Штатах, Гейден діяв обачніше. Усередині США прослуховування телефонних номерів дозволене лише за попередньої санкції суду. Гейден знав, що АНБ заборонено шпигувати всередині країни. Проте, як він згадував згодом, він ухвалив «тактичне рішення» скористатися наявними повноваженнями для стеження за іноземною розвідкою, хоча й агресивніше, ніж досі. Гейден обґрунтував своє рішення тим, що один кінець лінії зв'язку був розташований за межами Сполучених Штатів, отже, гра була чесною. Країна опинилася в кризовій ситуації, і в той момент ніхто б не оскаржив такого самовільного збільшення повноважень. Головний юрисконсульт АНБ визнав, що накази Гейдена були законними.

Однак щойно АНБ почала стежити за новими об'єктами, Гейден і його підлеглі стикнулися з, на їхню думку, суттєвими обмеженнями можливості агентства, коли йшлося про розгортання мережі стеження для запобігання іншій атаці. Білий дім хотів знати, що ще може зробити АНБ. Отож Гейден розпитав керівників служб і експертів з електронної розвідки про те, що їм потрібно для ефективної роботи.

Усі вони насамперед звернули увагу на величезну прогалину в організації міжнародної розвідки. АНБ моніторило іноземні загрози. ФБР відповідало за внутрішні загрози. Однак жодна організація не займалася іноземними загрозами, щойно вони входили в США. Це відбувалося почасти тому, що влада хотіла запобігти шпигунству за американцями. Проте ця розумна заборона, закріплена протягом

* Час Ч – військовий термін для позначення початку військової операції.

двадцяти років численними законами і постановами, здавалася тепер самогубною.

АНБ хотіло вдосконалити наявні закони так, щоб вони дозволяли перехоплювати інформацію, яка потрапляла до США транзитом, подорожуючи з однієї до іншої іноземної країни. Згідно з тодішнім правом, якщо агентство хотіло перехопити електронного листа іноземного терориста, який зберігався на сервері, розташованому в Сполучених Штатах, потрібно було отримати ордер. Звісно, у цьому випадку йшлося про міжнародну розвідку, просто інформація передавалася за допомогою оптоволоконного кабелю або потрапляла в базу даних на території США. Працівники АНБ стверджували, що мають право перехоплювати таку інформацію без постанови суду, так само як мають право перехоплювати повідомлення, які зберігалися на серверах в інших країнах.

Однак АНБ хотіло аналізувати більше місцевих комунікацій. Працівники агентства висунули ідею, яка народилася ще 1999 року, в ході підготовки до стримування терористичних загроз під час святкування Міленіуму. Агентство хотіло відстежувати «ланцюги контактів» американських телефонних номерів. Це кропіткий процес з'ясовування, хто кому телефонував і кому далі телефонували ці люди і хто телефонував їм на підставі аналізу записів про телефонні дзвінки. АНБ не знало прізвищ людей, пов'язаних із цими телефонними номерами, проте в агентстві вважали, що ланцюжок контактів допоможе ідентифікувати людей з потенційної терористичної мережі. У той час Міністерство юстиції ухвалило, що ордер потрібен навіть для відстежування так званих метаданих, позаяк ця інформація може стосуватися американських громадян або людей, які легально живуть у країні. Натомість АНБ хотіло відстежувати ланцюжки контактів телефонних номерів у Сполучених Штатах, аби шукати людей, які спілкуються з терористами, незалежно від того, перебувають вони за кордоном чи в країні. Гейден в адміністрації президента наполягав на тому, що за американськими законами метадані не належать до «контенту» і тому не підпадають під сформульовану в четвертій поправці Конституції заборону на несанкціоноване стеження. І справді, 1979 року Верховний суд США ухвалив, що уряду не потрібний судовий дозвіл для запису телефонних номерів, тому що особа добровільно відмовляється від приватності цієї інформації у ту саму мить, коли набирає якийсь номер, зареєстрований у телефонній компанії.

Зі списку побажань працівників АНБ було зрозуміло, що наявний закон про спостереження недієвий, тому що відстав від технічного поступу. Акт про негласне спостереження на користь зовнішньої розвідки (Foreign Intelligence Surveillance Act – FISA), що регулював процедуру шпигунства за американцями, ухвалили 1978 року, коли програмного забезпечення для збору інформації, яке б дозволяло відстежити ланцюжок контактів, іще не існувало. Не було тоді й глобальної телекомунікаційної мережі, в якій США були транзитним пунктом. І не існувало загрози міжнародного тероризму всередині США. Було очевидно, що наступний крок для адміністрації – звернення до Конгресу з проханням змінити законодавство, щоб дозволити АНБ зробити багато того, чого потребували Гейден і його підлеглі.

Однак радники президента Буша не палали бажанням звертатися до Конгресу за дозволом розширити повноваження зовнішньої розвідки, позаяк вважали, що це право належить президентові. Зокрема, віце-президент Чейні був проти того, щоб законодавці почали керувати операціями АНБ щодо «Аль-Каїди». Білий дім турбувало й те, що громадське обговорення змін у законі про спостереження підкаже терористам, як саме їх вистежує АНБ.

Чейні взяв список ідей і, співпрацюючи з директором АНБ і працівниками Білого дому, склав план збільшення повноважень агентства, що його мав схвалити президент. Тест складав Дейвід Аддінґтон, юридичний консультант і права рука Чейні в Білому домі. Нова президентська ухвала дозволяла АНБ відстежувати розмови на території Сполучених Штатів, якщо інший абонент перебував за межами країни і якщо були вагомі підстави запідозрити співрозмовників у тероризмі. АНБ уже не мусило отримувати судовий дозвіл для прослуховування приватних телефонних розмов або відстежування електронної пошти – ця процедура досі тривала від чотирьох до шести тижнів. Тепер АНБ могло йти по гарячих слідах, відстежуючи скільки завгодно комунікаційних каналів, а комп'ютери АНБ могли всю цю інформацію аналізувати.

Буш підписав наказ 4 жовтня 2001 року.

АНБ готувалося до війни, тож миттєво взялося до нових проектів. Агентство створило підрозділ для цілодобового стеження – Центр аналізу метаданих (Metadata Analisis Center – MAC). Він розташувався в дирекції відділу електронної розвідки – у тій частині АНБ, яка

викрадає або перехоплює інформацію з цифрових комунікаційних каналів. До складу нової команди ввійшли досвідчені аналітики й інженери АНБ; кожен із них підписав угоду щодо нерозголошення. Їм виділили офісні приміщення. А сама програма отримала кодову назву «Зоряний спалах» (Starburst). За кілька тижнів, 31 жовтня 2001 року, назву змінили на «Зоряний вітер» (Stellar Wind). Колектив відділу отримав удосталь нової техніки: 50 серверів для зберігання й обробки нових даних, зібраних у рамцях програми «Зоряний спалах». В агентстві не хотіли, щоб хтось здогадався про новий відділ, для якого закуповували велику кількість нового обладнання. Тому представники влади попросили виробника серверів скерувати партію товару, призначену для іншого замовника, до АНБ, нікому не розповідаючи про це. 13 жовтня у супроводі поліцейського ескорту сервери доправили до Форт-Міда.

Під час зустрічей із командою «Зоряного спалаху» 6 і 7 жовтня Гейден підкреслював, що несанкціонований збір інформації, переданої чи отриманої мешканцями Сполучених Штатів, спричинений гострою необхідністю і буде тимчасовим. Проте його слова спростовував бюджет програми у сумі $25 млн – аж надто великий як для програми, що мала тривати лише 30 днів.

Протягом першого тижня після старту програми майже 90 працівників АНБ отримали допуск до роботи. Після підписання ухвали Бушем двоє фахівців з офісу головного юрисконсульта АНБ переглянули програму й визнали її законність. Юридичний відділ не задокументував і не обґрунтував свого висновку.

До 7 жовтня, через три дні після підписання ухвали, новий відділ працював двадцять чотири години на добу, без вихідних, перемелюючи метадані, висмоктані електронними фільтрами АНБ. Двадцять аналітиків і розробників програмного забезпечення працювали в три зміни. Чимало нинішніх учасників програми власноруч вибудовували ланцюжки контактів агентів російської розвідки за часів холодної війни. Тепер цей процес був автоматизований і охоплював членів «Аль-Каїди» та тих, хто надавав цій організації фінансову і політичну підтримку або міг долучитися до терористів.

Якщо аналітик волів відстежити кожну людину в списку контактів об'єкта стеження й усі її зв'язки, потрібно було проаналізувати ланцюжок контактів, що охоплював мільйони осіб. Аналітики називають кожну ланку в ланцюжку контактів «стрибком». Відстеження

кожного такого «стрибка» задля пошуку людей, пов'язаних із вихідним об'єктом, нагадує гру «Шість кроків до Кевіна Бейкона», в якій гравці намагаються знайти зв'язок між цим популярним актором та якимось іншим актором, який знімався разом із ним у кіно або телесеріалі. Відділ звітував Гейденові щотижня, а його заступникові щовечора, і це свідчить про надзвичайну важливість нового методу боротьби з тероризмом.

Центр мав партнерів не лише в АНБ, а й за межами Форт-Міда. Агентство розвідки вибудувало антитерористичну «конвеєрну лінію», щоб надсилати в Центр специфічні завдання й аналізувати результати ланцюжків контактів. ФБР і ЦРУ давали Центрові вказівки щодо вибудовування ланцюжків контактів усередині Сполучених Штатів. Телефонні та інтернет-компанії також почали надсилати АНБ інформацію – записи телефонних розмов і текстові повідомлення, надіслані електронною поштою або через месенджери. Збір даних, які перебували в руках корпорацій, доручили групі спецоперацій із джерелами інформації АНБ – головному посередникові і провіднику співпраці з телекомунікаційними компаніями, інтернет-службами, операторами зв'язку та іншими компаніями, що передавали й зберігали інформацію, потрібну АНБ. Агентство встановило своє обладнання на технічному устаткуванні та інсталювало пристрої стеження на комп'ютерах і мережах, які ці компанії контролювали. Один із провідних учасників програми, компанія AT&T, якій належить величезна частина телекомунікаційних мереж, мала неподалік штаб-квартири АНБ у Форт-Міді секретний підрозділ, який віддавна постачав розвідці інформацію про більшість міжнародних телефонних розмов. У рамцях програми зі збору інформації в межах країни компанія дозволила урядові встановити обладнання для стеження також у своєму офісі в Сан-Франциско.

Не всі компанії здавалися без опору: одна з провідних фірм, Qwest Communications, відкинула вимогу агентства передавати телефонні метадані без судової постанови. Проте більшість компаній підкорялися вимогам агентства, покладаючись на запевнення в тому, що президент санкціонував збір інформації, узаконюючи його. Ці учасники телекомунікаційного ринку стали незамінними партнерами нової глобальної системи спостереження. І лише жменька керівників вищої ланки у цих компаніях знала про шпигунське устаткування АНБ. Працівники корпорацій отримували обмежений допуск до про-

грами й мінімум необхідної інформації, щоб уникнути ризику викриття секретної місії АНБ. Натомість останнє відбирало працівників для роботи в програмі у ручному режимі. Конвеєр набирав обертів. Тридцять днів потому, як президент підписав надзвичайну ухвалу, нова програма стеження працювала уповні. Так народився військово-мережевий комплекс.

Звісно, нові повноваження АНБ, що дозволяли прослуховувати телефонні розмови й читати електронні листи, були важливими, але ще важливішим був масовий збір телефонних і мережевих метаданих, розгорнутий у рамцях кампанії «Зоряний вітер». Людині-аналітикові забракло б часу прослуховувати всі ці розмови й прочитувати таку кількість повідомлень, та й терористи, найімовірніше, спілкувалися б шифрами та не говорили б прямо про те, що й коли планують атакувати. Але вибудовування ланцюжка контактів могло викрити існування мережі, доводячи зв'язок між об'єктами.

Потік метаданих линув у комп'ютери та сховища інформації агентства швидше, ніж його встигали аналізувати. Зрештою, агентству забракло місця для зберігання шпигунського улову та потужностей електромереж для комп'ютерів, які укладали інформацію в зрозумілі схеми. Утім, визначення «зрозумілі» тут доволі сумнівне. Аналітики АНБ вибудовували більші, ніж будь-коли, ланцюжки контактів. Вони переробляли метадані у масивні схематичні системи, які демонстрували зв'язки у вигляді сотень перехрещуваних ліній. Аналітики назвали ці схеми BAG (скорочено від big ass graph, тобто «жирнодупа схема»).

ФБР і ЦРУ також використовували метадані, зібрані АНБ. Ці агентства надсилали до АНБ специфічні запити щодо певного телефонного номера чи електронної адреси (які в АНБ називали «селекторами») або просили надати ширшу інформацію про контакти об'єкта спостереження. В АНБ ці запити називали «наведеннями». ФБР і ЦРУ могли давати «наведення», щоб знайти нові «наведення» і згодом провести власне розслідування. АНБ надавало на запит звіти-підказки, які містили аналіз ланцюжка контактів об'єкта, підозрюваного у зв'язках із терористами, або потенційних зв'язків терористів.

Обмін інформацією між розвідувальними службами не завжди відбувався гладко. Агенти ФБР нарікали, що чимало «наведень» від АНБ вели в глухий кут, зокрема коли йшлося про телефонні номери

людей, підозрюваних у тероризмі, які, на думку агентства, перебували в Сполучених Штатах або мали тут контакти. Проте це командне шпигунство стало простою моделлю об'єднаного центру, створеного шість років потому в Іраку. Створення ланцюжка контактів використала команда військових і розвідників в іракському місті Баладі, полюючи за місцевими повстанцями і терористами. Цю систему випробували в Іраку ще до того, як перший американський черевик ступив на землю країни. У 2003 році, ще до вторгнення Сполучених Штатів, президент Буш уповноважив АНБ шпигувати за співробітниками іракського розвідуправління, причетних, на думку ЦРУ, до терористичної діяльності, яка загрожувала безпеці Сполучених Штатів. (Цю саму заяву вкупі з висновком ЦРУ про вироблення і накопичення Іраком хімічної зброї згодом використали для публічного виправдання війни. Обидві заяви згодом спростували. АНБ припинило шпигувати за іракським розвідуправлінням у рамцях програми «Зоряний вітер» у березні 2004 року.)

Спливали місяці, і створення ланцюжків контактів у АНБ ставало більш автоматизованим. Аналітики розробили програми, які повідомляли про появу в ланцюжку нових людей, за якими варто було простежити. Інформацію про людей, які мали прямі контакти з особою зі списку АНБ, передавали у ФБР або ЦРУ. Зазвичай аналітики відстежували два «стрибки» від об'єкта спостереження. І саме вони визначали, чи слід подавати інформацію щодо контактів, а саме чи включати у звіти імена людей, знайдених у цифрових мережах. Це був важливий момент. Якщо аналітик виявляв, що електронна адреса або номер телефону пов'язаний із громадянином США чи легальним резидентом, згідно із законом слід було припинити аналіз і отримати дозвіл суду на стеження. Якщо в звіті навіть побіжно згадувалася розмова одного з таких американських суб'єктів, працівники АНБ повинні були вдаватися до анонімних описів – наприклад, «американський суб'єкт 1». Ця процедура, названа мінімізацією, була покликана захистити імена невинних американців від попадання у звіти розвідки й запобігти асоціюванню їх із терористами чи шпигунами, а також перешкодити АНБ збирати досьє на американців.

Проте АНБ не цікавила інформація про американців. Сам Гейден називав «справжнім золотим скарбом програми» іноземні розмови, які АНБ перехоплювало з телекомунікаційних ліній і устаткування

в США. Агентство могло шпигувати в усьому світі, не виходячи з будинку.

Згідно зі звітом головного інспектора агентства, від початку програми до січня 2007 року АНБ зібрало інформацію з 37 664 телефонних номерів і інтернет-селекторів, 92 % яких були іноземними. Про збір метаданих у звіті не йшлося, однак, як і під час перехоплення вмісту, увагу приділяли головно іноземним об'єктам. Невідомо докладно, яка саме частка зібраної інформації стосувалась об'єктів у Іраку. Але до 2007 року АНБ створило шпигунську інфраструктуру для збору всіх вихідних і вхідних комунікацій у країні, кожного телефонного дзвінка, кожного текстового повідомлення, кожного електронного листа або публікації в соціальній мережі. Інфраструктура «Зоряного вітру» з усіма її каналами зв'язку й устаткуванням для стеження, встановленим на комутаційних вузлах і в офісах найбільших поставників телекомунікаційних послуг у США, забезпечила АНБ кілька входів у глобальну мережу, а відтак і можливість сканувати й копіювати розмови та текстове спілкування, а також проводити кібератаки. Шпигунські стежки, прокладені «Зоряним вітром» завдяки устаткуванню для електронного прослуховування, використовувалися для доступу до іракських телефонів і комп'ютерних мереж, а також інсталяції шкідливого програмного забезпечення.

Позаяк публічно про це не говорили, лише кілька осіб знало, що ключову роль у перемозі в іракській війні відіграла шпигунська програма, створена для боротьби з тероризмом. Кібермережа, сплетена для стеження за американцями, допомогла військовим США вистежувати іракських повстанців.

Коли цю величезну машину обробки розвідувальної інформації експортували до Іраку, їй дали нову назву: «Регіональний шлюз реального часу» (Real Time Regional Gateway – RTRG). У літанії кодових назв АНБ, відомих своєю абсурдною загадковістю, як-от «Вельвет-рубчик» (Pinwale), «Егоїстичний жираф» (EgotisticalGiraffe), «Ніколи не труси немовлям» (Nevershakeababy), – назва RTRG виокремлюється, бо й справді описує проект. Аналітики складали розвідувальні звіти й пов'язували інформацію в реальному часі, тобто отримували миттєву відповідь на запит; програма зосереджувалася на географічному регіоні, у цьому випадку на Іраку; і це справді був своєрідний шлюз,

портал, через який користувач виходив у віртуальний простір, в якому були видимими всі зв'язки.

Рушійною силою RTRG був генерал Кіт Александер. Ця система стала кульмінацією його кар'єри, спрямованої на те, щоб донести здобутки національної розвідки вищого рівня до безпосередніх учасників бойових дій (те, про що мріяв Стасіо, вперше потрапивши в армію). Ключем до успіху RTRG була здатність системи комбінувати всю вхідну інформацію з рейдів, перехоплених розмов, протоколів допитів, зйомок за допомогою дронів і камер спостереження в єдину пошукову систему. Така собі приватна версія «ґуґла» для нових солдатів-шпигунів.

Засновників у RTRG було декілька. Прототип системи розробила компанія SAIC, давній підрядник Міністерства оборони. Ця компанія, розташована в Каліфорнії, мала такі давні та глибокі зв'язки з шпигунським бізнесом, що її частенько називали АНБ-Захід. У АНБ програмою керував полковник Роберт Гармс із Розвідувального управління збройних сил США. У 2009 році, після звільнення з армії, він почав працювати в SAIC.

Серед розробників програми був також один із найзагадковіших шпигунів кінця XX століття – колишній полковник військово-повітряних сил Педро «Піт» Рустан. Його легендарна й таємнича кар'єра допомагає зрозуміти важливість RTRG для очільників розвідувальних і військових організацій, таких як Александер і Петреус, які вірили в її вирішальну роль в іракській війні. Після атаки 11 вересня Рустан, який 1967 року студентом коледжу втік із комуністичної Куби, залишив вигідну кар'єру в приватному бізнесі та повернувся на державну службу в Національне управління військово-космічної розвідки США, організацію, секретнішу за АНБ, де очолював проекти зі створення шпигунських супутників для армії й ЦРУ. Кадрові офіцери розвідки, які знали Рустана, тримали роти на замку щодо того, чим саме займався він, проте говорили про нього як про справжню живу легенду шпигунської справи й людину, яка рятує людські життя. У 1980-х Рустан розробив технологію захисту військових літаків од ударів блискавки. Працювала вона бездоганно – після впровадження розробки Рустана армія не втратила через блискавку жодного літака. На початку 1990-х Рустан керував спільною програмою Міністерства оборони і НАСА зі створення експериментального космічного корабля для дослідження поверхні Місяця, що отримав назву «Клементина»

(Clementine). Від розробки до запуску супутника минуло лише 22 місяці, і це було дивовижне досягнення інженерної справи й проектного менеджменту, яке посилило репутацію Рустана як людини, здатної досягати у стислі терміни блискучих результатів.

Після атаки 11 вересня його робота була тісно пов'язана з новими функціями військової розвідки. Рустан частенько їздив на лінію фронту, і його добре знали й шанували як секретного воїна Об'єднаного командування спецоперацій. Після ліквідації в Пакистані Усами бен Ладена загоном «морських котиків» учасники операції подарували Рустанові прапор, що майорів над їхньою базою в Афганістані. Після смерті Рустана у 2012 році, Майкл Гейден зазначив у інтерв'ю газеті «Вашинґтон пост»: «Він належав до тих хлопців, про яких ніколи не чує нація, однак саме вони відповідають за безпеку американців».

В інтерв'ю галузевому виданню 2010 року Рустан говорив, що жодна державна структура не шукала закономірностей у розвідувальній інформації, складаючи докупи розрізнені клаптики. Саме це була покликана робити програма RTRG. Він пояснив:

> «Уявіть, що ви в Іраку. Там повстанці. Вони мають телефони і телефонують. Цей сигнал можна перехопити наземно (антенами), у повітрі чи в космосі. Якщо ви достатньо метикуваті, щоб поєднати цю інформацію в реальному часі, ви зможете визначити, де зараз Дік. Він у двадцять третьому районі і щойно сказав, що збирається підкласти бомбу… Інформація з трьох пристроїв надіслана туди, де хтось зможе ухвалити рішення щодо початку операції, і танк, фургон або бійці вирушають прямо на місце. І полковник може сказати: "Ми визначили, що оцей поганий хлопець перебуває ось тут. Ідіть і схопіть його"».

Програма RTRG була унікальною тому, що об'єднувала не лише розвідників, а й інших людей – військових високопосадовців, найрозумніших людей в уряді та фахівців приватних підприємств. Це був рідкісний приклад успішної співпраці в умовах федеральної бюрократичної павутини.

АНБ так добре впоралося з обробкою великої кількості інформації (насправді величезною кількістю), тому що відкинуло традиційні підходи. Замість того щоб намагатися зберігати всю інформацію RTRG у централізованій базі даних і аналізувати її за допомогою

суперкомп'ютерів, агентство використало систему розподілених обчислень. Підприємці з Кремнієвої долини розробили програмне забезпечення, яке розбивало великі масиви інформації на менші блоки, які легше аналізувати, і надсилало кожен блок на окремий комп'ютер. Тепер тягар аналізу величезних обсягів інформації не лягав на одну машину. Працюючи спільно, комп'ютери виконували завдання швидше й дешевше, ніж у разі, якби все навантаження взяв на себе один головний комп'ютер. Цей революційний підхід до обробки інформації дозволив компаніям Facebook, Twitter і Google управляти власними сховищами даних, які від кінця 2000-х експоненціально зростали. АНБ застосовувало той самий метод розподіленого обчислення в програмі RTRG. Система вельми нагадувала пошукову систему Google не лише ззовні, а й зсередини. Трохи згодом АНБ розробило власне програмне забезпечення для розподілених обчислень Accumulo на основі технології Google.

Але законність збирання АНБ величезної кількості електронної інформації вважали вельми сумнівною. Навесні 2004 року юридичний відділ Міністерства юстиції дослідив програму й виявив, що принаймні один із методів збирання інформації не відповідав чинному законодавству. Йшлося про величезну кількість так званих інтернет-метаданих, зокрема інформацію про відправників і одержувачів електронних листів. Фахівці АНБ вирішили, що позаяк ухвала президента Буша дозволяла їм здійснювати пошук за ключовими словами та іншими критеріями, то опосередковано вона дозволяла збирати й інтернет-метадані. На думку юристів агентства і його директора Майкла Гейдена, інформацію не можна було вважати «здобутою», якщо її не переглядали. З погляду закону комп'ютерний збір і зберігання інформації не означали здобуття й аж ніяк не підпадали під визначення «шпигунства» у розумінні агентства.

Коли президент Буш зробив наступний крок і вдруге санкціонував програму попри заперечення Міністерства юстиції, чільники юридичного департаменту почали загрожувати відставкою. Серед невдоволених були голова юридичного департаменту Джек Ґолдсміт, директор ФБР Роберт Мюллер, генеральний прокурор Джон Ешкрофт і його заступник Джеймс Комі, якого президент Обама згодом призначить на місце чільника ФБР Мюллера.

Загроза масових відставок стала унікальним моментом в історії президентства Буша. Якби ці чиновники звільнилися, причини їхніх

рішень зрештою стали б відомими через витоки інформації щодо цього в пресі та розслідування в Конгресі. Американці дізналися б не лише про існування шпигунської програми в країні, а й про те, що вищі чини правоохоронних органів пішли у відставку, тому що вважали цю програму почасти незаконною.

Але всі ці бурхливі пристрасті довкола збирання інтернет-метаданих не вгамували шпигунського апетиту АНБ. Лише сім днів потому, як Буш наказав АНБ припинити масовий збір інтернет-метаданих, представники Міністерства юстиції порадили юридичному департаментові АНБ і представникам підрозділу радіотехнічної розвідки знайти нові законні підстави для перезапуску програми. Цього разу їм довелося звернутися за дозволом суду з контролю зовнішньої розвідки – тієї самої інстанції, яку Буш оминув, санкціонуючи стеження після атак 11 вересня. Представники Міністерства юстиції активно співпрацювали з суддею, шукаючи законні підстави для продовження програми. Гейден особисто двічі пояснював судді, які повноваження потрібні АНБ для масового збору інтернет-метаданих. Отримана судова постанова визначала канали передачі інформації, за допомогою яких може збирати інформацію АНБ, і обмежувала кількість людей, які мають доступ до здобутої інформації. Менш ніж через чотири місяці потому, як президент Буш наказав припинити масовий збір даних з інтернету, АНБ знову взялося до справи. Майбутнє програми RTRG було забезпечене.

Програма RTRG розвивалася, і її регіональні межі розширювалися. Полюючи за спонсорами повстанців і терористів, аналітики почали нишпорити за межами Іраку. Вони відстежили чимало найзухваліших терористичних актів, визначивши навіть конкретних осіб у Сирії, які передавали гроші групам підривників і допомагали забезпечити безпечний перехід територією Ірану новим бойовикам. Коли Петреус дізнався про причетність сирійців, він передав докази цього колегії радників президента Буша, які спілкувалися під час щотижневих відеоконференцій. Розмовляючи зі Стюартом Льові, заступником міністра фінансів із питань боротьби з тероризмом і фінансової розвідки, Петреус наполіг, щоб Міністерство заморозило сирійські активи й заблокувало рахунки країни в міжнародній фінансовій системі. Всі учасники відеоконференції знали, що вимогу Петреуса краще не відхиляти, бо якщо вони вчинять так, генерал поскаржиться прези-

дентові Бушу, з яким спілкувався під час прямих відеоконференцій, що відбувалися щопонеділка о 7:30 за вашинґтонським часом.

Розвідка також виявила докази підтримки Іраном екстремістів-шиїтів у Іраку. Проте цю інформацію використали для ведення війни іншого формату – війни ідейної. Сполучені Штати не мали наміру вторгатися до Ірану або проводити таємні диверсійні рейди для виявлення спонсорів Іраку. Тому розвідка передавала цю інформацію іракському урядові та місцевій владі під час особистих зустрічей.

«Чітке розуміння іракцями того, що іранські елементи підтримували членів найекстремальніших шиїтських угруповань, допомогло налаштувати частину іракців проти втручання Теґерана в справи їхньої країни», – згадував Петреус 2013 року. Американці використали здобуту інформацію у власних пропагандистських цілях, і це мало неабиякий ефект.

Від початку й до того, як останні американські підрозділи в грудні 2011 року залишили Ірак, війна забрала життя майже 4500 американців. Але ця війна також породила новий спосіб боротьби. Відтоді розвідка АНБ і загони спеціального призначення ще не раз працювали спільно. У травні 2011 року, коли загін «морських котиків» висадився в пакистанському містечку Абботтабаді, у таборі Усами бен Ладена, їх скеровували розвідники з АНБ. Елітний підрозділ хакерів агентства, відділ операцій з особливим доступом (Tailored Access Operations – TAO), віддалено встановив шпигунське програмне забезпечення на мобільні телефони агентів «Аль-Каїди» та інших «потрібних людей». ЦРУ допомогло знайти географічне розташування одного з цих телефонів, який указав шлях до табору.

Успішна операція зі знищення Усами бен Ладена була найвідомішою зі сотень інших подібних операцій останніх років. Вона стала новим доказом того, що американські солдати-шпигуни знали віддавна: віднині війни будуть іншими. Хакерство і віртуальне шпигунство використовуватимуться в усіх майбутніх операціях і стануть так само незамінною зброєю, як амуніція, з якою солдати вирушають у бій.

3
СТВОРЕННЯ КІБЕРАРМІЇ

На створення кіберпідрозділу, який так ефективно спрацював у Іраку, знадобилося майже десятиліття. До цього успіху спричинилося чимало людей, але якщо комусь належить особливе визнання за представлення концепції кібервійни американським можновладцям, то це, безумовно, Майк МакКоннелл.

Понад десять років до того, як він переконав Джорджа Буша санкціонувати кібератаки в Іраку, МакКоннелл, що вже мав звання віце-адмірала, керував АНБ, де 1996 року заснував перший підрозділ «інформаційної війни». У штаб-квартирі агентства у Форт-Міді розвідка і військовий персонал спільно працювали над впровадженням нових технологій захисту комп'ютерних мереж – і зламування їх.

За часів холодної війни АНБ стало справжнім експертом у перехопленні супутникових передач, встановленні підслухувальних пристроїв на підводних телефонних кабелях і розшифровуванні секретних повідомлень ворогів Сполучених Штатів. Але тепер, коли Радянський Союз відійшов у минуле, а натомість з'явилася всесвітня мережа, можновладців непокоїла нова туманна загроза. Вони вже знали, що іноземні розвідслужби намагаються проникнути в секретні комп'ютерні мережі уряду. У 1996 року Університет національної оборони провів військову гру з метою проробити можливі «катастрофічні» сценарії, як-от комп'ютерні атаки на банки або електричні мережі США. Того самого року міністр оборони наказав усім підрозділам готуватися до «інформаційних військових атак» на мережі, які належали Пентаґону, але не використовувалися активно, зокрема на телефонну мережу загального користування і інтернет, який Міністерство оборони не лише впровадило, а й винайшло.

Інформаційна війна (термін «кібервійна» ще не набув поширення у військовому жаргоні) стала роботою, наче призначеною для АНБ. Підслухувальні пристрої та обладнання для перехоплення інформації, якими володіло агентство, нишпорили й підглядали у світових

мережах. Суперкомп'ютери працювали двадцять чотири години на добу, намагаючись зламати шифрувальні коди, які захищали інформацію на іноземних комп'ютерах. Фахівці АНБ знали, як вламуватися в мережі. А опинившись усередині, могли навіть знищити її.

МакКоннелл був справжнім лідером цієї місії. Під час операції «Буря в пустелі» (1991 рік) він був радником із питань розвідки голови Об'єднаного комітету начальників штабів Коліна Павелла і став справжньою знаменитістю в колах військової розвідки. МакКоннелл прославився тим, що передбачив вторгнення Саддама Гусейна до Кувейту за день до цієї події. Його прогноз не стримав Ірак від нападу на сусідню країну, проте, безсумнівно, привернув увагу американського керівництва. МакКоннелл майстерно використовував супутникові знімки й перехоплені переговори – плоди праці розвідки – для створення картини того, що відбувається на землі. Куди зараз рухається ворог. Куди він, імовірно, вирушить згодом і що там робитиме. МакКоннелл, уродженець Південної Каліфорнії, був відвертим і привітним у спілкуванні. Він так добре поводився на внутрішніх брифінґах, що Павелл доручив йому проводити щоденні брифінґи для журналістів зі всього світу.

У 1992 році звільнялася посада директора АНБ – президент Джордж Буш призначив адмірала Вільяма Стадмена, вельми шанованого офіцера військової розвідки, на посаду заступника директора ЦРУ. Павелл і міністр оборони Дік Чейні підтримали кандидатуру МакКоннелла. Однак цю посаду міг обіймати лише військовий офіцер зі званням віце-адмірала, натомість МакКоннеллу, якому невдовзі мало виповнитися 50 років, бракувало зірочки на погонах. Тож Павелл і Чейні подбали про його підвищення в званні.

Коли МакКоннелл очолив АНБ, агентство почало шукати шляхи до вирішення складних питань, уникнення ризиків і вивчати потенційні переваги кібервійни.

Першим кібервоїнам АНБ довелося вибудувати своєрідний арсенал, вишукуючи вразливі місця в мережах, програмуванні й обладнанні, які вони могли використовувати для зламування системи, а потому й для зараження вірусами чи установки прихованих бекдорів для проведення майбутніх операцій. АНБ приховувало ці вразливі місця від творців технологій, якими користалося. Якби фахівці агентства розкривали їх, виробники могли б залатати діри, зробивши програми безпечнішими для інших користувачів. Але це позбавило б АНБ

секретного доступу. Принаймні 18 різних організацій у складі агентства збирали інформацію про вразливі місця програм, тримаючи в секреті свої знахідки навіть одна від одної. «Агенти розвідки хочуть захистити свої джерела й методи, – писав анонімний працівник АНБ. – Ніхто насправді не знає, який обсяг знань накопичили в кожному секторі». Без цих знань була б неможливою «повномасштабна національна» підготовка до кібервійни, яка проводилася не тому, що цього прагнуло АНБ, а за наказом Пентаґону.

Під керівництвом МакКоннелла розвиток кіберзброї трохи пригальмовував. Спочатку АНБ захопилося стратегічними перевагами, які могли здобути США у разі проникнення в інформаційні мережі, що стрімко поширювалися світом. Однак можновладців непокоїло те, що будь-яку розроблену ними кіберзброю можна використати також проти Сполучених Штатів. В АНБ працювало чимало блискучих криптографів і програмістів, але в агентстві розуміли, що ввійти на це поле битви доволі легко. Знання про експлуатацію мереж поширювалися так само швидко, як і самі мережі. Було зрозуміло, що кібервійна не стане лише державною прерогативою.

Незабаром кібервоєнна лихоманка вихлюпнулася за межі АНБ. Наприкінці 1990-х військово-повітряні сили почали формувати наступальні кіберпідрозділи під керівництвом спецгрупи, створеної для захисту службових мереж. Армія теж підтримала ініціативу і почала шукати способи «вирубати світло Тегеранові», як висловився один колишній офіцер.

У 1996 році МакКоннелл звільнився з АНБ і пішов на роботу в компанію Booz Allen Hamilton, яка працювала на уряд, і завдяки своєму досвідові та зв'язкам заробив там мільйони. Він створив у Booz підрозділ, який спеціалізувався на – на чому ж іще? – на кібербезпеці. Усе, чого він навчився в АНБ, відтепер він продавав урядові.

23 грудня 2006 року, десять років потому, як МакКоннелл залишив державну службу, в його просторий кутовий кабінет в офісі компанії Booz, розташованому за 30 кілометрів од передмістя Вашинґтона, увійшла секретарка.

– Вам телефонує віце-президент, – доповіла вона.

– Віце-президент чого? – перепитав МакКоннелл.

– Віце-президент Сполучених Штатів.

МакКоннелл підхопився з місця і схопив слухавку. Його колишній шеф Дік Чейні сказав, що президент Буш хоче висунути його

кандидатуру на посаду директора національної розвідки. Це була невдячна робота, і МакКоннелл знав, що від цієї посади вже відмовилися значно впливовіші за нього особи, найвідомішими з яких були Роберт Ґейтс, колишній директор ЦРУ і давній товариш МакКоннелла, який нині обіймав посаду міністра оборони.

МакКоннелл відповів Чейні, що йому потрібно поміркувати і він відповість після Різдва. Він поклав слухавку, а потім зателефонував Ґейтсу, який уже знав про вакантну посаду. МакКоннелл сказав, що візьметься за цю роботу, якщо йому дозволять провести деякі кардинальні зміни в методах роботи розвідки і якщо Ґейтс стане на його бік. Той пообіцяв підтримку.

Коли МакКоннелл звільнявся з АНБ, методи кібервійни перебували у зародковому стані. За його відсутності вони увійшли в підлітковий вік. І МакКоннеллу довелося б ввести їх у доросле життя.

МакКоннелл перебував на посаді директора національної розвідки, очолюючи всі державні агентства розвідки трохи менше двох років. Проте він залишив вагомий слід у розвитку служби, методів шпигунства і кібервійни.

Саме МакКоннелл переконав президента Буша схвалити розроблену АНБ тактику ведення кібервійни в Іраку. Також він був ініціатором суттєвих змін в Акті про негласне спостереження на користь зовнішньої розвідки – законі, який обмежував повноваження АНБ. Сталося так, що, коли МакКоннелл почав працювати на новій посаді, федеральний суддя суду з контролю зовнішньої розвідки, покликаного наглядати за електронним шпигунством, постановив, що для перехоплення розмов між іноземними громадянами, які перебувають за межами США, за допомогою обладнання, розташованого на території країни, потрібний дозвіл суду. Упродовж червня і липня МакКоннелл пояснював законодавцям, що більшість світового телекомунікаційного трафіку проходить кабелями, роутерами й комутаторами, розташованими на території США. Тому, якщо АНБ використовує це обладнання з метою шпигунства за іноземцями, дозвіл не потрібен, адже, зрештою, не йдеться про шпигунство за американцями.

МакКоннелл розповів законодавцям, що у разі, якщо АНБ не дозволять моніторити всі міжнародні комунікації за допомогою розташованого у США обладнання, агентство не зможе стежити за багатьма іноземцями, зокрема за членами «Аль-Каїди» та іракськими

повстанцями. На його думку, не ті були часи, щоб утратити доступ до високотехнологічної інфраструктури, яка стала зброєю у новому різновиді війни, яку вели Сполучені Штати.

Наближалися літні канікули в Конгресі, і демократи, які мали більшість у сенаті та керували Білим домом, не хотіли здаватися неспроможними протидіяти тероризму, якщо не зможуть ухвалити зміни, необхідні АНБ для проведення нових операцій і розвитку. Більшість законодавців нічого не знали про методи кібервійськових операцій, проте представники адміністрації президента віддавна публічно заявляли, що шпигунська діяльність агентства відіграє важливу роль у запобіганні терористичним атакам у Сполучених Штатах.

МакКоннелл вхопився за нагоду й проштовхнув значно більше за незначні поправки в законі. Він хотів переписати Акт про негласне спостереження на користь зовнішньої розвідки, щоб уможливити розширене стеження за групами індивідуальних об'єктів: скажімо, за всім вихідним телефонним трафіком із Ємену. Це було безпрецедентне розширення закону. Конституцію ще ніколи не використовували для виправдання стеження за цілими групами людей. Згідно з четвертою поправкою, влада повинна була назвати людину і місце, за якими потрібно простежити. І хоча Акт про негласне спостереження на користь зовнішньої розвідки дозволяв шпигувати за людьми, особа яких іще не ідентифікована, закон вимагав од влади назвати конкретну особу як об'єкт стеження. Натомість МакКоннелл прагнув дозволу для масового стеження.

Однак насправді АНБ уже мало такі повноваження, поки шпигувало за кордоном і не стежило за американськими громадянами або резидентами країни. Але критики боялися, що зміни в законі дозволять розгорнути широке стеження всередині Сполучених Штатів і АНБ зможе вимагати в американських технологічних компаній доступу до величезних масивів інформації, прикриваючись необхідністю захисту національної безпеки.

Саме це й трапилося. У серпні 2007 року демократи, які вважали, що МакКоннелл і Білий дім загнали їх у глухий кут, неохоче підписалися під законопроектом. А місяць потому АНБ поповнило нову систему збору інформації Prism величезною кількістю електронних листів та інших видів мережевої комунікації, отриманою від американських компаній. 11 вересня 2007 року на борт програми Prism уперше ступила компанія Microsoft. Компанія Yahoo приєдналася

в березні наступного року. Протягом наступних чотирьох років до списку партнерів програми увійшли найбільші американські компанії, зокрема Google, Facebook, YouTube і Apple. До жовтня 2012 року в програмі стеження Prism брали участь дев'ять компаній, які нині відповідають за величезну частину інтернет-трафіку і мають найбільше користувачів у Сполучених Штатах. Лише на Google припадає четверта частина трафіку, що її передають інтернет-провайдери у Північній Америці. На YouTube припадає майже 20 % усього вхідного трафіку в Сполучених Штатах. (Найближчий його конкурент – це Netflix, провайдер інтернет-служби потокового мультимедіа, на який припадає близько третини цього трафіку.) Сервіси електронної пошти, що надаються цими компаніями, використовують мільярди людей у всьому світі. Три роки потому, як Google долучилася до програми Prism, компанія оголосила, що її продукт Gmail використовують 425 млн осіб (актуальніша інформація недоступна). У грудні 2012 року Yahoo повідомила про 281 млн користувачів поштового сервісу. А в лютому 2013 року Microsoft повідомила, що поштовою системою Outlook послуговуються 420 млн користувачів. Apple, яка останньою із відомих компаній долучилася до програми Prism, 2012 року заявила, що того року продала 250 млн айфонів.

Попри масштабність програми Prism, якщо представники влади хотіли отримати вміст повідомлень американців, їм був надалі потрібен судовий дозвіл. Щодо решти світу, гра там велася більш-менш чесно. Суддів, які схвалили Акт про негласне спостереження на користь зовнішньої розвідки, попросили надати «зелене світло» зверненням високопосадовців президентської адміністрації, які визначили досить широкі категорії об'єктів стеження та наводили доволі складні пояснення того, яким чином АНБ забезпечить збір інформації лише щодо зазначених категорій. У теорії це звучало здійсненним, однак насправді агентство частенько навіть не знало, скільки зібраної ним інформації стосується іноземців, а скільки американців. Річ у тім, що визначити національність і місце розташування відправника або отримувача електронного листа, надісланого через мережу інтернет не як окреме повідомлення, а як серія пакетів даних, розділених і розкинутих у мережі найшвидшими і найефективнішими маршрутами, а потім зібраними в одне ціле на місці призначення, неймовірно складно. Місцем призначення часто є не комп'ютер отримувача повідомлення, а сервер поштової служби, яку той використовує, наприклад

Hotmail компанії Microsoft чи Gmail від Google. Позаяк АНБ може й не знати, де саме перебувають відправник і отримувач або хто вони, то й не матиме певності, що шпигує лише за іноземцями.

На перший погляд зміни в законі про спостереження лише посилили шпигунські можливості АНБ. Але водночас агентство отримало більше інтернет-плацдармів, з яких могло вести кібервійськові операції. А з доступом до систем головних поштових та інтернет-компаній АНБ могло збирати більше інформації про ворогів і створювати повідомлення, які здавалися б надійними, а насправді містили віруси та інше шкідливе програмне забезпечення. Інтернет був полем битви, і новий закон дозволив АНБ воювати ефективніше.

Що більше можливостей з'являлося в АНБ, то ширші тенета воно розкидало, інсталюючи прилади перехоплення навіть на комунікаційних підводних кабелях міжконтинентального зв'язку. Агентство почало фільтрувати вміст усіх вхідних і вихідних листів, які проходили територією США, вишукуючи імена, телефонні номери або адреси електронної пошти підозрюваних у тероризмі осіб. АНБ зуміло здолати системи захисту Google і Yahoo, викрадаючи повідомлення під час їхньої подорожі від закордонних приватних дата-серверів компаній до загальнодоступної мережі.

Другий вагомий внесок МакКоннелла у методи кібервійни, кількість яких стрімко зростала, припав на закінчення його служби в АНБ у 2008 році. Після перемоги сенатора Барака Обами на президентських виборах у листопаді МакКоннелл прилетів до Чикаґо, де зустрівся з майбутнім головнокомандувачем у надійному місці місцевого відділу ФБР. Він у загальних рисах змалював нові методи бою. Зокрема, МакКоннелл наголосив на слабких місцях у захисті Сполучених Штатів і розповів про деякі кроки, зроблені адміністрацією Буша для їхнього зміцнення. Згодом, під час особистої зустрічі з Бушем, Обама дізнався, що президент санкціонував низку таємних кібератак на іранські атомні об'єкти, проведених за допомогою комп'ютерного «хробака» Stuxnet. Буш розповів Обамі, що ця саботажна операція під кодовою назвою «Олімпійські ігри» (Olympic Games) була однією з двох шпигунських місій, які, на його думку, новому президентові припиняти не варто. Іншою місією була програма ЦРУ зі знищення підозрюваних у тероризмі та бойовиків у Пакистані за допомогою озброєних безпілотних літальних пристроїв.

Обама визнав важливість обох операцій. А 2009 року також наказав провести нову серію атак вірусом Stuxnet. На відміну від Буша, який волів поволі пригальмувати створення ядерної зброї і підірвати спроможність іранців, Обама хотів спричинити масштабні руйнування на заводі в місті Нетенз*. Сполучені Штати розробили нову версію «хробака», який міг змусити ротори центрифуг обертатися з небезпечною швидкістю. Цей вірус також містив численні нові коди атаки, здатні проникати у різні комп'ютерні програми крізь приховані вразливі місця, не виявлені іранцями. Ці нові можливості зробили вірус зброєю масового ураження. Дослідники звинувачують Stuxnet у руйнуванні тисячі центрифуг у 2009–2010 роках. Але це лише близько 20 % від загальної кількості центрифуг на заводі, а в іранців були запасні центрифуги для заміни тих, що вийшли з ладу. Проте представники адміністрації Обами стверджували, що Stuxnet відкинув іранську програму озброєння на два роки назад. А це значний час, якщо, як здавалось у цьому випадку, Stuxnet розробили для запобігання війні, а не для її початку.

Ці агресивні можливості програми також підвищили ризик виявлення вірусу, що й сталось у червні 2010 року, коли нікому не відома білоруська компанія знайшла перші докази існування комп'ютерного «хробака», який згодом отримав назву Stuxnet. Спочатку дослідники припускали, що помилка в коді вірусу (який, звісно, став складнішим, отже, вірогідність помилок збільшилася) дозволила йому «втекти» за межі мереж, які він був покликаний зруйнувати, коли якийсь інженер із Нетеза під'єднав свій ноутбук до зараженого комп'ютера, а потім забрав пристрій додому чи в офіс і ввійшов у інтернет. Але більшість людей не знають, що оця здатність до поширення, вірогідно, була аж ніяк не помилкою, а специфічною рисою вірусу. Окрім спроможності нищити центрифуги, Stuxnet був створений також для розвідки. Він надсилав інтернет-адреси та імена вузлів заражених комп'ютерів до свого командного центру. Чи потрібні ці можливості зброї, створеній для руйнування машин, не під'єднаних до інтернету? Очевидна відповідь полягає в тому, що творці Stuxnet знали, що вірус не лишиться в ізоляції довго. І, цілком імовірно, вони й не прагнули цього.

---

* У 2002 році супутникові знімки виявили в іранському місті Нетенз підземний дослідний завод зі збагачення урану, що міг використовуватися для вироблення ядерної зброї.

Stuxnet створили, щоб нишпорити в мережах і комп'ютерах Нетенза, вишукуючи цілі для атаки. Працівники заводу також працювали для інших замовників. Якщо заразити їхні ноутбуки «хробаком» Stuxnet і вони візьмуть свої комп'ютери на інші об'єкти, «хробак» виконуватиме свої шпигунські функції на інших ядерних об'єктах Ірану. Stuxnet міг розповісти Сполученим Штатам, на кого ще працювали ядерники, де розташовані інші ядерні об'єкти в Ірані і, можливо, як далеко просунулися ці заводи в справі збагачення ядерного палива. Це б дозволило американцям довідатися про іранську ядерну програму більше, ніж будь-коли довідувався шпигун-людина. Рішення Обами щодо ескалації атак «хробаком» Stuxnet було ризикованим, але надто вже принадною здавалася перспектива зібрати розвідувальну інформацію, щоб знехтувати нею. Не дивно, що МакКоннелл і Буш присвятили стільки часу, щоб розповісти новому головнокомандувачу про методи кібервійни та її переваги.

Термін контракту МакКоннелла добігав кінця, і він готувався повернутися в компанію Booz Allen Hamilton, проте відчував, що потрібно завершити ще одну справу. АНБ зробило значний поступ у кібервійні. Армія розвивала власні можливості. Проте досі не було командира, який би відповідав за їхню спільну роботу. Військові дотримувалися суворої ієрархії, філософія якої ґрунтувалася на переконанні, що під час війни збройні сили діють спільно. Армія і повітряні війська не вступають у бій із різними завданнями й цілями. Вони розробляють спільний план, а відтак воюють разом. На переконання МакКоннелла, у кібервійні повинно бути так само.

Він хотів заснувати нове кіберкомандування на кшталт структури Об'єднаного командування збройних сил, поділеного для виконання завдань у певному географічному регіоні на Тихоокеанське, Європейське, Центральне командування для країн Близького Сходу і таке інше, а також для виконання особливих місій. Війська особливого призначення, які активно співпрацювали з АНБ в Іраку, підпадали під управління Командування особливих операцій США. Натомість Стратегічне командування проводило операції в космічному просторі й управляло ядерною зброєю Сполучених Штатів.

МакКоннелл вважав, що кібервійськовим потрібне власне командування, що дозволило б уповні використати унікальний досвід і можливості кожного підрозділу збройних сил. Військові чільники і представники адміністрації президента поволі звикали до думки,

що майбутні війни вестимуться не лише у фізичній площині, а й в інтернеті. І створення нового командування засвідчило б, що кібервійна – це не минуще явище. МакКоннелл був переконаний, що немає кращого способу зміцнити кіберсили, ніж підпорядкувати їх армійській структурі командування.

Сталося так, що наприкінці жовтня, менш ніж за два тижні до виборів, військові мережі заразив комп'ютерний «хробак», і спричинені ним серйозні ушкодження переконали Пентаґон у ненадійності його власного кіберзахисту. АНБ швидко нейтралізувало вірус і проводило очищення мереж до закінчення президентського терміну Буша. МакКоннелл порадився зі своїм давнім товаришем Бобом Ґейтсом, який погодився залишитися на посту міністра оборони після приходу нової адміністрації. Ґейтс підтримав ідею щодо необхідності кіберкомандування. Проте цього не сталося, поки МакКоннелл залишався на посаді директора АНБ. Офіційний Вашинґтон був зайнятий передачею президентської влади: представники адміністрації Буша «передавали ключі» новій команді та детально пояснювали все, над чим працювали. Але Ґейтс таки взявся до справи. У червні 2009 року він наказав командирові Стратегічного командування США створити нове Кібернетичне командування, або ж КіберКом. Стратегічне командування здавалося очевидним дахом для КіберКома, адже мало номінальні повноваження для координування інформаційної війни між військовими угрупованнями. Але фактично ця місія була покладена на АНБ. Отже, КіберКомом повинен керувати директор АНБ, вважали в Пентаґоні. План полягав у тому, щоб на якийсь час підпорядкувати нове командування, дозволити йому стати на ноги, а потім надати КіберКому статус повноцінного військового командування.

У той час мало хто здогадувався, що тодішній директор АНБ, генерал Кіт Александер, готувався очолити кіберкомандування протягом усієї своєї армійської кар'єри. З часом він розкриється як ерудований знавець технологій, спритний воїн і один із найздібніших у політиці генералів сучасності. А тоді, коли нове кіберкомандування підводилося на ноги, він був одним із найпалкіших його прибічників на Капітолійському пагорбі, у військових колах і в Білому домі.

21 травня 2010 року Александер склав у Форт-Міді присягу як перший командир Кіберкомандування США. На церемонії були присутні Ґейтс і Дейвід Петреус, який очолював тоді Центральне командування. На церемонії не було лише одного «батька-засновника»,

МакКоннелла. Але він уже виконав своє завдання: Сполучені Штати офіційно вступили в епоху кібервійни.

Військово-розвідницький альянс довів свою доцільність під час атак на повстанців і терористів у Іраку. Але що як Сполучені Штати зіткнуться з потужним, організованим іншою державою військовим формуванням на полі битви в кіберпросторі і ця сила даватиме відсіч?

Щоб з'ясувати це, 7 травня 2010 року близько 600 осіб прибуло на базу військово-повітряних сил «Нелліс» у передмісті Лас-Веґаса для участі у «Воєнній грі Шрайвера». Щороку сюжет цієї гри базується на актуальних стратегічних завданнях, що стоять перед збройними силами США. (У 2012 році учасники гри боролися з піратами неподалік Сомалійського півострова.) Розробник цієї гри Шрайвер, чиїм іменем назвали військову базу в Колорадо, був важливою людиною в історії військово-повітряних сил США. Німецький іммігрант Бернард Адольф Шрайвер, або Бенні, 1961 року став американським генералом і був піонером розробки космічних і балістичних ракет.

Серед учасників гри 2010 року були старші армійські офіцери, представники всіх військових командувань, а також військові і цивільні фахівці з кібербезпеки з понад 13 американських урядових організацій, зокрема з АНБ, Міністерства внутрішньої безпеки і Національного управління військово-космічної розвідки, яке відповідає за мережу супутників-шпигунів і, ймовірно, є найсекретнішою з усіх служб розвідки. Були там і керівники технологічних компаній у супроводі політичних задротів, офіційні делегації з Австралії, Канади та Великої Британії (трьох найближчих союзників США), а також один колишній член Конгресу, Том Дейвіс, на виборчому окрузі якого було розташовано чимало великих компаній, що працювали за контрактами на Міністерство оборони і розвідку. У воєнній грі Дейвіс грав роль президента Сполучених Штатів.

Події гри відбувалися 2022 року. «Регіонального противника» в Тихоокеанському регіоні (його не називали, хоча усім було зрозуміло, що йдеться про Китай або Північну Корею) спровокував союзник США. У відповідь противник провів руйнівну кібератаку на комп'ютерні мережі союзника. Той нагадав Сполученим Штатам про двосторонню оборонну угоду, і Вашинґтон мусив реагувати.

Американський генерал, що брав участь у грі, запропонував такий сценарій: поки збройні сили США обмірковували свій перший крок, противник зробив попереджувальний удар, вдаючись до «агресивної, продуманої і рішучої» атаки з метою блокування доступу до комп'ютерних мереж, які американці використовують для зв'язку та відправки наказів.

«Червоні блокують Синіх», – повідомили гравців.

«Сині» готувалися до блокади на воді, але не в інтернеті. Вони знали, як повідомити противникові: «Ми тебе бачимо – відступи». Вони могли сказати це за допомогою радіозв'язку, сигнальних вогнів, звукових сирен. Вони могли згрупуватися з іншими кораблями для демонстрації сили. Вони знали всі рішучі, але не смертельні прийоми зупинки противника, до яких міг вдатися командир, не відкриваючи вогонь у бік ворожого флоту.

Проте єдине, що гравці уміли робити в кіберпросторі, – це атакувати ворожу мережу й знищити її, ігноруючи всі попередження та негайно вступаючи в битву. Вони не знали жодного кібереквівалента командам бойової готовності. Треба було атакувати або ні. Традиційна стратегія стримування тут не діяла.

Було також незрозуміло, має подібну стратегію стримування противник чи хоча б переконаний у її необхідності. Військові стратеги люблять порівнювати кіберзброю з ядерною, тому що обидві спричиняють масштабні руйнування стратегічного рівня та вимагають санкції президента. Однак, коли йдеться про ядерну зброю, існує декілька визначених, взаємозрозумілих прийомів, до яких може вдатися кожна сторона, щоб уникнути необхідності її застосування. Під час холодної війни Сполучені Штати і Радянський Союз підтримували крихкий мир здебільшого тому, що чітко давали зрозуміти одне одному, як саме можуть (і будуть) знищувати противника. Радянський Союз випробував нову ракету, американці демонстрували власну й розповідали про розташування ракет поблизу цілей в Європі, а американський президент відкрито говорив про можливість застосування ядерної зброї, висловлюючи надію, що до цього не дійде. У цьому перетягуванні канатів не бракувало погроз і гучних заяв, хоча обидві сторони потай погодилися, що намагатимуться уникати ядерної війни, а не розв'язувати її. Попереджаючи ворога про наміри, кожна зі сторін давала противникові час відступити, охолонути й зберегти лице.

Але зараз, у цій грі, регіональний противник продовжував зненацька атакувати. Після удару по комп'ютерних мережах американських сил він відправив у космос літальний апарат, щоб взяти «на абордаж» американські супутники, зіштовхуючи їх з орбіти і виводячи з ладу.

Протягом наступних чотирьох днів армійські командири напружено намагалися знайти якийсь розв'язок, щоб уникнути повномасштабної війни, яка, на їхнє переконання, призведе до величезних жертв з обох боків. До них долучилися високопосадовці Міністерства оборони і Білого дому. Американські сили виявили, що у них немає жодних угод з іноземними союзниками на випадок кібервійни, тому й немає плану міжнародної відповіді. Військові звернулися за допомогою до керівників корпорацій. Які технології використовують компанії, щоб послати ворогові певний сигнал і змусити його змінити тактику? Чи існує щось таке, як неворожа кібератака? Ніхто цього напевно не знав.

Ворог уже вирішив, що кібернетичні та космічні атаки – кращий спосіб протистояти агресії сусіда й захиститися від відповіді США. Противник уже «перетнув червону лінію». І він відбився від реакції Сполучених Штатів, які загрузали дедалі глибше, бо надто багато керівників високого рівня висловлювали свої міркування щодо того, які саме дії будуть ефективними або ж законними. Могутня супердержава зменшилася до купки спантеличених і неорганізованих гравців. А найгірше, за словами одного з учасників, було те, що здавалося, ніби саме цього й прагнув ворог. «Ми мимохіть слухняно слідували сценарію, написаному противником, а наша стратегія стримування не мала жодного впливу на його рішення».

Усі воєнні ігри починаються з озвучення низки передумов; сподіваючись, що ці факти матимуть місце в реальному житті, і не розглядаючи альтернативи, гравці ризикують програти. У сценарії «Воєнної гри Шрайвера» Китай або Північна Корея проводили превентивну кібератаку. Звісно, вони могли й не робити цього. Можливо, в реальних умовах противник злякається кібератаки, ба навіть гірше – ядерного удару США. Можливо, один із уроків цієї воєнної гри полягав у тому, що військові повинні ретельно аналізувати передумови, оцінюючи вірогідність того, що інша країна завдасть кібердару першою, і зважити на можливі масштаби руйнувань для обох сторін.

Натомість гра лише зміцнила природну схильність військових до війни. І переконала вищих офіцерів і керівників Пентаґону: якщо кібервійна будь-коли спалахне, це станеться «зі швидкістю світла», практично без жодних попереджень. Відтоді щоразу, виступаючи перед Конгресом або громадськістю чи пресою, вони попереджали про стрімку й руйнівну природу кібервійни. Це переконання стало їхнім кредо, коли йшлося про планування. Сполучені Штати, стверджували вони, повинні готуватися до неминучого конфлікту й удатися до надзвичайних заходів – для оборони і нападу.

Хоч як тривожили наслідки воєнної гри, американську владу непокоїли й реальніші загрози. У травні 2009 року, під час промови, виголошеної в Східному кабінеті Білого дому, президент Обама повідомив, що «кіберзлочинці розважують спроби зламування наших електричних мереж, а в інших країнах кібератаки занурюють у пітьму цілі міста». Обама не сказав, що іноземні хакери насправді вже вимикали світло в Сполучених Штатах. Однак під час приватних розмов деякі розвідники розповідали, що два масштабних знеструмлення у 2003-му і 2008 році – справа рук китайських хакерів. Перше знеструмлення стало найбільшим за всю історію Північної Америки і охопило територію площею понад 240 тис. кв. км, зокрема штати Мічиґан, Огайо, Нью-Йорк і частину Канади. Від аварії постраждало близько 50 млн осіб. Це знеструмлення викликало таку сильну паніку, що президент Буш виступив зі зверненням до нації, щоб запевнити людей у тому, що струм повернеться. І справді, протягом 24 годин електропостачання здебільшого відновили.

Один експерт з інформаційної безпеки, що працював за контрактом на державу та великий бізнес, детально проаналізував китайські шпигунські програми і віруси, виявлені в комп'ютерах замовників, і ствердив, що під час другого знеструмлення китайський хакер, що працював на Народно-визвольну армію Китаю, вивчав енергомережу штату Флорида і, ймовірно, припустився помилки. «Можливо, керівництво доручило хакеру викрасти схему системи, але хлопця занесло і йому закортіло дізнатися, "а що станеться, якщо я натисну ось тут"». Експерт вважав, що хакер випадково запустив каскадний ефект, унаслідок якого вимкнулася значна частина енергосистеми Флориди. «Я підозрюю, що, коли вимкнулася система, хакер сказав щось штибу "Упс, лоханувся", лише китайською».

Компанії, які управляли мережами й електростанціями, категорично відкидали припущення щодо кібератаки, посилаючись на урядові розслідування, які дійшли висновку, що знеструмлення сталося через природні причини, зокрема замикання дротів електропередач через надто високі дерева. Ніхто з офіційних осіб не навів переконливих доказів того, що за знеструмленням стояли китайці. Проте постійні чутки про причетність цієї країни демонструють масштаби параної і страху перед кібератаками у Вашинґтоні.

Окрім імовірних атак на електромережі, владу сильно непокоїла безперервна крадіжка інтелектуальної власності та комерційних секретів американських компаній, зокрема хакерами з Китаю. Александер, який очолив Кібернетичне командування 2010 року, назвав загрозливі масштаби китайського промислового шпигунства «найбільшим в історії перерозподілом багатства». У 2012 року Конгрес був змушений ухвалити законопроект. Це сталося шість років потому, як у комп'ютерах законодавців виявили шпигунське програмне забезпечення, інстальоване, ймовірно, китайськими хакерами. Комп'ютери в офісах кількох комітетів у Палаті представників (зокрема, комітетів нагляду за торгівлею, транспортом, інфраструктурою, внутрішньою безпекою і навіть Бюджетний комітет) також були заражені. Виконавча комісія Конгресу в справах Китаю, яка моніторить дотримання прав людини і законів у Китаї, також постраждала: у більшості комітетських офісів виявили один-два заражених комп'ютери. У комітеті з міжнародних відносин (який тепер називають Комітетом у закордонних справах), що наглядає за зовнішньою політикою США, зокрема і за переговори з Китаєм, виявили 25 інфікованих комп'ютерів і заражений сервер.

У 2012 році на розгляд Конгресу потрапили пропозиції, які, серед іншого, збільшували повноваження уряду для збирання інформації про кібервторгнення і шпигунство в комп'ютерних мережах компаній. Ідея полягала в тому, щоб ділитися з приватним бізнесом інформацією про потенційні погрози, а також спонукати компанії підсилити заходи безпеки. Однак деякі підприємства стали дибки, бо боялися, що законопроект означатиме для них нові витрати, нав'язані згори. Компанії непокоїлися також через те, що співпраця з урядом дасть підставу клієнтам подавати судові позови. Провайдери інтернет-сервісів хотіли юридичних гарантій того, що коли вони передаватимуть інформацію про атаки в Міністерство оборони або

внутрішньої безпеки, то не нестимуть відповідальність за розголошування будь-яких персональних даних, які може містити ця інформація, як-от ідентифікаційна інформація про користувачів або інтернет-адреси людей, чиї пакети даних були перехоплені або чиї комп'ютери опинилися в небезпеці.

Торговельна палата США, впливова комерційна асоціація з глибокими кишенями й довгою історією підтримки республіканців, заявила, що законопроект забезпечить владі «надто великий контроль над заходами бізнес-спільноти із захисту власних комп'ютерів і мереж». У той самий час як консервативні чиновники засуджували закон про охорону здоров'я президента Обами за втручання в приватне життя громадян, Торговельна палата стала найзатятішим опонентом законопроекту про кібербезпеку як чергового прикладу державного втручання. Конгресмени з Республіканської партії стали пліч-о-пліч, і законопроект, який охоплював усі аспекти кібербезпеки, утратив будь-який шанс на життя.

Попри несхвалення Конгресу, президент Обама в лютому 2013 року підписав ухвалу щодо «посилення безпеки й стійкості критично важливої національної інфраструктури». Поняття «критично важлива інфраструктура» навмисне сформулювали широко, щоб охопити ним більшість промислових і комерційних компаній. Президент визначив його як «системи і ресурси, фізичні або віртуальні, так життєво необхідні для Сполучених Штатів, що виведення з ладу або руйнування цих систем і ресурсів матиме руйнівний вплив на безпеку, національну економіку або національну охорону здоров'я чи на їхню сукупність». Згідно з цим визначенням, електростанція, безсумнівно, – це критично важливий об'єкт. Так само як банк. І лікарня. А також потяги, автобуси і транспортні компанії. Чи можна вважати критично важливою інфраструктурою службу доставки UPS? Якщо зважити на те, що чимало підприємств залежать від надійних вантажоперевезень і своєчасної доставки товарів і послуг, тоді цілком можливо.

Цією ухвалою адміністрація Обами заявила Конгресові та підприємцям, що не збирається очікувати на новий закон, що посилить контроль влади над інтернетом. Згідно з президентським наказом, федеральні агентства починали активніше обмінюватися інформацією щодо кіберзагроз із приватними підприємствами; Міністерство торгівлі та Національний інститут стандартів і технології (NIST) зобов'язали розробити стандарти безпеки й заохочувати компанії до їхнього до-

тримання; міністрові внутрішньої безпеки доручили скласти перелік найважливіших об'єктів, «кібератаки на які можуть призвести до катастрофічних наслідків регіонального або державного масштабу».

Білий дім був готовий надалі боротися за новий закон про кібербезпеку. А наразі ухвала Обами давала військовим «зелене світло» на підготовку до кібервійни.

Постанова Обами вкупі з секретною президентською директивою, підписаною п'ять місяців тому і не оприлюдненою, чітко демонструвала, що саме військові керують національною обороною під час кібератак. Так само як збройні сили, які переймають ініціативу у випадку вторгнення іноземної армії або запуску ракет у напрямку американських міст, кіберсили країни встануть на захист у разі цифрових атак і завдадуть удару у відповідь.

Ухвала спростила Міністерству оборони впровадження секретної програми обміну інформацією про шпигунські програми за межами підприємств оборонної промисловості, поширюючи її на «критично важливі інфраструктурні об'єкти», визначені владою. Ще одна директива, відома під назвою PDD-20, окреслила дії військових у разі кібервійни й відповідальність за накази.

Початок будь-якої кібератаки відбувається за наказом президента. Але в надзвичайній ситуації останній може передати свої повноваження міністрові оборони. До прикладу, якщо під загрозою кібератаки опинилася електростанція і немає часу на схвалення президентом стратегії захисту, зокрема на контрудар по джерелу атаки, міністр оборони може віддати наказ самостійно.

Однак у PDD-20 ідеться не зовсім про кіберзахист. Згідно з директивою, військові повинні скласти перелік зарубіжних цілей «державної важливості», які легше або доцільніше атакувати кіберзброєю, аніж звичайною зброєю. Такий собі еквівалент часів холодної війни – високопріоритетні цілі в Радянському Союзі, які піддадуть бомбардуванню в разі війни. Директива PDD-20 не називала конкретні цілі, проте до об'єктів державного значення, звісно, входили телекомунікаційні системи, мережі оперативно-командного управління збройних сил, мережі фінансових організацій, системи протиповітряної оборони і управління польотами, а також критично важливі об'єкти інфраструктури, як-от електричні мережі. Тобто ті самі об'єкти, на які б у разі кібервійни з США націлилась іноземна армія.

Директива також містила інструкції для інших міністерств і служб – Державного департаменту, ФБР, АНБ, Міністерства фінансів і Міністерства енергетики – щодо розробки плану дій у відповідь на «тривалу зловмисну кіберактивність, спрямовану проти інтересів США», якщо «захист мереж або заходи законного примусу неефективні або не можуть бути своєчасно застосовані». Військові також мусили діяти згідно з президентськими інструкціями.

Військові командири і цивільні особи вбачали у PDD-20 правила дорожнього руху в разі кібервійни, важливий документ, який окреслював розподіл повноважень і підпорядкування, а також загальні принципи. Тут ішлося про те, що Сполучені Штати вестимуть кібервійну відповідно до норм міжнародного права для збройних конфліктів: удари повинні спричиняти мінімальні супутні руйнування й відповідати рівню загрози або силі атаки на Сполучені Штати. Військові повинні діяти обачно, щоб не пошкодити й не зруйнувати мережі, ймовірно пов'язані з об'єктом атаки. Вірус або «хробак», створені для атаки на електростанцію в Ірані, не повинні виводити з ладу електростанцію в Китаї. «Ми не хочемо розпочинати Третю світову», – заявила Енн Беррон-ДіКамілло, високопосадовиця з Міністерства внутрішньої безпеки, яка працювала спільно з Міністерством оборони над координацією дій у відповідь на кібератаки в Сполучених Штатах.

Не менш важливо й те, що в PDD-20 були окреслені фундаментальні принципи майбутніх воєн: кібероперації підносилися до рівня традиційних битв, а збройні сили мусили поєднувати кібервійну «з іншими наступальними можливостями США» на землі, у повітрі, в морі та космосі.

Військові відповідали за три види кібермісій, поділених між трьома підрозділами.

Перша місія, покладена на найбільший підрозділ, підтримує й захищає військові мережі в усьому світі – від полів битви в Ірані та Афганістані до вод Тихого океану, де об'єднані сили сухопутних, морських і повітряних військових сил утворювали першу лінію нападу під час будь-якої війни з Китаєм. Ці «сили кіберзахисту», як їх називають військові, запобігають проникненню іноземних противників і хакерів у згадані військові мережі. Спроби вторгнення повторюються по декілька тисяч разів на день, але здебільшого це зондування, а не

справжні атаки і від них можна відбитися за допомогою програм автоматичного захисту. Міністерство оборони також обмежило кількість вузлів під'єднання до інтернету, що допомагає посилити військову оборону. Кожну порцію інформації сканують фільтри, які проходять через ці вузли, шукаючи «хробаків», віруси та інші ознаки спроб вторгнення, як-от вихідний трафік з інтернет-адрес, які, ймовірно, контролюють іноземні війська або розвідувальні служби.

Це повсякденний захист. Сили оборони можуть заробляти справжні зірочки на погони в разі повномасштабної війни, якщо противник США скористається своєю найхитрішою кіберзброєю та залучить до атаки найкращих воїнів, аби вивести з ладу мережі оперативно-командного управління або пошкодити інформацію. Ці кіберудари можуть відбуватися ще до першої перестрілки як прелюдія до традиційних методів битви або ж як складова активної операції. Наприклад, під час війни на Балканах у 1990-х американські хакери проникли в систему протиповітряної оборони Боснії та перепрограмували систему контролю так, що вона показувала зовсім інший напрям руху літаків.

Оборонна місія військових ускладнюється тим, що військові насправді не володіють більшою частиною мережевої інфраструктури і не контролюють її: 99 % електропостачання і 90 % служб голосового зв'язку, використовуваних військовими, надходять через приватні кабельні мережі, маршрутизатори та інші інфраструктури. Захист військових мереж «не стає простішим, тому що ми покладаємося на мережі та системи, які не перебувають під безпосереднім контролем Міністерства оборони», – розповідає генерал-майор Джон Дейвіс, радник із питань військової кібербезпеки в Пентаґоні.

Отже, сили кібероборони створили «мисливські загони», які спільно з кібершпигунами з АНБ і Розвідувального управління працюють над пошуком потенційних погроз для військових мереж. У рамцях цієї співпраці військові мають доступ до бази даних, що містить досьє на кожного відомого хакера в Китаї, – розповів один посадовець із Пентаґону, що працює з постачальником систем стеження. У досьє зазначено, які саме види шкідливого програмного забезпечення любить використовувати хакер, які системи він намагався атакувати й де, імовірно, працює. У деяких випадках досьє містить фотографію, здобуту розвідниками в Китаї або придбану в приватних розвідувальних компаній, працівники яких переслідують хакерів у

реальному світі. Якщо військові ідентифікують хакерів, то зможуть посилити захист потенційних мішеней. Крім того, вони можуть спокусити хакера зайти в систему за допомогою «горщика з медом» (неправдивої або оманливої інформації), а відтак відстежити його дії в контрольованому середовищі. Що довше хакер залишається у системі, намагаючись украсти важливі, на його думку, документи, то довше американські шпигуни можуть аналізувати його методи й знаходити способи протидії.

Підрозділ АНБ, відомий як Відділ порушень, спеціалізується на такому ось стеженні за хакерами, але цим не обмежується. Відділ спостерігає, як хакер зламує комп'ютерну систему в іншій країні, а потім іде за ним. У 2010 році під час операції Ironavenger («Залізний месник») Відділ порушень виявив електронні листи, що містили шкідливу програму, надіслані до урядової організації ворожої країни – однієї з тих, про які АНБ хотіло б дізнатися більше. Аналіз виявив, що шкідливе програмне забезпечення прийшло від союзника США, розвідка якого намагалася зламати систему. Американці дозволили союзникам зробити всю чорну роботу й мовчки спостерігали, як ті викачували паролі та секретні документи із системи противника. Американці побачили все, що побачили союзники, та ще й отримати деяку інформацію про їхні методи шпигунства.

Друга місія військових кіберпідрозділів полягає в підтримці збройних сил під час бою: кібервоїни б'ються пліч-о-пліч із традиційно озброєними товаришами. Вони входять до складу загонів, які беруть участь в обороні та нападі, а також розподілені до всіх військових підрозділів. Кожен загін має особливе завдання, яке залежить від місця служби. Наприклад, кібервоїни військово-повітряних сил натреновані зламувати системи протиповітряної оборони й управління польотами, натомість кіберзагін сухопутних військ зосереджується на наземних операціях, до прикладу, проникає в системи оперативно-командного управління артилерією.

Найсуттєвіша зміна від початків кібервійни полягала в тому, що тепер для здійснення бойових кібератак не потрібно щоразу отримувати дозвіл президента. Згідно з інструкцією щодо визначення цілей Об'єднаного комітету начальників штабів, більшість рішень про те, кого і що атакувати, покладено на голову Кібернетичного командування США. «Визначення цілей у кіберпросторі зазвичай відповідає процесам і процедурам, застосовним під час традиційного

визначення цілей», – зазначено в інструкції. Іншими словами, відтепер військові не бачать великої різниці між кіберзброєю, ракетами, бомбами і кулями. Військові командири повинні пам'ятати про «унікальну природу кіберпростору, відмінну від традиційного фізичного світу», а саме про вірогідність спричинення кіберзброєю масштабних супутніх руйнувань.

Ці загони підтримки мають навички також із суміжних сфер, а це означає, що в майбутніх війнах армійські хакери можуть без особливих проблем перескочити до військово-повітряної місії. Під час іракської війни армійські оператори зламували стільникові телефони повстанців і надсилали їм недостовірні повідомлення, позаяк з повстанцями боролися піхотинці. Але кібервоїни повітряних сил також уміють вводити ворога в оману, тож нічого не стоїть на заваді, щоб і їм вступити в гру, якщо армійці заклопотані іншими битвами. Так само кібервоїн військово-морських сил, навчений зламувати навігаційні системи ворожого підводного човна або «підсмажувати» корабельні радари, може спричинити хаос у комерційній телекомунікаційній мережі.

Третє головне завдання полягає в захисті самих Сполучених Штатів і покладене на так звані Сили національної кібермісії. Останні проводять лише наступальні операції. Вони вступають у бій за наказом президента або міністра оборони, якщо, скажімо, Китай наважиться вивести з ладу електростанцію або якщо Іран спробує змінити бази даних провідних банків чи систем фінансових операцій. Члени Сил національної місії навчені перенаправляти трафік шкідливого програмного забезпечення від об'єкта атаки, вторгатися в мережі у разі потреби або відбивати атаки на джерело загрози й виводити його в офлайн. Ці сили підпорядковуються Кіберкомандуванню США, яке пов'язане з АНБ і його хакерським Відділом особливого доступу. Сили національної кібермісії – це лише крихітна частинка військових кіберсил, імовірно, близько одного відсотка кіберармії, хоча точна цифра засекречена.

Пентаґон «з максимальною швидкістю розробляє метод впровадження наших служб» у трирівневу структуру кіберсил США, розповідає Дейвіс. З 2011 року військові беруть участь у регулярних кібервоєнних іграх на авіабазі Нелліс, де відбувалася стратегічна «Воєнна гра Шрайвера». Влада заснувала у кожному військовому командуванні об'єднані центри кібероперацій під керівництвом генерал-

полковників чи адміралів, організовані за географічним принципом. Нині всі центри обладнані системами надзвичайного конференц-зв'язку, тому в разі загрози або початку кібератаки на Сполучені Штати військові, Міністерство оборони, розвідка і дипломати можуть зв'язатися з президентом і Радою національної безпеки, що виконує під час кібервійни функції Кабінету міністрів, щоб ухвалити план дій у відповідь. Існує також система оперативно-командного управління для американських кібератак, а також надзвичайна лінія зв'язку між Вашинґтоном і Москвою – кібернетичний аналог «червоного телефону» часів холодної війни.

Отже, основна інфраструктура для ведення кібервійни була розбудована. Сполучені Штати почали збирати армію.

Щоб створити кіберармію, військові мусили насамперед завербувати найкращих воїнів. Для кожного виду збройних сил розробили тести на визначення здібностей за зразком корпоративних тестів, щоб з'ясувати, доручити новобранцеві технічне обслуговування і захист мереж або ж рідші, але складніші наступальні місії. Усі допоміжні підрозділи запровадили базові курси з кібербезпеки для нових офіцерів; у військово-повітряних силах таке навчання вже було обов'язковим. У п'яти військових академіях запровадили нову дисципліну – методи ведення кібервійни. З 2000 року кращі хакери з кожної академії змагалися один з одним у щорічній воєнній грі, спонсором якої виступало АНБ. Ця гра покликана не лише зіштовхнути лобами різні навчальні заклади, а й перевірити характер майбутніх бійців у протистоянні з кращими кібервоїнами держави.

«Ми створювали мережу з нуля, а потім захищали її від команди з АНБ», – розповідає Мартін Карлайл, викладач комп'ютерних наук в Академії військово-повітряних сил і директор академічного Центру досліджень кіберпростору. Битва тривала два з половиною дні. У 2013 році академія скерувала на змагання команду з 15 курсантів (фахівців у комп'ютерних науках та інженерній справі), які виступили проти «червоної команди АНБ» (так у військовій грі називався агресор), що складалася з близько 30 військових офіцерів, цивільних фахівців і підрядників АНБ. Команда агентства не мала дозволу використовувати проти курсантів будь-які секретні техніки зламування, проте проводила операції, в яких, імовірно, курсантам доведеться брати участь, якщо Сполучені Штати колись таки вступлять у повно-

масштабну кібервійну з іноземною армією. «Червона команда» АНБ спробувала проникнути в мережу військово-повітряних сил (ВПС) і змінити найважливішу інформацію, щоб курсанти більше не могли бути упевнені в її достовірності. Вони запустили в мережу курсантів відомі комп'ютерні віруси і спробували встановити в їхніх системах бекдори.

Команда ВПС перемогла двічі поспіль у змаганнях 2012–2013 років, хоча з 2001 року перемагала лише чотири рази.

Майбутні фахівці з кібербезпеки ВПС США проходять спеціальне навчання на авіабазі Кіслер, розташованій в долині Міссісіпі на узбережжі Мексиканської затоки. Щоб стати пілотом, потрібно закінчити льотну школу, і так само майбутні кібервоїни повинні перейти крізь усі тернії навчання, перш ніж отримають емблему кіберпідрозділу – пару срібних крилець, перехрещених блискавками, на тлі земної кулі.

Наступний і найважливіший крок у навчанні кібервоїнів – це стажування на робочому місці, «з пальцями на клавіатурі», – розповідає генерал-лейтенант Майкл Басла, керівник підрозділу інформаційного домінування і головний фахівець із питань інформації військово-повітряних сил. Поняття «інформаційного домінування» охоплює пропаганду, дезінформацію і комп'ютерні операції. А головний фахівець із питань інформації – це головний технар організації, відповідальний за актуалізацію та підтримку мереж. Фахівці з технічного обслуговування мереж у військово-повітряних силах працюють пліч-о-пліч із фахівцями із захисту цих мереж, а також із тими людьми, які проводять атаки. Це одне велике об'єднання технарів.

Приблизно 90 % кіберпідрозділів ВПС (в яких станом на 2013 рік служило близько 12 600 осіб) працює на оборону. Вони охороняють мережі, латають уразливі місця та намагаються стежити за оновленнями в програмному й апаратному забезпеченні, які можуть створювати «діри» у захисті. Менше 1 % кібервоїнів військово-повітряних сил займаються тим, що Басла називає «вишуканою» роботою з проникнення в комп'ютерні системи ворога.

У цієї диспропорції є дві серйозні причини. Насамперед, напад значно складніший за оборону. Їхні інструменти й методи здебільшого однакові. Але наказати захиснику піти та зламати надійно захищений ворожий комп'ютер – це наче попросити автомеханіка, хоч би яким обдарованим він є, відремонтувати двигун реактивного

літака. Він може розуміти засадничі принципи, проте застосування теорії на практиці – значно складніше завдання.

Друга причина такого маленького відсотка наступальних операцій полягає в тому, що військові зробили ведення кібервійни пріоритетним завданням зовсім нещодавно. Захист військових мереж і комп'ютерів, кількість яких за останніх 15 років значно зросла, тривалий час був частиною цієї місії. Нині акцент змістився, позаяк кібервійна інтегрована до загальної військової доктрини.

Проте якщо колись почнеться війна, американська кіберармія зіштовхнеться з не менш підготованим й у кілька разів більшим ворожим військом.

Групи хакерів із Китаю діють понад десять років. Кілька перших зразків їхньої роботи датовані 1999 роком, коли американські війська ненавмисно розбомбили китайське посольство в Югославії під час війни в Косово. Розлючені «хакери-патріоти» зламали сайти Міністерств енергетики, внутрішніх справ і Служби національних парків США. Хакери замінили контент сайтів антиамериканськими лозунгами: «Протестуйте проти нацистських дій США! Протестуйте проти брутальних дій НАТО!». Білий дім зазнав масованої DDOS-атаки*, під час якої сервер не міг упоратись із вхідним трафіком. З обережності Білий дім вимкнув сервер на три дні.

Нині ці групи китайських хакерів, мотивовані відчуттям національної гордості й опором іноземному війську, отримують накази від керівників китайських військових і розвідувальних служб. Вони не виступають під прапором Народно-визвольної армії, яка таємно надає їм підтримку й водночас не зауважує їхнього існування. Останнім часом робота хакерів полягає здебільшого у викраданні інформації. Китайські хакери проникали або намагалися зламати секретні комп'ютерні системи кожного міністерства або підрозділу федерального уряду. Вони зламали незліченну кількість баз даних, викрадаючи комерційні таємниці. Так само як ті хакери, які 2007 року проникли в мережі підрядників Міністерства оборони, вони вишукують будь-які клапті інформації (малі чи великі), які дають Китаю

* DDOS-атака (*англ.* [Distributed] Denial-of-service attack) – напад на комп'ютерну систему з метою зробити її недоступною для постійних користувачів.

військову або економічну перевагу та сприяють глобальній стратегії розвитку країни.

Китайські хакери талановиті й невтомні. А також безсоромні. Вони частіше нехтують замітанням слідів, ніж їхні американські противники. Почасти тому, що знають: американський уряд не оголошуватиме, що його найважливіші торговельні партнери й кредитори стали жертвами глобальної шпигунської кампанії. Але китайці вважають кібершпигунство і кібервійну тактичними прийомами, що допомагають їхній країні конкурувати з передовішими економічними, військовими і розвідувальними організаціями. Вони не надто переймаються голосом сумління, зламуючи системи конкурентів, бо знають, що це одна з небагатьох можливостей отримати бодай якусь перевагу над противниками. Китай не має океанської флотилії, здатної вести бойові дії в Світовому океані. Але у нього є кібервійсько, спроможне завдати шкоди американським об'єктам з іншого кінця світу.

Китайське кібервійсько, так само як аналогічні підрозділи в Росії, розробило технології зламування американських військових літаків. Зокрема, китайці винайшли метод упровадження комп'ютерних вірусів через безпровідний зв'язок у системи трьох моделей літаків, які військово-повітряні сили США використовують для спостереження та розвідки. За допомогою електромагнітних хвиль хакери атакують бортові системи спостереження. Це геніальна й потенційно руйнівна тактика: такий удар може вивести з ладу системи керування літаком, спричинивши авіакатастрофу.

Проте ці досягнення можна було передбачити. Упродовж століть китайці вдосконалювали стратегію асиметричного удару, перемагаючи сильніших противників за допомогою атаки їхніх слабких місць звичайною зброєю. Кібершпигунство і кібервійна – це просто найновіші приклади у довгій традиції, якою так пишаються китайці.

Однак говорити про китайських хакерів, як про групу, трохи неправильно. Вони не працюють як єдиний колектив, і принципи їхньої організації досі невідомі. На відміну від американців, китайці не оприлюднюють свою кібервійськову ієрархію та структуру командування. Проте, розробляючи методи протидії, американські фахівці з безпеки часто вважають хакерів єдиною організацією, яку об'єднують спільні риси – національна гордість, віра в економічне шпигунство як інструмент розвитку нації, а також відданість стратегії асиметричної

сили. Американські експерти в галузі безпеки дали орді китайських кібервоїнів назву – «підвищена постійна загроза» (Advanced persistent threat – APT). Саме вона, на думку американської влади, відповідальна за глобальне поширення шкідливого програмного забезпечення, яке заразило або намагалося заразити кожну важливу комп'ютерну систему в США. Кожна американська компанія, що працює за кордоном і має справи з Китаєм, або в Китаї, або з будь-яким із китайських конкурентів, може бути впевнена, що перетворилася на мішень. Багато хто навіть не здогадується про це. Більшість компаній не зауважує проникнення у власні мережі принаймні місяць.

Точна кількість китайських кібервоїнів невідома, але неофіційно експерти погоджуються з двома фактами: ця армія дуже велика, ймовірно, десятки тисяч осіб, і, на відміну від американців, китайські кібервоїни орієнтовані здебільшого на напад.

У 2013 році Джо Стюарт, директор відділу вивчення шкідливого ПЗ компанії Dell Secure Works, розповів виданню Bloomberg Businessweek про те, що відстежив 24 тисячі інтернет-доменів, на його думку, орендованих або зламаних китайськими кібершпигунами для проведення операцій, націлених проти влади США й американських компаній. Важко полічити точну кількість хакерів, однак Стюарт ідентифікував триста видів шкідливого програмного забезпечення та технік зламування, використаних китайцями, і це удвічі більше, ніж він виявив у 2012 році. «З їхнього боку була залучена величезна кількість людських ресурсів».

У 2013 році фірма Mandiant, що досліджувала питання комп'ютерної безпеки, оприлюднила приголомшливий звіт, в якому ідентифікувала й виявила місце перебування однієї підозрілої хакерської групи з APT, відомої під назвою «Підрозділ 61398» (Unit 61398) – китайська військова кодова назва, – що базувалася в Шанхаї. Один із головних операційних центрів групи розташовувався в 12-поверховій будівлі площею понад 1200 кв. м, здатній вміщати близько двох тисяч осіб. Компанія відстежила діяльність «Підрозділу 61398» від 2006-го до 2013 року і виявила, що група зламала системи близько 150 організацій. Mandiant вважає цю групу одним із найпродуктивніших шпигунських підрозділів Китаю. Інші експерти у галузі комп'ютерної безпеки пов'язують діяльність групи з вторгненням у мережі канадського відділення компанії Telvent, яке розробляє промислове програмне забезпечення для управління вентилями та системами безпе-

ки для нафтових і газових компаній у Північній Америці. Керівництво Telvent виявило, що із системи викрали файли проектів. Хакери могли використати цю інформацію для побудови схеми мереж нафтогазових компаній і пошуку їхніх слабких місць.

«Підрозділ 61398» становив серйозну загрозу і був явно зацікавлений потенційними атаками на критично важливі об'єкти інфраструктури. Але це була лише одна з двадцяти хакерських груп, яку відстежили в Mandiant. Китайські хакери здебільшого зайняті шпигунством. Проте учасники цих груп завиграшки можуть перемкнутися в режим кібервійни й почати виводити з ладу системи, знищувати інформацію або запускати шкідливе ПЗ у мережі таких критично важливих об'єктів інфраструктури, як-от електростанції та телекомунікації. Якщо у кожній із цих двадцяти груп працює навіть удвічі менше хакерів, ніж у «Підрозділі 61398», тоді китайська «підвищена постійна загроза» (APT) складається з понад 20 тисяч осіб.

Щоб зрівнятися кількістю з кібервійськом Китаю, Сполученим Штатам потрібно подолати чималий шлях. У 2013 році у відділі особливого доступу – елітному хакерському підрозділі АНБ – працювало близько 300 осіб. У штаті Кіберкомандування США, відповідального за координацію всіх військових кіберпідрозділів, служило близько 900 осіб, до них належали адміністративні працівники й офіцери, які не займалися активними хакерськими організаціями. До кінця 2016 року Міністерство оборони планувало збільшити штат кібервійська до 6 тисяч осіб. Якби Китай припинив нарощування кіберсил, кількість китайських кібервоїнів, однак, принаймні у п'ять разів перевищувала б кількість американських фахівців.

Для збільшення кібервійська США командири планують перевчити захисників мереж на воїнів. До прикладу, у військово-повітряних сил більшість учасників кіберкоманди – це технічний персонал і системні адміністратори, тобто різновид служби технічної підтримки.

Проте ці фахівці – усе, що військово-повітряні війська мають нині. А розширяти штат кіберпідрозділів планів немає. Правда у тім, що у військово-повітряних силах нині служить найменше осіб, ніж будь-коли, і ця кількість зменшується через рішення про скорочення військових витрат 2013 року. Кіберкомандування США, яке наглядає за всіма кібероперaціями, також планує вийти з лав допоміжного персоналу. Уряд намагається автоматизувати більшість функцій тех-

нічної підтримки військових мереж, плануючи вивільнити персонал для наступальних операцій.

«Бракує фахівців із критично важливими навичками», – каже генерал-майор Джон Дейвіс, старший військовий радник із питань кібернетичної політики в Пентаґоні. Військове відомство не може платити своєму персоналові стільки, скільки платять у приватному секторі, де найкраще підготовані військові хакери можуть заробляти принаймні удвічі більше, працюючи на підрядників уряду. «Військово-повітряні сили ніколи не виграють війни пропозицій» у бізнесу, каже Марк Мейбері, старший науковий співробітник військового відомства. Те саме стосується інших військових підрозділів. І в цієї проблеми немає очевидного розв'язку. Армія не має грошей, щоб завербувати нових кібервоїнів. А Конгрес не палає бажанням підвищувати зарплату навіть тим солдатам, що служать.

Військові переконали коледжі та університети в необхідності навчання методам кібервійни так, як це роблять ВПС. Лише кілька навчальних закладів прислухалися до них. Але більшість ставиться до комп'ютерного хакерства як до сумнівної справи. «Університети не хочуть цього навчати, вони не бажають мати репутацію закладів, де навчають людей хакерства», – розповів журналістам Стівен ЛаФонтен, співробітник АНБ, який допомагає розробляти нові навчальні програми. І коли вчорашні студенти потрапляють на роботу до агентства, виявляється, що вони не вміють працювати за стандартами АНБ. «Нам доводиться вчити їх технічним основам, які, як ми вважали, вони повинні були отримати в навчальному закладі, а потім навчати специфічних навичок, пов'язаних з їхньою місією», – сказав ЛаФонтен.

АНБ знайшло однодумців у кількох університетах, яким допомагає складати навчальні програми. (Студенти, які хочуть навчатися за цим курсом, повинні пройти ретельну перевірку й отримати право доступу до секретної інформації. У рамцях курсу вони відвідують секретні семінари в АНБ.) Агентство також допомагає деяким студентам оплатити навчання на бакалавраті з комп'ютерних наук і пройти курс з основ інформаційної безпеки – агентство навіть видає їм ноутбуки й виплачує щомісячну стипендію. Натомість після закінчення навчання такі студенти йдуть працювати до агентства. Більшість таких навчальних закладів, від Принстонського університету до невеличких місцевих коледжів у майже кожному штаті, не навчають того, як

здійснюються кібератаки. Цю частину бере на себе АНБ, навчаючи вчорашніх студентів, які починають на нього працювати.

Іще до вступу студентів до коледжу військові спонсорують клуби кіберзахисту й змагання для школярів, такі як програма «Кіберпатріот» – загальнодержавне змагання для учнів середніх і старших класів. Програму спонсорують підрядники Міністерства оборони, як-от Northrop Grumman і SAIC – компанія, що створила прототип RTRG. Партнери змагання – організації бойскаутів, «Клуби хлопчиків і дівчаток Америки», а також програма підготовки молодих офіцерів запасу, члени «Цивільного повітряного патруля» і загони Корпусу морських кадетів. Дейвіс називає цю програму «можливістю [для молодих людей] зробити свій внесок у забезпечення цивільної і економічної безпеки нації».

Але, щоб залучити найталановитіших, АНБ доводиться конкурувати з приватним бізнесом, який відбирає працівників із кращих навчальних закладів, де навчають комп'ютерних наук, зокрема зі Стенфордського і Карнегі-Меллон університетів. Представники бізнесу їздять на найважливіші щорічні з'їзди хакерів Black Hat і Def Con, які відбуваються у Лас-Веґасі. У липні 2012 року директор АНБ Кіт Александер виступив із промовою на Def Con, закликаючи всіх хакерів об'єднати зусилля з його агентством, працюючи в ньому або співпрацюючи з його командою. Чимало хакерів працювали на компанії, що займалися комп'ютерною безпекою, але деякі були фрилансерами, які заробляли собі на життя тим, що шукали дірки в системах безпеки, а потім попереджали виробників або розробників, аби ті могли їх залатати. Щоб сподобатись аудиторії, Александер змінив армійську уніформу на джинси і чорну футболку. «Це найкраща у світі громада зі сфери кібербезпеки. У цьому залі таланти, потрібні державі для захисту кіберпростору, – сказав він хакерам, багатьох із яких правоохоронні органи США могли б назвати злочинцями. – Інколи, хлопці, вам шиють кримінал, – вів далі Александер. – На мій погляд, те, що ви робите для пошуку вразливих місць у наших системах, – просто чудово. Ми повинні знаходити й усувати їх. Саме ви, хлопці, захищаєте передову».

Проте Александер був не єдиним вербувальником у Лас-Веґасі. Керівники й представники компаній, що працюють у галузі кібербезпеки, роздавали у конференц-залі власні брошури й фірмові фут-

болки. Серед них були й колишні працівники АНБ, яких агентство зробило висококласними хакерами.

Наступного літа програма вербування для Александера ускладнилася, позаяк стався витік інформації: колишній працівник АНБ, якого в агентстві навчили хакерства, оприлюднив величезну кількість документів, у яких ішлося про таємні спроби агентства шпигувати в усьому світі, зокрема й про програму, що дозволяла агентству збирати записи всіх телефонних розмов у США, і про іншу програму збирання даних, отриманих від найбільших світових технологічних компаній, серед яких були Google, Facebook і Apple. Звісно, те, що АНБ шпигує, секретом не було, але масштаби цього шпигунства приголомшили навіть деяких хакерів (а що вже казати про пересічних людей). Def Con скасував запрошення Александера і його виступ на наступному заході. Натомість той з'явився на конференції Black Hat, де його різко розкритикували.

4
ПОЛЕ БИТВИ – ІНТЕРНЕТ

До того як очолити Кіберкомандування США у 2010 році, Кіт Александер уже п'ять років удосконалював методи радіоелектронної розвідки на посаді директора АНБ. Він був здібним технічним фахівцем. «Коли він розмовляв із нашими інженерами, то занурювався в деталі питання так само глибоко, як і вони. І розумів усе, про що вони говорили», – розповів один із колишніх керівників АНБ. Пізніше, коли в 2007-му і 2008 році до законодавства США внесли зміни, які відкрили розвідці ширший доступ до комунікаційних мереж, Александер відчув сприятливу політичну ситуацію та перетворив АНБ на безперечного лідера інтернет-шпигунства. Агентство отримало повноваження та кошти на створення загону хакерів. Формально хакери були працівниками служби розвідки, які лише спостерігали за комп'ютерними мережами. Але після підпорядкування їх Кіберкомандуванню хакери ставали солдатами. Вони вільно переходили від однієї місії до іншої, стираючи межі між шпигунством і бойовими діями. Зокрема, одна з таких хакерських груп стала секретною зброєю АНБ.

Найобдарованіші та найдосвідченіші хакери агентства працюють у Відділі особливого доступу (Tailored Access Operations – TAO). За різними оцінками, кількість працівників цього відділу коливається від принаймні 300 до 600 осіб, щоправда, це друге припущення може стосуватися не лише хакерів, а й аналітиків і служби підтримки.

Кілька груп у межах TAO вирішують різноманітні завдання, пов'язані зі шпигунством і кібератаками. Одна група веде спостереження, складаючи карту комп'ютерних мереж, що належать об'єктам стеження, і вишукуючи їхні вразливі місця. Інша – досліджує найновіші хакерські методи й техніки проникнення в захищені комп'ютерні мережі. Ще одна група розробляє методи проникнення в телекомунікаційні мережі. Хакери з цієї групи створюють інструменти контролю над відеокамерами, зокрема встановленими на ноутбуках, промисловими системами управління, пристроями, які регулюють роботу

енергомереж, ядерними реакторами, греблями та іншими інфраструктурними об'єктами. Також існує група, яка здійснює атаки на комп'ютерні мережі спільно із відділом технологічного менеджменту ЦРУ, який допомагає АНБ вламуватись у важкодоступні мережі, для проникнення в які потрібна людина, що власноруч встановлює вірус або шпигунську програму, скажімо, за допомогою USB-носія.

Відділи ТАО розташовані у Форт-Міді (штат Меріленд), у будівлі під ретельною охороною. Щоб потрапити всередину, працівники мусять пройти процедуру сканування сітківки ока й ввести шестизначний цифровий код перед величезними сталевими дверима, що охороняються озброєними людьми. Хакерський підрозділ – одна з найсекретніших організацій у розвідницький спільноті. Лише кілька працівників АНБ мають такий високий рівень допуску до секретної інформації, щоби знати, що саме роблять у ТАО, або можуть увійти до фортеці відділу у Форт-Міді.

У хакерів ТАО одне-єдине завдання: будь-що проникнути в мережі противника. Вони викрадають або зламують паролі, встановлюють шпигунські програми, інсталюють бекдори і співпрацюють із мережею агентів ЦРУ – роблять будь-що, аби здобути інформацію. Це шпигунство заради досягнення двох цілей. Перша – здобути секрети конкурентів США або ж друзів їхніх ворогів. Друга – зібрати інформацію, яка допоможе знищити комп'ютерні мережі та пов'язану з ними інфраструктуру, якщо президент будь-коли накаже зробити це. На інтернет-полі битви ТАО стежить за потенційними мішенями. Якщо надійде наказ атакувати, хакери допоможуть провести цю операцію.

Влада США й експерти зі сфери розвідки вважають, що ТАО встановив шпигунські пристрої принаймні у 85 тисячах комп'ютерних систем у 89 країнах світу, як випливає із секретних документів, оприлюднених колишнім співробітником АНБ Едвардом Сноуденом. У 2010 році ТАО провів 279 операцій. Саме цей підрозділ зламав криптозахист, використовуваний поширеними системами електронної пошти, зокрема BlackBerry, щоб шпигувати за користувачами в усьому світі. Справи зайшли так далеко, що комп'ютери, які поставлялись об'єктам стеження, спочатку привозили до АНБ, де на них встановлювали шпигунське програмне забезпечення. Розповідаючи про свої звершення, фахівці ТАО хвалькувато використали в презентації

PowerPoint дещо змінену версію всім відомого логотипу фірми Intel: «TAO Inside».

Більшість власників заражених комп'ютерів навіть гадки не мають, що за ними стежать хакери TAO, тому що цей підрозділ покладається на так звану вразливість нульового дня, тобто невиявлені користувачами недоліки комп'ютерної системи, відомі лише хакерам. Агентство купує інформацію про ці вразливості на тіньовому ринку в хакерів, які виявили їх, інколи сплачуючи по декілька тисяч доларів за кожну інформацію. Іноді АНБ платить компаніям – розробникам програмного забезпечення та комп'ютерів за приховування інформації про вразливі місця або бекдори у їхніх продуктах, щоб агентство й хакери з TAO могли використовувати їх.

Проникнувши у такі комп'ютери, хакер зможе прочитати й скопіювати будь-які незашифровані документи, зокрема текстові файли, електронну пошту, аудіовізуальні файли, презентації, списки контактів – геть усе. Зашифровану інформацію прочитати важче, але можливо. Зрештою, одним із завдань АНБ є зламування кодів, і агентство лідирує в цій справі вже понад 60 років.

Чи не єдине завдання, з яким хакери TAO впоратися не можуть, – це шпигунство в країнах з обмеженим доступом до інтернету. Саме тому Північна Корея перебуває за межами досяжності елітного підрозділу. Комунікації цієї держави зі зовнішнім світом такі обмежені й так ретельно охороняються та відстежуються, що TAO має мізерні шанси туди проникнути.

А ось про Китай цього не скажеш.

Китай – це одна з найважливіших мішеней у програмах стеження та планування кібервійни АНБ. І хоча уряд Китаю вдався до широких заходів, щоб контролювати доступ до інтернету й активність у мережі в межах країни, Китай – це велика країна зі стрімким технологічним розвитком, що робить її вразливою.

Дослідник історії розвідки, журналіст Метью Ейд довідався, що TAO «майже 15 років тому успішно проникнув у китайські комп'ютерні та телекомунікаційні системи, отримуючи звідти найважливіші й найнадійніші розвіддані про те, що відбувається в Китайській Народній Республіці». Насправді, саме TAO надав урядові США докази того, що Китай проникнув у комп'ютерні мережі оборонних підрядників та інших американських компаній. З таємних документів АНБ

випливає, що агентство націлилося на мережі китайської компанії Huawei – найбільшого у світі виробника телекомунікаційних пристроїв. Керівники розвідслужб і деякі американські конгресмени роками підозрювали Huawei у співпраці з військовими відділами та розвідкою Китаю. Американські організації контролю заборонили установку телекомунікаційного обладнання Huawei, зокрема комутаторів і маршрутизаторів, у країні, позаяк боялися, що китайці використають це устаткування для кібершпигунства.

Едвард Сноуден розповів китайським журналістам, що АНБ зламало комп'ютери Пекінського університету Цінхуа – одного з провідних освітніх і дослідницьких центрів країни. Сноуден назвав це зламування масштабним. Він показав журналістам документи, які свідчили про те, що в січні 2013 року АНБ проникнуло принаймні до 63 університетських комп'ютерів і серверів. За словами Сноудена, ці документи доводили втручання АНБ, позаяк містили IP-адреси, які могла отримати лише людина, яка мала фізичний доступ до комп'ютерів.

Навіщо АНБ було зламувати комп'ютери китайського університету? Журналісти, з якими розмовляв Сноуден, знали, що Університет Цінхуа – це домівка освітньої та дослідницької мережі Китаю – державної комп'ютерної системи, що містить «інтернет-дані мільйонів китайських громадян». Можливо, це було однією з причин того, що АНБ прагнуло проникнути в систему. Однак американські аналітики й дослідники вважають, що китайські університети – це основний ресурс кадрів для уряду й органів влади. «Підрозділ 61398» Народно-визвольної армії Китаю, розташований у Шанхаї, «активно вербує юні таланти на науково-технічних факультетах навчальних закладів, зокрема Харбінського інституту технологій і Коледжу комп'ютерних наук і технологій провінції Чжецзян», вважають у фірмі Mandiant, що працює у сфері комп'ютерної безпеки. «Більшість "кодів професій" для посад, на які "підрозділ 61398" набирає персонал, вимагають високого рівня володіння комп'ютерними технологіями».

Цілком імовірно, що, зламавши комп'ютери Цінхуа, АНБ намагалося дізнатися імена китайських новобранців або ж довідатися більше про методи їхнього навчання. Факультет комп'ютерних наук і технологій Університету Цінхуа пропонує програми навчання для бакалаврів, магістрів і аспірантів. Згідно з міжнародним дослідженням, Цінхуа є провідним університетом континентального Китаю в

сфері комп'ютерних наук і посідає 27 місце в світовому рейтингу. Університет відкрито називає себе передовою організацією. АНБ і Міністерство оборони США зберігають у базі даних усіх відомих хакерів, що працюють в Китаї. Якщо агентство хотіло знайти майбутніх китайських хакерів, які роблять перші кроки на цьому полі, було цілком логічно почати пошук у Цінхуа.

Китай – це найбільша мішень останніх років, однак не єдина, на яку націлилися хакери ТАО. Вони допомагали вистежувати сотні терористів «Аль-Каїди» і повстанців під час іракської операції 2007 року. Саме цього року хакери отримали нагороди від керівників АНБ за роботу зі збирання розвідданих щодо стану іранської програми ядерного озброєння. Метью Ейд пише, що «ТАО стало бажаним місцем роботи», як стверджує нещодавно звільнений працівник АНБ. Працівники, які прагнуть кар'єрного зростання або професійного визнання, жадають перейти до ТАО, де матимуть безліч можливостей проявити себе в електронному шпигунстві. Тереза Ші отримала посаду голови департаменту радіотехнічної розвідки – одну з найпрестижніших і найважливіших посад в агентстві – саме завдяки роботі, яку виконувала як керівничка підрозділу ТАО, якому до снаги збирати інформацію, що не може здобути жодна державна організація.

Служба в хакерському підрозділі допомагала працівникам здобути значні професійні переваги й досвід, завдяки якому вони могли згодом отримати прибутковішу працю в галузі кібербезпеки у приватному бізнесі. Колишні співробітники ТАО йшли працювати на державних підрядників, зокрема на розробника програмного забезпечення SAP, у Lockheed Martin або в такі відомі корпорації, як Amazon; вони створювали власні приватні фірми у галузі кібербезпеки, проводили за контрактом хакерські операції проти компаній та іноземних груп, що намагалися вкрасти особисті дані клієнтів приватних компаній.

У ТАО працювали елітні хакери АНБ, але еліта еліти скупчилася в одному з його підрозділів. Офіційна назва цього підрозділу – Центр віддалених операцій (Remote Operations Center), хоча інсайдери називали його просто ROC – вимовляється як «rock» (англ. скеля, камінь).

ROC – це домівка найкваліфікованіших і найдосвідченіших хакерів країни, які працюють у Форт-Міді або в представництвах центру в Колорадо, Джорджії, Техасі та на Гаваях, поза зоною досяжності вашинґтонських політиків. Згідно з таємним бюджетом АНБ, у 2013-му фінансовому році центр отримав $651,7 млн на зламування комп'ютерних систем у цілому світі. Це вдвічі більше, ніж витрати всіх розвідувальних структур, які працюють на захист військових і секретних комп'ютерних мереж США від атак.

Формально передбачалося, що Кіберкомандування США співпрацюватиме з військовими командуваннями для ведення кібервійни. Але насправді під час операцій зі спостереження та нападу ROC і Кіберкомандування працювали пліч-о-пліч і ROC зазвичай відігравав провідну роль. Діяльність ROC нерозривно пов'язана з кібервійною, адже атаці завжди передує спостереження. Цей підрозділ мав дозвіл на розвідку в системах і мережах і надавав Кіберкомандуванню інформацію про об'єкти атаки. А позаяк обидві організації підпорядковуються одній особі – директорові АНБ, який сидів на двох стільцях, очолюючи ще й Кіберкомандування, ці структури могли співпрацювати без особливих проблем.

У регіональних центрах активно стежили за іноземними ворогами і навіть за союзниками. У другій половині 2009 року невеличка команда Гавайського центру націлилася на високопріоритетні об'єкти з «Аль-Каїди». Хакери, так само як і під час кібероперацій в Іраку, зламали електронні пристрої терористів і вивели військових на їхній слід.

Під дахом регіональних центрів також проводилися найсумнівніші шпигунські операції проти союзників США. У травні 2010 року команда центру в Сан-Антоніо (штат Техас) відзвітувала про успішне зламування поштового сервера президента Мексики та його адміністрації. У надсекретному звіті, що стосувався операції під назвою Flatliquid, члени підрозділу TAO вихвалялися тим, що отримали «вперше в історії доступ до публічної електронної адреси президента Феліпе Кальдерона». Команда співпрацювала із ЦРУ та шпигунськими групами в американських посольствах у Мексиці, перехоплюючи телефонні розмови й текстові повідомлення у мексиканських мережах.

Той самий сервер електронної пошти також використовували члени мексиканського кабінету міністрів. Отже, американські шпигуни отримали доступ до «дипломатичних, економічних і політичних

переговорів, що дозволило поглянути зсередини на політичну систему Мексики та її внутрішню стабільність». Кальдерон, надійний союзник США, мимохіть став «цінним джерелом інформації».

Ця операція була особливо підступною, адже Кальдерон активно співпрацював із розвідувальними, військовими і правоохоронними органами США, борячись із небезпечними мексиканськими наркокартелями, які вбивали представників правоохоронних органів і захопили практично всі мексиканські міста, тероризуючи їхніх мешканців. Керівники американської розвідки, розповідаючи про американо-мексиканські стосунки, щоразу вихваляли Кальдерона й відкритість його уряду до співпраці з американцями, які забезпечували мексиканську розвідку інформацією про наркокартелі, зокрема передавали записи розмов, перехоплених тим самим агентством, яке шпигувало за мексиканським президентом.

Річ була не в тім, що американський уряд сумнівався у бажанні Кальдерона перемогти у війні з наркотиками. Проте американці хотіли впевнитися, що він виконує всі свої обіцянки і що йому не загрожує небезпека, яку він не може виявити або якій не може запобігти. Такий собі патерналізм укупі з поблажливістю – здається, американці вважали, що ситуація в країні аж надто нестабільна й наодинці Кальдерон не впорається.

Утім, Америка пильнувала власні інтереси, шпигуючи за Кальдероном. Представники американської влади вважали, що наркокартелі можуть поширити свій терор за межі Мексики, на територію Сполучених Штатів, ба навіть скинути уряд Кальдерона або послабити його владу так, що Мексика стане нестабільною державою. Влітку 2012 року АНБ отримало доступ до електронної пошти кандидата в президенти Енріке Пенья Ньєто, який обійняв посаду президента в грудні того самого року. У надсекретному документі АНБ ідеться також про перехоплення телефонних розмов самого кандидата, його «дев'яти найближчих помічників» і понад 85 тисяч текстових повідомлень, надісланих Ньєто та наближеними до нього особами. Шпигуни скористалися графічною програмою для візуалізації зв'язків між абонентами, за допомогою якої визначали найважливіші контакти. За цими людьми спостерігали пильніше.

Сказати, що в АНБ не усвідомлювали чутливих політичних аспектів власної діяльності, означає неправильно витлумачити те, чим займалося агентство. Хоча шпигунство проти союзників США – оче-

видне зловживання довірою, це стандартна шпигунська практика, а керівники й працівники АНБ наполягають, що лише виконують накази президента, його адміністрації і законотворців. Усі вони двічі на рік розробляють і ухвалюють документ із переліком основних питань, відповіді на які повинні надати АНБ та інші розвідслужби. Спостереження за внутрішньою роботою мексиканського уряду важливе для підтримки безпеки в обох країнах – вирішили в адміністрації президента Обами. АНБ не шпигувало за Мексикою з власної волі, а виконувало поставлене завдання.

Поєднання професійного досвіду і людських ресурсів розвідслужб і військових відомств унаслідок співпраці підрозділу ROC і Відділу особливого доступу – головна особливість кібервійни: вона розмиває кордони між розвідувальними і військовими операціями. Згідно з американськими законами, розвідслужби можна залучати до проведення секретних операцій, що порушують закони та суверенітет інших країн, якщо причетність уряду США залишається в таємниці. Військові операції проводять із дотриманням міжнародного військового законодавства, і хоча вони не завжди відкриті, проте завжди прозоріші й зрозуміліші, ніж робота розвідки. Одночасне проведення обох операцій ускладнює завдання юристів і керівників, адже визначити, коли операція повинна проводитися згідно із законами та постановами, що регулюють діяльність розвідки, а коли – за військовими законами, доволі складно. На практиці рішення ухвалюють керівники АНБ усіх рівнів і особисто директор, який поєднує функції шпигуна в агентстві та солдата в Кіберкомандуванні.

Ця взаємозамінюваність шпигуна й солдата віддзеркалює зміни у світі сил особливого призначення, в якому військовий спецназ, навчений веденню бойових дій, вирушає на секретні розвідувальні місії. Операція зі знищення бен Ладена проводилася під керівництвом голови Об'єднаного командування спеціальних операцій, адмірала Вільяма МакРейвена, хоча, згідно із законом, спецоперацію мусив очолити директор ЦРУ Леон Панетта. На практиці це означало, що Панетта сидів у своєму кабінеті в Ленґлі (штат Вірджинія), звідти віддав наказ про початок операції МакРейвену і наглядав за перебігом операції. Проте не викликає сумніву, що саме МакРейвен насправді керував операцією і саме його солдати виконали завдання. Однак це правове розмежування було доволі важливим. По-перше, уряд

США міг заперечити свою причетність до операції, якщо б її розкрили. По-друге, США могли обійти деякі військові закони, а саме домовленість щодо того, що жодна держава не може вторгатися на територію іншої країни (йшлося про Пакистан, де переховувався бен Ладен), якщо вони не перебувають у стані війни. Однак перетворення солдатів на шпигунів – це поширена практика. Те саме відбувається в кіберпросторі.

Насправді АНБ не могло провести жодної хакерської операції без допомоги ЦРУ. Співробітники ЦРУ здійснили понад сто нелегальних дій із вторгнення на фізичні об'єкти й установки шкідливого або шпигунського програмного забезпечення в комп'ютерні системи іноземних урядів, військових відомств і корпорацій, зокрема телекомунікаційних компаній і операторів інтернет-послуг. Віддалений доступ до таких комп'ютерів – доволі складна справа навіть для АНБ.

Ці секретні вторгнення проводить Спеціальна служба збору інформації, об'єднаний відділ ЦРУ й АНБ зі штаб-квартирою поблизу міста Белтсвілля (штат Меріленд), звідки можна дістатися АНБ за якихось 10 хвилин. За часів холодної війни ця група, яка займалася прослуховуванням керівників Комуністичної партії Радянського Союзу та країн Східного блоку, здобула репутацію навіжених відчайдухів. Членів групи порівнювали зі спритними злодіями-акробатами з телесеріалу «Місія нездійсненна» (Mission: impossible) і фільму з такою самою назвою. Подейкують, вони скеровували на вікна лазери, записуючи розмови людей у приміщенні, та прив'язували підслухувальні пристрої до голубів, які товклися на зовнішніх підвіконнях радянського посольства у Вашинґтоні.

Нині Спеціальна служба збору інформації працює з 65 локацій, тобто «постів прослуховування», в американських консульствах і посольствах. Її нові мішені – це терористи у віддалених районах, в яких складно розмістити підслухувальний пристрій, а також уряди іноземних держав, які створюють власні кіберармії, особливо в Китаї і Східній Азії. (Александер відрядив кількох підлеглих працювати з кібервійськом в Іраку, щоб полювати на повстанців і терористів.) Ця група надає неоціненну допомогу АНБ, створюючи спільно з ним цифрові плацдарми, необхідні для прослуховування важкодоступних комунікаційних мереж і пристроїв, а також для запуску їх у разі потреби, знищення або виведення з ладу цих систем під час кібератаки. Кілька років тому Спеціальна служба збору інформації здобула доступ

до комутаційного центру, що обслуговує декілька оптоволоконних магістральних ліній в одній південноазійській країні. Отже, АНБ дістало змогу перехоплювати повідомлення військових керівників країни, а також мало доступ до її телекомунікаційних артерій. Унаслідок подібних операцій американці досягнули одразу дві мети – встановили стеження й організували плацдарм для проведення кібератак. АНБ потай перебирало на себе управління комп'ютерами в цих країнах, щоб згодом використовувати їх для запуску шкідливого програмного забезпечення та замести сліди, які вели до Сполучених Штатів. Кілька десятків секретних співробітників ЦРУ, навчених проведенню нелегальних операцій зі встановлення шпигунського ПЗ, нині працюють на повну ставку в штаб-квартирі АНБ у Форт-Міді.

ЦРУ також створило власний хакерський відділ – Центр інформаційних операцій (Information Operations Center – IOC). Згідно з бюджетним документом, оприлюдненим Едвардом Сноуденом, протягом кількох останніх років ця група розрослася і тепер у ній працюють сотні людей, що робить її однією з найбільших груп у ЦРУ. Згідно з документами, IOC здійснює кібератаки та вербує іноземних шпигунів, які сприяють проведенню операцій.

Інтернет перетворився на поле битви. Протягом останніх років альянс солдатів і шпигунів посилився, а територія спільних бойових дій – розширилася.

Вони перенесли до Афганістану методи «полювання», які довели свою ефективність в Іраку. Хакери АНБ вступили в зону бойових дій і працювали пліч-о-пліч із бойовими загонами, оточуючи й знищуючи бойовиків «Талібану». В рамцях програми «Рухома тінь» агентство прослуховувало мобільні телефони та визначало місце розташування бойовиків у Афганістані, використовуючи «іноземну точку доступу», як сказано в секретній документації. Проте в систему аналізу завантажувалася й інша інформація: наприклад, результати соціологічних опитувань, звіти про рух транспорту та навіть вартість продуктів на місцевому ринку. Аналітики намагалися відслідковувати настрої суспільства й знайти зв'язки, наприклад, між зростанням ціни на картоплю та спалахами насильства. Результати були неоднозначними. Один американський можновладець заявив, що ця система може «передбачити майбутнє», визначаючи час і місце атак «Талібану» з 60–70-відсотковою точністю. Інші зневажливо називали систему па-

фосним і дорогим експериментом з інтелектуального аналізу даних, від якого насправді не варто чекати жодних корисних результатів, заявлених прихильниками програми.

Однак, попри суперечливу ефективність програми, вищі військові чини в Афганістані були переконані, що саме кібервійна дала вагомі результати, і, коли війна затягнулася, трохи підняли завісу над зазвичай секретними операціями. «Можу вам сказати, що, як командувач в Афганістані 2010 року, я проводив кібероперації проти своїх противників і вони були успішними, – розповів генерал-лейтенант ВМС Річард П. Міллз під час виступу на технологічній конференції у Балтиморі в серпні 2012 року. – Я міг увійти у ворожу мережу, заразити оперативно-командний центр і захистити себе від майже невпинних спроб проникнути в мої лінії зв'язку й перешкодити нашим операціям». У той час Міллз був найвищим за посадою офіцером ВМС в Афґаністані та керував бойовими операціями в південно-західній частині країни. У публічних промовах він описував ті самі методи й тактичні прийоми, які застосовувалися в Іраку.

Під час обох воєн АНБ відрядило в зону бойових дій понад 600 своїх співробітників, 20 з яких загинули. Тому не можна сказати, що кібервійна не несе жодного ризику для тих, хто бере у ній участь.

Кібервоїнів також висилали на менш тривалі війни.

2011 року, під час американської військової операції в Лівії, яка призвела до усунення від влади Муаммара Каддафі, АНБ співпрацювало з кібервоїнами ВМС, допомагаючи відстежувати цілі в Лівії та створювати «ударні пакети». За допомогою електронних пристроїв і радіосигналів хакери відстежували наземні цілі, а потім передавали координати ударній групі військово-повітряних сил авіаносця Enterprise. Здійснювало ці кібероперації Командування інформаційних операцій ВМС, розташоване, як і АНБ, у Форт-Міді.

Навряд чи це був перший приклад спільної роботи АНБ і ВМС. У 2010 році, під час реалізації шестимісячного проекту під керівництвом міністра оборони, Командування інформаційних операцій ВМС співпрацювало з АНБ, зокрема з підрозділом особливих операцій із джерелами інформації, який стежив за діяльністю американських телекомунікаційних компаній, у тому числі і тих, які постачали інформацію для системи Prism. Деякі деталі операції залишаються засекреченими. Зокрема, невідомо, яка саме мережа – урядова чи терорис-

тична – була об'єктом стеження. Але, за словами учасників операції, вони вели спостереження в реальному часі за близько 600 окремими об'єктами щонайменше в 14 країнах світу, а результати операції були викладені у понад 150 письмових звітах. Ця спільна діяльність ознаменувала початок еволюції методів кібервійни і шпигунства, адже збройні сили почали працювати із розвідкою заради здобуття інформації американських компаній. Раніше військові структури трималися здаля від проведення операцій у границях Сполучених Штатів. І хоча їхні цілі розташовувалися поза межами країни, засоби для ведення цієї війни нового штибу перебували саме тут. У такі моменти інтернет здавався полем бою без жодних кордонів.

Кібервоїни перемагали й такі терористичні групи, які також не визнавали жодних кордонів. У центрі ROC фільтрували вміст вебсайтів і форумів, що їх використовували для спілкування активісти «Аль-Каїди». У приватній розмові хакери з ROC якось сказали, що можуть заразити вірусом або шпигунською програмою «практично будь-кого», хто відвідає певний форум.

На бойовому рахунку кібервоїнів США – приголомшливі перемоги над залишками «Аль-Каїди» та її прихильниками. У серпні 2013 року старший рядовий авіації (еквівалент звання армійського капрала) 17-го розвідувального авіакрила ВПС США аналізував перехоплену інформацію та звернув увагу на розмову, що здалася йому підозрілою. Цей підрозділ, який звітував Кіберкомандуванню США у Форт-Міді, регулярно проникав у іноземні комунікаційні мережі, викрадаючи інформацію про озброєння, для контролю за дотриманням досягнутих угод і здобуття зашифрованої оперативно-командної інформації. Однак у тій перехопленій розмові йшлося про інше. Старшого рядового авіації, лінгвіста за освітою, стурбувала інформація про «телефонну нараду» лідерів «Аль-Каїди», які планували терористичну атаку. Він попередив старшого офіцера, а той передав інформацію вгору ланцюжком командування президентові Обамі.

Отримана інформація спонукала Державний департамент США тимчасово зачинити посольства в 22 країнах Близького Сходу. Це була найбільша терористична загроза за останній час. Розвідників, військових і всіх американських громадян, які перебували за кордоном, попередили про можливі атаки на американські посольства та інші державні установи за межами США.

Нарада керівників «Аль-Каїди» відбувалася не в телефонному режимі, а за допомогою інтернет-системи обміну зашифрованими повідомленнями. Зі статті в інтернет-виданні The Daily Beast, яке першим оприлюднило інформацію про цю нараду, а також із заяв генерала ВПС можна виснувати, що старший рядовий авіації натрапив на протоколи наради у форматі текстових документів, надіслані зв'язковим «Аль-Каїди» на кілька зашифрованих електронних адрес. Службовець розшифрував і переклав ці документи, і це дозволило Сполученим Штатам перехопити інформацію та виявити розташування зв'язкового, якого за допомогою ЦРУ вистежили й заарештували в Ємені. У зв'язкового знайшли запис іншої інтернет-наради, в якій брали участь понад 20 вищих керівників «Аль-Каїди» зі всього світу.

Життя на фронтовій лінії кібервійни змінило американських солдатів і розплющило їм очі на світ загроз, якими вони досі нехтували. У 2007 році, після повернення з Іраку, капітана Боба Стасіо запросили на урочистий обід у штаб-квартирі АНБ у Форт-Міді і посадили за один стіл із генерал-лейтенантом. Кімната була вщент заповнена чоловіками й жінками у військових строях, і Стасіо почув, як хтось із них читає витяги зі звіту, в яких вихваляли роботу Стасіо та його кібервоїнів у Іраку. Почув про те, як маленький підрозділ радіотехнічної розвідки, що складався лише з 35 осіб, посприяв захопленню 450 високопріоритетних об'єктів – приголомшливе досягнення для будь-якого військового угруповання, а що вже казати про один невеличкий підрозділ. Почув, як менш ніж за рік підрозділ зумів скоротити на 90 % кількість атак. Стасіо і його колеги отримали престижну нагороду директора АНБ – вище визнання для радіотехнічної розвідки, – хоча підрозділ Стасіо був найменшим з усіх, що отримали цю винагороду.

Коли промовець назвав ім'я Стасіо, аудиторія вибухнула оплесками, а генерал-лейтенант, що сидів поруч, усміхнувся і легенько штовхнув його ліктем. «Чудова робота», – сказав Кіт Александер, директор АНБ.

Це було лише початком їхніх нових взаємин. Александер призначив Стасіо командиром «А-команди», свого передового підрозділу. Стасіо підпорядковувався старшому офіцерові, який звітував безпосередньо Александеру, і брав участь в організаційній роботі,

що передувала створенню нового Кібернетичного командування. У 2009 році він очолив команду АНБ, що відповідає за проведення військових кібероперацій, отримавши у підпорядкування 70 солдатів і вдосталь небачене ним раніше найновіше й найдорожче обладнання. Стасіо мав подвійне навантаження, позаяк також виконував обов'язки вахтового офіцера в Центрі операцій у комп'ютерних мережах, який, як йому здавалося, вельми нагадував Центр управління польотами НАСА в Космічному центрі Джонсона. Врешті-решт Стасіо звільнився з армії, але залишився працювати в АНБ як контрактний співробітник і очолив відділ операцій у Кібернетичному центрі АНБ.

Там Стасіо працював, за його ж словами, у «режимі постійної кризи». Він дізнався, що хакери повсякчас зондують і сканують військові мережі, шукаючи способу проникнути в них, і що в інтернеті повно людей, які намагаються вкрасти інформацію, захопити управління комп'ютерами або й знищити інформаційні мережі та супутню інфраструктуру. Ця робота розплющила йому очі на світ загроз, відомих, на його думку, лише жменьці людей, яким могла протистояти ще менша кількість. Стасіо знав, яку шкоду можуть заподіяти хакери, адже він сам це робив. Інколи, почувши у випуску новин історію про потяг, що зійшов із колії, він замислювався: чи не хакер спричинив цю аварію?

Минали роки, а Стасіо продовжував очікувати катастрофічну кібератаку на Сполучені Штати. Після звільнення з АНБ він організував власну компанію із забезпечення кібербезпеки – Ronin Analytics, – де не раз вислуховував чільників корпорацій, які вихваляли свої хитромудрі методи кіберзахисту і непроникні мережі. Стасіо вислуховував їхні пихаті запевнення у чудовому захисті… у безпеці.

А сам хитав головою і думав: *«Ви не бачите того, що бачу я»*.

5
ВОРОГ СЕРЕД НАС

Інтернет перетворився на поле битви. Але ворог ховався на відстані витягнутої руки. Кіт Александер бачив загрози у кожному куточку кіберпростору. Для банків. Для енергомереж. Для мереж військових і розвідувальних організацій. Як кібервоїнам АНБ виявити всі ці загрози?

Через рік після початку роботи в АНБ Александер попередив свою команду про наближення «війни в мережі». Агентству довелося відійти від контртерористичної діяльності, розгорнутої після атак 11 вересня, і зосередитися на розшуку хакерів і боротьбі з ними, незалежно від того, працюють вони на терористичні організації, кримінальні кола або іноземні держави. Александер надіслав указівки співробітникам АНБ, задіяним у секретній програмі «Турбуленція» (Turbulence). Це була одна з перших спроб стеження за хакерами всього світу та їхніми шкідливими програмами за допомогою системи сенсорів, і в деяких випадках для нейтралізації загроз доводилося проводити кібератаки. Александер повідомив членів команди, задіяних у програмі, що «в агентстві немає нічого важливішого» за їхню роботу.

Для завершення своєї місії АНБ повинно було діяти агресивніше, інсталюючи пристрої прослуховування і стеження в комп'ютерні системи цілого світу. Американські хакери, які присягнули захищати державу від кіберзагроз, повинні були навчитися думати так само, як їхні противники, тобто стати хитрими й підступними. Їм довелося запозичити чимало тактичних прийомів, від яких вони раніше захищалися. Кібервоїни готувались увійти в сіру зону й підірвати основи інтернету заради його власної безпеки.

Кібервоїни АНБ, скануючи інтернет-горизонт у пошуках загроз, усвідомлювали, що деякі властивості кіберпростору стали перешкодою для здійснення їхньої місії. Тому вирішили цих перешкод позбутися. Передусім вони взялися за популярну систему маршрутизації Tor, яка дозволяла людям цілого світу анонімно заходити в мережу.

У самій технології Tor немає нічого кримінального, та й створили її аж ніяк не вороги Сполучених Штатів. Систему розробили в дослідній лабораторії ВМС Сполучених Штатів у 2002 році, і нині її використовують борці за демократію та політичні дисиденти різних країн, уникаючи переслідування деспотичної влади. Але водночас цю технологію застосовують хакери, шпигуни й шахраї, приховуючи місце свого розташування під час здійснення протиправних дій. Система Tor веде в найтемніші куточки інтернету, де люди анонімно купують і продають протизаконні товари й послуги, зокрема наркотики, зброю, комп'ютерні віруси, хакерські послуги та навіть послуги найманих вбивць.

Анонімність – це прокляття кібервоєнних операцій АНБ. Хакери не спроможні прицільно вистрілити, якщо не знають, де розташована мішень. Тому не дивно, що 2006 року АНБ почало робити спроби підірвати анонімні можливості технології Tor і протягом кількох років не полишало цієї діяльності.

Користувачі системи Tor, в основі якої лежить цибулева маршрутизація*, завантажують безкоштовне програмне забезпечення на власні комп'ютери. Скажімо, користувач хоче анонімно зайти на сайт. Програма автоматично скеровує його через мережу з тисяч мережевих вузлів, роботу яких підтримують головно добровольці. Трафік у межах Tor шифрується, минаючи різні мережеві шари, – звідси й з'явилася «цибулева» метафора. Щойно користувач з'єднується із сайтом, його дані шифруються стільки разів, а інформація проходить через таку кількість проміжних вузлів, що визначити місце розташування користувача практично неможливо. Систему Tor може використовувати будь-хто – наркоторговці, розповсюджувачі дитячої порнографії, хакери, терористи і шпигуни, будь-хто, кому вкрай необхідно залишатись анонімним у мережі й уникнути переслідування правоохоронних органів і розвідки.

Протягом шести днів у лютому 2012 року АНБ об'єднало зусилля зі своїми британськими колегами з Центру урядового зв'язку і вони інсталювали 11 «ретрансляторів» у мережі Tor. Ретранслятор, або ж

* Цибулева маршрутизація – технологія анонімного обміну інформацією завдяки багаторазовому шифруванню повідомлень і пересиланню їх через кілька мережевих вузлів, кожен з яких видаляє шар шифрування.

маршрутизатор чи вузол, розподіляє трафік усередині системи. Встановлені державою ретранслятори отримали назву Freedomnet.

Установка шпигунських ретрансляторів у мережі Tor здавалася кращою альтернативою прямим атакам на вузли цієї мережі з метою їхнього вимкнення, хоча, згідно з надсекретними документами АНБ, хакери пропонували й такий варіант. Проте вирішили відмовитися від безпосередніх атак, тому що не могли щоразу непомильно визначити, розташований вузол у Сполучених Штатах чи за кордоном, а використання спецобладнання для атак усередині США пов'язане з низкою правових проблем. Знищення вузлів було ризикованою авантюрою, адже в мережі Tor тисячі ретрансляторів, розташованих у найрізноманітніших місцях. Отож, АНБ спробувало ідентифікувати користувачів усередині мережі за допомогою власних вузлів ретрансляції, перенаправляючи трафік на них. Хакери АНБ також надсилали потенційним користувачам системи Tor фішинґові повідомлення – електронні листи, які виглядали так, наче надіслані з надійного джерела (наприклад, від друга або людини зі списку контактів користувача), але насправді містили вірус або посилання, перейшовши за яким, користувач потрапляв на сайт, заражений шпигунським програмним забезпеченням.

Згідно зі стислим документом під назвою Tor Stinks, хакери розглядали можливість організації збою у мережі Tor. Можливо, вони хотіли сповільнити її або «встановити велику кількість по-справжньому повільних вузлів Tor (розрекламованих як високошвидкісні) для дестабілізації роботи мережі». Вони розмірковували щодо виставлення перешкод, які заважатимуть під'єднуватися до системи Tor. АНБ хотіло стати злим гремліном, який підступно гатить по механізмові, поки не зруйнує його вщент.

Агентство також намагалось атакувати користувачів Tor із зовнішньої мережі, заражаючи або «позначаючи» їхні комп'ютери чимось штибу електронного маркера, коли вони входили в систему Tor або виходили з неї. Хакери АНБ шукали різноманітні шляхи проникнення у комп'ютери, які могли використовувати цю мережу. Якось вони виявили особливо вразливе місце в інтернет-браузері Firefox, через яке позначили комп'ютери, що використовували цей браузер. Нікому не спадало на думку, що та сама вразливість, якщо її не усунути, могла зашкодити користувачам, які й гадки не мали

про мережу Tor і не робили жодної спроби приховати сліди онлайн-активності.

Анти-Tor'івська кампанія АНБ розпочалася 2013 року, як випливає з надсекретних документів, оприлюднених Едвардом Сноуденом. Із цих таки документів зрозуміло, що заходи були переважно безуспішними. АНБ зуміло ідентифікувати й визначити місце розташування лише кількох десятків користувачів Tor. Це доказ того, що система працює добре. Натомість атаки АНБ показали, як далеко може зайти агентство у своєму бажанні за будь-яку ціну дістати перевагу над противниками. Зважаючи на те, що АНБ не завжди може визначити місце розташування комп'ютера, якщо користувач входить у мережу через Tor, агентство майже напевно заразило комп'ютери багатьох американських користувачів. За оцінками аналітиків Tor, лише у Сполучених Штатах системою користується близько 400 тисяч осіб.

Методи АНБ не відповідали заявленій американцями зовнішній політиці. Протягом кількох останніх років Держдепартамент виділив мільйони доларів на підтримку Tor, заохочуючи іноземних активістів і дисидентів, зокрема сирійських повстанців, які брали участь у виснажливій громадянській війні задля закінчення диктату Башара Аль-Асада, користуватися мережею. У АНБ знали, що Держдепартамент просуває Tor, проте агентство атакувало цю мережу. У США тепер конкурують дві протилежні політичні тенденції: підтримка мережі Tor і спроби зламати цю систему.

Колишній директор АНБ Майкл Гейден висловився про цю дилему доволі різкими словами: «Держсекретар відмиває гроші через громадські організації для популяризації програмного забезпечення в арабському світі, щоб захистити людей на вулицях арабських країн від стеження тамтешніх урядів, – заявив він 2012 року у вашинґтонському «мозковому» центрі ще до того, як усі довідалися про операції АНБ проти Tor. – Тому, з одного боку, ми боремося з анонімністю, а з другого – розкидаємося програмними продуктами, які захищають анонімність у мережі».

Натомість операції АНБ стали на перешкоді зусиллям США з поширення демократії і вільного доступу до інтернету. «В уряду Сполучених Штатів надто багато різних програм. І наші співробітники не завжди дотримуються тих самих поглядів на світ, що їх сповідує АНБ, – стверджує Ден Мередіт, директор фонду Open Technology, при-

ватної неприбуткової організації, яка щороку отримує через радіостанцію «Вільна Азія» державне фінансування уряду США на проекти боротьби з цензурою в інтернеті, зокрема й на роботу з мережею Tor. – Спробуйте-но пояснити це активістам у Судані, які навряд чи у це повірять. Інколи я витрачаю п'ятнадцять хвилин, намагаючись переконати людей, що я не [шпигун]».

Над руйнуванням засад безпеки і недоторканності приватного життя в інтернеті працює не лише АНБ. У рамцях секретної програми SIGINT Enabling Project агентство домовляється з технологічними компаніями щодо впровадження бекдорів у їхні комерційні продукти. У 2013 році Конгрес США виділив $250 млн на реалізацію цього проекту. Завдяки тісній співпраці з ФБР АНБ дізналося про одну особливість програми Microsoft Outlook для роботи з електронною поштою, яка могла б створити перешкоди для стеження, якщо не втрутитися. Агентство також отримало доступ до листування та розмов у Skype і до хмарного сховища Microsoft SkyDrive, і аналітики АНБ могли читати повідомлення користувачів іще до шифрування.

Секретні документи також свідчать, що АНБ спонукає виробників криптографічних продуктів дозволити експертам агентства аналізувати продукцію компаній під приводом боротьби за надійність алгоритмів шифрування. Проте насправді експерти АНБ інсталюють у ці продукти вразливості, щоб згодом використати їх у шпигунських або кібервоєнних операціях. В одному документі йдеться про те, що ця робота дозволяє агентству «доставляти або отримувати інформацію до/з цільового кінцевого пункту віддалено». Інакше кажучи, красти інформацію з комп'ютера або встановлювати на ньому шкідливий код.

Такі плацдарми в технологічних продуктах, що продаються і використовуються в усьому світі, дозволяють агентам АНБ шпигувати потай, а за потреби вивести з ладу технологічний продукт. Принцип дії комп'ютерного «хробака» Stuxnet, який знищив центрифуги на іранському ядерному виробництві, ґрунтується на невідомій раніше вразливості в системі управління компанії Siemens. Експерти з комп'ютерної безпеки запитували себе: можливо, виробник знав про цю вразливість і погодився залишити її? У будь-якому разі немає жодного сумніву, що АНБ володіло детальною інформацією про недоліки системи й використало її для створення «хробака» Stuxnet.

Військові навчили кібервоїнів, які працювали під керівництвом Кібернетичного командування США, зламувати деякі поширені види телекомунікаційного обладнання. Армія скеровувала солдатів на курси, на яких навчали принципів роботи й експлуатації мережевого устаткування Cisco. Не лише тому, як обслуговувати обладнання, а й тому, як його зламувати й захищати від зламування.

У рамцях програми SIGINT Enabling Project АНБ також платило телефонним і інтернет-компаніям за те, щоб, будуючи свої мережі, вони залишали лазівки для агентства або, якщо використовувати менш зрозумілу мову секретного бюджетного документа, «забезпечували безперервну співпрацю з основними постачальниками телекомунікаційних послуг для формування глобальної мережі з доступом для інших методів збирання інформації».

Уся ця секретна робота свідчить про рівень залежності АНБ від корпорацій, які розробляють програмне й апаратне забезпечення, а також володіють сегментами глобальної мережі та обслуговують їх. Без співпраці з такими компаніями агентство не змогло б вести шпигунську й кібервоєнну діяльність. Проте спроби агентства запанувати у «п'ятому вимірі» військових дій не обмежувались угодами з приватними корпораціями.

Упродовж десяти останніх років АНБ спільно з британськими колегами з Центру урядового зв'язку поклало чимало зусиль на боротьбу з криптографічними технологіями, інсталюючи приховані вразливості в поширені стандарти шифрування. Шифрування – це процедура перетворення даних (наприклад, електронного листа) в мішанину цифр і символів, яку можна розшифрувати лише за допомогою ключа, яким володіє адресат. Якось АНБ вступило у відкриту боротьбу за отримання доступу до ключів шифрування, щоб розшифровувати повідомлення за власним вибором, але програло битву. Тоді агентство взялося за послаблення алгоритмів шифрування, які використовуються насамперед для кодування онлайн-комунікацій.

АНБ – це домівка найкращих у світі криптографів, яких регулярно консультують різноманітні інституції, зокрема й державні агентства, щодо збільшення стійкості алгоритмів шифрування. У 2006 році, через рік після призначення Александера на посаду директора АНБ, агентство допомагало розробляти стандарт шифрування, який згодом затвердив Національний інститут стандартів і технологій (NIST) –

державне агентство, яке має вирішальне слово щодо прийнятності засобів вимірювання, використовуваних для калібрування розмаїтих інструментів, промислового обладнання та наукових приладів. Схвалення стандарту шифрування інститутом – це своєрідний знак якості. Він переконує компанії, групи лобістів, приватних осіб і державні структури в усьому світі, що цей стандарт можна використовувати. NIST працює абсолютно прозоро, дозволяючи експертам аналізувати стандарт і коментувати його. Це одна з причин того, що схвалення інститутом має таку вагу. Довіра до NIST така велика, що будь-який алгоритм шифрування, який використовується в комерційних продуктах, що продаються в США, повинен дістати схвалення інституту.

Проте за лаштунками цього здебільшого відкритого процесу АНБ активно розробляло такий алгоритм, як генератор випадкових чисел – основний компонент шифрування. Згідно з секретними документами, АНБ заявляло, що хотіло лише злегка «вдосконалити» деякі деталі алгоритму, проте насправді стало його «одноосібним редактором» і засекретило процес створення. Підірвавши довіру до генератора випадкових чисел, агентство поставило під сумнів надійність цілого процесу шифрування й здобуло лазівку для розшифрування інформації або отримання доступу до комп'ютерних систем.

Праця АНБ зі створення алгоритму не була таємницею. Участь агентства навіть додавала процесові певної престижності. Але не минуло й року після затвердження стандарту, як фахівці в галузі безпеки виявили в алгоритмі очевидні вразливості та висловили припущення, що ці бекдори – справа рук шпигунського агентства. Відомий експерт із комп'ютерної безпеки Брюс Шнаєр звернув увагу на один із чотирьох методів генерації випадкових чисел, схвалених NIST. Цей метод, писав він 2007 року, «не схожий на інші».

Шнаєр зауважив, що цей алгоритм працював утричі повільніше за інші. Крім того, його «вибороло АНБ, яке вперше запропонувало цей метод кілька років тому в рамках проекту зі стандартизації Американського національного інституту стандартів».

Шнаєр занепокоїло те, що NIST заохочував людей користуватися посереднім алгоритмом, запропонованим агентством, місія якого полягала в зламуванні шифрів. Проте не було жодних доказів того, що АНБ замислило щось лихе. Недосконалість генератора випадкових чисел не робила його неужитковим. Як зауважив Шнаєр, недолік можна було завиграшки виправити, однак навряд чи хтось потурбувався

про це. Але ця вразливість непокоїла криптографів. Безсумнівно, АНБ знало про невдоволення фахівців, а також про збільшення кількості доказів таємного втручання агентства, однак покладалося на офіційне схвалення нового алгоритму міжнародною організацією зі стандартизації, до якої прислуховуються 163 країни. АНБ хотіло впровадити алгоритм у цілому світі у таких масштабах, щоб людям було важко відмовитися від його використання.

Та передусім Шнаєра спантеличило те, що АНБ використало як бекдор таку очевидну й усім відому вразливість. (Рік тому цю вразливість виявили фахівці компанії Microsoft.) Почасти відповідь полягала у тому, що АНБ уклало угоду з компанією RSA, одним із провідних підприємств світу в галузі комп'ютерної безпеки й піонером у цій індустрії. Згідно зі звітом агентства Reuters, оприлюдненим 2013 року, компанія почала застосовувати створений алгоритм АНБ «іще до його схвалення в NIST. Згодом АНБ посилалося на раннє впровадження алгоритму… в урядових організаціях, наводячи цей факт як арґумент для схвалення його в NIST». Алгоритм став «опцією за замовчуванням для генерації випадкових чисел» у програмному продукті bSafe компанії RSA, як відомо зі звіту Reuters. «Нікого це не збентежило, як визнали колишні працівники, позаяк угоду укладали управлінці, а не технарі». Згідно зі звітом Reuters, за згоду й готовність упровадити алгоритм зі вразливістю у технологічний продукт компанії RSA заплатила $10 млн.

АНБ створило для себе очевидну лазівку, але це не мало жодного значення. Алгоритм продавала одна з провідних світових компаній у галузі безпеки, а схвалила його не лише NIST, а й міжнародна організація зі стандартизації. Кампанія АНБ з ослаблення глобальної безпеки заради власних цілей виявилася ефективною.

Про діяльність АНБ заговорили 2013 року, після оприлюднення Едвардом Сноуденом деяких документів, і RSA та NIST відмежувалися від шпигунського агентства, хоча й не спростували інформації про інсталяцію бекдорів.

У заяві, зробленій після оприлюднення звіту Reuters, компанія RSA заперечувала таємну змову з АНБ, наполягаючи, що ніколи не мала «будь-яких домовленостей або спільних проектів із наміром ослаблення продуктів RSA або впровадження потенційних бекдорів у продукти масового вжитку». Але компанія не заперечувала, що бекдор існував або міг існувати. RSA визнала, що кілька років тому, коли

ухвалювали рішення щодо використання вразливого генератора випадкових чисел, «АНБ користувалося довірою суспільства й докладало зусиль задля підвищення безпеки шифрування, а не його ослаблення». Тепер усе змінилося. Оприлюднені Сноуденом документи доводили втручання АНБ, і компанія RSA закликала відмовитися від використання цього генератора випадкових чисел. Так само вчинив і NIST.

Після викривальних заяв Сноудена Комітет зі стандартизації оприлюднив власну заяву, ретельно добираючи слова. «NIST не ослабляв би криптографічні стандарти навмисне, – йшлося у цій заяві організації, яка не відкидала закидів, але й не заперечувала того, що АНБ таємно інсталювало вразливість або зробило це проти волі NIST. – NIST має тривалу історію тісної співпраці з експертами з криптографії світового рівня заради підтримки надійних стандартів шифрування. [АНБ] брало участь у криптографічних розробках інституту, позаяк в агентстві працюють визнані експерти в цій галузі. Статут інституту передбачає консультування з АНБ».

Інститут стандартизації чітко заявив світові, що не міг перешкодити АНБ. Навіть якщо б установа хотіла усунути АНБ від розробки стандартів, згідно із законом цього вчинити не могла. Один із керівників АНБ навів саме цей арґумент. У грудні 2013 року Енн Нойберґер, яка відповідала за співпрацю АНБ з технологічними компаніями, під час інтерв'ю блогові Lawfar, присвяченому питанням безпеки, прямо запитали, чи агентство втручалося в розробку алгоритму. Вона не підтвердила, але й не спростувала ці звинувачення. Нойберґер назвала NIST «надзвичайно шанованим, близьким партнером у багатьох питаннях». Але зауважила, що інститут «не є членом розвідувального співтовариства».

«Усе, що вони роблять… чистий білий аркуш, – продовжувала Нойберґер, маючи на увазі відсутність зловмисних намірів і прагнення передусім захистити шифрування та сприяти його безпеці. – Вони відповідають лише за стандарти й за те, щоб зміцнити їх так, як це тільки можливо».

І АНБ начебто зовсім не причетне. Здається, Нойберґер видала NIST перепустку на волю, звільняючи інститут від будь-якої відповідальності за впровадження вразливості.

Спроби послабити безпеку генератора випадкових чисел у 2006 році не були одиничним випадком. Це частина масштабної три-

валої кампанії АНБ з ослаблення безпеки основних стандартів захисту інформації, якими користуються приватні особи й організації цілого світу. Документи свідчать, що АНБ почало співпрацювати з NIST іще на початку 1990-х, намагаючись послабити стандарти шифрування ще до їхнього прийняття. АНБ контролювало процес розробки стандарту цифрового підпису (DSS) – методу верифікації відправника електронного повідомлення та достовірності інформації у ньому. «NIST відкрито запропонував [стандарт] у серпні 1991 року і спочатку не згадував про будь-яку участь АНБ у розробці цього стандарту, призначеного для використання в несекретних цивільних системах комунікації», – йдеться у доповіді Інформаційного центру захисту електронних персональних даних, який отримав документи щодо процесу розробки стандарту, посилаючись на закон про свободу інформації. Потому, як група експертів із комп'ютерної безпеки подала судовий позов, NIST визнав, що АНБ розробило стандарт, який «масово розкритикували представники комп'ютерної індустрії за ненадійність і посередній рівень, якщо порівнювати з наявними технологіями перевірки достовірності. <…> Багато спостерігачів припускали, що АНБ не підтримало [наявної] технології, тому що насправді вона була безпечнішою за алгоритм, запропонований агентством».

З погляду АНБ жодного підступу в його спробах контролювати процес шифрування немає. Зрештою, агентство займається зламуванням закодованої інформації. Це завдання, яке йому доручили і виконання якого очікують. Якщо агентство зробило лазівки в алгоритмах шифрування, про які знало лише воно, кому це зашкодить?

Проте ці лазівки не були секретом. До 2007 року про бекдори в генераторі випадкових чисел писали популярні сайти й провідні експерти з кібербезпеки. Використати цю вразливість, тобто підібрати ключ, який відкривав би «чорний хід», залишений АНБ, було складно, але можливо. Іноземні служби могли знайти спосіб зламати алгоритм шифрування, щоб потому шпигувати за власними громадянами або за американськими компаніями й агентствами, які використовували цей алгоритм. Злодії мали змогу використовувати вразливості алгоритму для крадіжки персональної й фінансової інформації. Алгоритм був уразливий скрізь, де його застосовували, зокрема і в продуктах однієї з провідних світових компаній у сфері безпеки.

Фахівці АНБ могли заспокоювати себе, припускаючи, що криптографічні служби інших країн, безсумнівно, спробують обійти шиф-

рування, зламуючи й ті алгоритми, якими маніпулювало АНБ. Звісно, так воно й було. Проте це не відповідь на запитання: навіщо свідомо дискредитувати не лише один алгоритм, а й процес створення стандартів шифрування загалом? Секретне втручання АНБ підірвало довіру до NIST і зруйнувало давню репутацію агентства як надійного й цінного партнера у створенні деяких засадничих технологій в Інтернеті та пристроїв, в яких люди зберігали власну інформацію, захищаючи недоторканність особистого життя. Лише уявіть, що АНБ займалося б виробництвом дверних замків і заохочувало всі будівельні компанії країни віддавати перевагу моделям, в яких є прихований недолік. Ніхто би цього не терпів. Споживачі завалили б компанію судовими позовами та вимагали б відставки керівників організації.

Проте реакція на антишифрувальну кампанію АНБ була порівняно кволою. Почасти тому, що багато експертів, серед яких були й криптографи, віддавна були переконані в причетності агентства до подібної тіньової діяльності. Нове викриття було скандальним, але особливого подиву не викликало. Натомість американські законодавці та можновладці мали стійке переконання, що саме цим і повинно опікуватися АНБ. Агентство зламує шифри, щоб викрадати інформацію. NIST затверджує нові стандарти за допомогою відкритої та прозорої процедури. А це прокляття для секретної діяльності АНБ.

З погляду агентства Комітет зі стандартизації створює загрозу поширення стійких до зламування алгоритмів і криптографічних технологій, які надійно захищають інформацію, тобто робить усе, що перешкоджає АНБ виконувати свою роботу. Упродовж багатьох років законотворці, які затверджували бюджет АНБ, а також представники адміністрації президента, які наглядали за його роботою, були на стороні агентства. Не бажаючи непорозумінь, вони цілком покладалися на той факт, що спритна діяльність АНБ залишається в секреті, отже, збиток безпеці інтернету і репутації Сполучених Штатів був мінімальним. Викриття 2013 року поклали край цим сподіванням.

Зі всіх темних справ АНБ, напевно, жодна інша не загрожувала безпеці інтернету й користувачів так, як секретні розробки кіберзброї.

Протягом останніх 20 років аналітики АНБ вивчали світове програмне й апаратне забезпечення та мережеве обладнання, намагаючись знайти помилки й уразливості, які допоможуть розробити

методи атак на комп'ютерні системи, так звані експлойти* нульового дня, названі так, бо йдеться про невідомі раніше вразливості, захисту від яких наразі не існує. (Ціль має «нуль днів», щоб підготуватися до атаки.)

Уразливість нульового дня – найефективніша кіберзброя з ефектом несподіванки, що дає величезну перевагу в битві. Експлойт нульового дня розробляють з огляду на конкретну вразливість. А позаяк недолік системи, найімовірніше, «залатають», щойно об'єкт зрозуміє, що його атакували, скористатися вразливістю можна лише один раз.

Атаки нульового дня розробляти доволі складно, оскільки невідомі вразливості знайти непросто. Однак АНБ упродовж багатьох років накопичувало інформацію про них. У 1997 році, згідно з нещодавно розсекреченим інформаційним бюлетенем АНБ, принаймні 18 підрозділів агентства таємно збирали дані щодо вразливості технологій, використовуваних приватними особами, компаніями та державними установами всього світу. Нині експерти з безпеки та державні діячі одноголосно визнають, що АНБ – єдиний і найбільший власник експлойтів нульового дня, більшість яких агентство скупило на тіньовому інтернет-ринку в незалежних хакерів і корпоративних посередників.

Цей ринок не зовсім легальний, але якось функціонує на околицях інтернету. Діє він так: фахівці з питань безпеки (інша назва хакерів) виявляють уразливості. (Чимало цих фахівців базується в Європі, де місцеві та державні закони, скеровані на протидію хакерству, значно лагідніші, ніж у Сполучених Штатах.) Потім фахівці розробляють експлойти, тобто способи атаки через виявлену вразливість, про яку знають лише ті, хто її виявив. Експлойти продають посередникам, якими зазвичай є великі оборонні підприємства. Два найбільших гравці на цьому ринку – компанії Raytheon і Harris Corporation – розробляють традиційні системи озброєння і є найбільшими й найавторитетнішими підрядниками Пентаґону. Ці підприємства мають давні й тісні зв'язки з військовими та АНБ. Збором і продажем уразливостей нульового дня також займаються невеликі спеціалізовані фірми. Деякі з них очолюють колишні армійські офіцери або розвідники.

---

* Експлойт – програма, фрагмент програмного коду або послідовність команд для здійснення атаки на комп'ютерну систему завдяки вразливостям програмного забезпечення.

Після отримання інформації про виявлені вразливості нульового дня, посередники пропонують її своєму клієнтові – АНБ. Проте ланцюжок постачання починається з хакера. Щоб стати хорошим мисливцем на вразливості нульового дня, хакер повинен влізти в шкуру програміста-розробника й знайти недоліки в його коді. Автоматизація спрощує цей процес. Наприклад, техніка фазинґу полягає в тому, що на вхід програми подаються невідповідні або випадкові згенеровані дані, що можуть викликати креш (фатальний збій) системи. Потім хакер аналізує недоліки, які спричинили це падіння програми.

Проте, аби відшукати найприхованіші недоліки, хакер повинен придумувати нові, майстерніші методики, щоб змусити комп'ютер показати слабкі місця. Наприклад, 2005 року аспірант Каліфорнійського університету в Лос-Анджелесі виявив, що вимірювання «невеличких, мікроскопічних коливань» у внутрішньому годиннику комп'ютера (генераторі тактових імпульсів) допомагає безпомильно ідентифікувати кожен комп'ютер у мережі з тисяч машин. Згодом він написав у науковій статті, що ця методика корисна зловмисникам, «розташованим за тисячі кілометрів» од атакованого комп'ютера, які хочуть обійти такі програмні засоби приховування фізичного розташування комп'ютера, як Tor, тобто маршрутизатори-анонімайзери, які АНБ так затято намагалося знищити. Через рік після публікації статті дослідник із Кембриджського університету виявив, що існує реальна можливість ідентифікації сервера із запущеним програмним забезпеченням для збереження анонімності в мережі Tor, отже, і цю мережу можна позбавити найважливішої переваги. Він зумів це зробити, надсилаючи на анонімний сервер мережі Tor численні запити, які збільшували навантаження на сервер, у буквальному сенсі перегріваючи його. Підвищення температури призводить до зміни інтенсивності руху електронів у мікросхемах, а це впливає на точність генератора тактових імпульсів. Хоча дослідник не зміг визначити розташування анонімного сервера, він викликав унікальний «фазовий зсув імпульсів», що дозволило «опитати» комп'ютери в глобальному інтернеті, щоб знайти потрібний сервер. Так він і вчинив. Фазовий зсув дав йому змогу визначити місце розташування прихованого сервера мережі Tor. У секретному документі АНБ під назвою Tor Stinks ідеться про те, як «АНБ намагалося знищити мережу, вивчаючи обидві методики фазового зсуву задля пошуку маршрутизаторів мережі».

Геніальна майстерність у розшуку таких прихованих, заледве помітних недоліків – це те, що відрізняє геніальних хакерів від просто здібних і допомагає першим знаходити вразливості нульового дня. Експлойти нульового дня коштують чимало. Якщо вони поставляються у формі «зброї», тобто готовими до вживання проти будь-якої системи, їхня ціна починається від $50 тисяч і може досягати $100 тисяч, як твердять експерти. Деякі експлойти коштують навіть дорожче, якщо за їхньою допомогою можна атакувати цінніші або важкодоступні об'єкти. Середня вартість експлойтів для атаки операційних систем Apple iOS, інстальованих у смартфонах iPhone та інших мобільних пристроях цієї компанії, за словами одного з експертів, – близько півмільйона доларів. А складніші експлойти, наприклад ті, що цілять у вразливі місця внутрішньої механіки елементів обладнання, можуть коштувати навіть мільйони доларів. Ці експлойти такі дорогі, бо атакують апаратну систему обладнання, недоліки якої не можна усунути так, як усувають помилки в програмному забезпеченні, – за допомогою кількох нових рядків коду. Засоби та мотив купувати подібну зброю є лише в злочинних угруповань і державних органів.

Серйозні покупці інформації про вразливості нульового дня, як-от АНБ, не обмежуються разовими купівлями за потреби. Вони створюють резерви для майбутніх атак.

За словами колишнього високопосадовця, який отримав цю інформацію під час секретної наради з керівниками АНБ, тільки для потенційного вживання проти китайських електронних систем агентство накопичило інформацію про понад дві тисячі вразливостей нульового дня. Це приголомшливо величезна кількість експлойтів. Комп'ютерний «хробак» Stuxnet, створений спільними зусиллями США й Ізраїлю для боротьби з іранською програмою ядерного озброєння, містив чотири експлойти нульового дня, а це зовсім небагато для однієї атаки. Колекція з 2 тисяч експлойтів нульового дня – це кібернетичний аналог ядерного арсеналу.

Цей арсенал піддає загрозі людей цілого світу. Якщо АНБ накопичує інформацію про вразливості, замість того щоб повідомляти виробників високотехнологічної продукції про вади в їхньому апаратному та програмному забезпеченні, то, ймовірно, агентство приховує цінну інформацію, яку можна використати для захисту від зловмисних хакерів. Звісно, АНБ використовує накопичені знання щодо експлойтів нульового дня, щоб залатати дірки у технічних засо-

бах, які воно застосовує або може застосувати для військової чи розвідувальної діяльності. Але агентство не попереджає про них решту світу, адже тоді експлойти нульового дня втратять свою ефективність. Якщо АНБ повідомить технологічні компанії про вразливості їхніх продуктів, відповідні агентства в Китаї або Ірані зможуть підготуватися до відбиття атак.

Але на тіньовому ринку вразливостей нульового дня ніхто не дає гарантій ексклюзивного доступу до інформації. Один сумнівний продавець, французька компанія Vupen, продає інформацію про ті самі вразливості та експлойти багатьом клієнтам, серед яких державні органи різних країн. АНБ також є клієнтом компанії Vupen – загальнодоступні документи свідчать, що агентство купує інформацію про вразливості нульового дня за підпискою, яка передбачає здобуття інформації про певну кількість вразливостей згідно з договором. (Озброєне цією інформацією, АНБ може створювати власні експлойти.) Компанія Vupen також має каталог складних, готових до реалізації атак нульового дня, які коштують значно дорожче за інформацію, надану підписникам.

АНБ знає, що Vupen не завжди укладає ексклюзивні угоди, тому агентству доводиться купувати щораз більше інформації про вразливості нульового дня, усвідомлюючи, що принаймні якийсь відсоток із них стане непридатним для атак, якщо інша держава, приватна компанія або кримінальне угруповання скористаються ними.

Критики звинувачують компанію Vupen у «гонці кіберозброєння» –підбурюванні державних розвідслужб і збройних сил різних країн одне проти одного. Клієнти компанії знають: якщо знехтують можливістю придбати нову інформацію про вразливість, компанія обов'язково знайде іншого покупця. Вразливості, інформацією про які володіє Vupen, не унікальні для якоїсь однієї країни. Чимало з них виявлені у популярних технологічних продуктах, використовуваних у всьому світі. Отже, держави мають стимул купувати якнайбільше інформації про вразливості нульового дня і для самозахисту, і для атак на своїх противників.

Представники компанії Vupen стверджують, що лише продають інформацію «надійним організаціям», під якими мають на увазі «підприємства зі сфери безпеки, що займаються захистом», державні організації у «схвалених країнах» і «всесвітні корпорації», серед яких компанії з першої тисячі рейтингу журналу Fortune. Це довгий пере-

лік потенційних клієнтів, і компанія визнає, що не в змозі засвідчити надійність кожного з них і гарантувати, що клієнти, які купують за підпискою або каталогом, не передадуть інформацію людям, яким компанія ніколи не продасть її безпосередньо. Керівники непереконливо пояснюють, що існує внутрішня процедура перевірки клієнта, щоб незалежні хакери та посередники не отримали небезпечні продукти й інформацію, продану державним структурам. Особливе занепокоєння викликають країни Північної Африки і Близького Сходу з репресивним режимом правління, влада яких, намагаючись здолати опір борців за демократію, залучає хакерів для впровадження шкідливого ПЗ в комп'ютери протестувальників. Ці шкідливі програми купують у таких компаній, як Vupen, представники яких стверджують, що ніколи не продають власних продуктів для таких негідних цілей. Однак ці продукти повсякчас виявляють на комп'ютерах і в мобільних телефонах активістів, деякі з яких зазнали переслідувань або насильства від влади та інших переслідувачів.

На ринку – чорному, сірому чи будь-якому іншому – найбільші покупці мають змогу диктувати власні умови й правила. Як загальновизнаний найбільший покупець вразливостей і експлойтів нульового дня, АНБ може збурити ринок, якщо почне купувати інформацію й оприлюднювати її. Бюджет агентства на підтримку кібербезпеки становить мільярди доларів. Чом би не витратити частину цих коштів на попередження світу про існування вразливостей, які можна усунути? Яка відповідальність чекає агентство, якщо воно не попередить власників і операторів небезпечної технології щодо існування загрози атак? Це етична дилема, яку АНБ не мусить вирішувати. Проте, якщо колись станеться кібератака на США і призведе до значних матеріальних збитків або масової паніки, а можливо, навіть смертей, агентство буде змушене відповідати за те, що не запобігло катастрофі. Цілком імовірно, що колись у майбутньому директор АНБ сяде на місце свідка і під прицілом телевізійних камер пояснюватиме членам Конгресу і громадянам США, чому, знаючи про вразливість, якою скористалися вороги Америки, тримав її в таємниці лише тому, що АНБ просто чекало нагоди використати її для власних цілей.

Найуразливіші для нищівних кібератак нульового дня – саме ті об'єкти, які так прагне захистити АНБ: електростанції, підприємства атомної промисловості, газові трубопроводи та інші критично важливі

об'єкти інфраструктури, а також банки й фінансові компанії. Не всі ці компанії мають системи обміну інформацією про відомі вразливості та експлойти, знайдені й оприлюднені здебільшого «білими» хакерами, які бачать своє покликання у попередженні компаній-виробників щодо недоліків у їхніх продуктах і не шукають особистого зиску. Коли компанія виявляє загрозу, «латання дір» і оновлення системи стає додатковим навантаженням, натомість технологічна гнучкість різних компаній різна. Одні готові до оперативного виправлення недоліків, інші можуть навіть не усвідомлювати, що використовують уразливе програмне забезпечення. Інколи компанії просто не отримують від виробників сповіщень щодо необхідності оновлення або зміни параметрів безпеки продукту для її посилення. Навіть якщо компанія використовує програмне забезпечення, для якого випускаються регулярні оновлення, системні адміністратори компанії повинні погодити операцію, переконатися, що оновлення проведене в усіх системах компанії, і продовжувати відстежувати майбутні оновлення. Багатьом адміністраторам здається, що оновлення сотні або тисячі комп'ютерів на підприємстві – вельми важке завдання.

Купуючи так багато експлойтів нульового дня, АНБ підтримує ринок кіберзброї, загрозливий для американських компаній і критично важливих об'єктів інфраструктури. Якщо якась держава або терористична група захочуть вимкнути струм в одному з американських міст, найімовірніше, вони скористаються експлойтом, придбаним в однієї з компаній, яка продає експлойти АНБ. Продавці експлойтів нульового дня принаймні номінально винні у зменшення безпеки інтернету. Проте вони покладають провину на виробників програмного забезпечення, яке можна зламати. «Ми не продаємо зброю, ми продаємо інформацію, – відповів засновник компанії ReVuln, що продає експлойти, коли журналіст Reuters запитав його, чи хвилюватиме компанію, якщо одну з її програм використають для атаки, яка призведе до знищення систем або смерті людей. – Це запитання краще поставити виробникам, що залишають діри в своїх продуктах».

Така стратегія захисту нагадує звинувачення виробника замків у пограбуванні будинку. Так, слюсар створює продукт, який запобігає проникненню в будинок. Проте, якщо грабіжник таки потрапить усередину й украде телевізор, ба навіть гірше – атакує власників будинку, ми не висунемо звинувачень слюсареві. Звісно, такі компанії, як ReVuln, нікого не грабують, але продають аналоги відмичок.

Напевно, вони теж несуть певну міру відповідальності за доконані злочини – якщо не правову, то бодай моральну.

А як щодо АНБ? У кримінальному світі діяльність агентства не має аналогів. Адже ніхто не тиняється там, щоб купити відмичку про всяк випадок. АНБ претендує на роль охоронця інтернету. А що зазвичай відбувається, якщо охоронець, найнятий для патрулювання околиць, бачить відчинене навстіж вікно, але не повідомляє про це власників будинку? Ба більше, а якщо він сам виявляє недолік у конструкції вікон усіх помешкань у дільниці, який дозволяє злодієві відчинити вікно зовні? Якщо охоронець не попередить домовласників, його просто звільнять, а можливо, вимагатимуть його арешту. Мешканці не повірять, що він приховав інформацію про ваду в конструкції вікон, захищаючи домовласників. Вірогідно, поліція також не йнятиме віри охоронцеві, який приховав інформацію, якою міг скористатися для грабування будинків.

Аналогія не ідеальна. АНБ – не правоохоронний орган, це насамперед військова й розвідувальна організація. Діяльність агентства регламентована іншими законами та спрямована на вирішення інших завдань. Але позаяк агентство невпинно торохтить про кібервійну й позиціонує себе як найкраще озброєну організацію, покликану захищати державу від зловмисників та їхніх атак, то повинно й поводитися радше як охоронець, а не як грабіжник.

У 2013 році бюджет АНБ на придбання експлойтів нульового дня становив $25 млн, що було прописано у внутрішньому бюджетному документі агентства як «таємне придбання інформації про програмні вразливості». Проте АНБ, купуючи кіберзброю, не залежить лише від тіньового, нерегульованого ринку. Агентство здебільшого створює власну зброю. А чом би й ні? Агентство має власну виробничу базу, на якій працюють найкращі хакери країни, більшість яких зробила кар'єру в армії і навчалася державним коштом на університетських курсах із комп'ютерної безпеки. Такий персонал – це коштовна й довготривала інвестиція. Сполучені Штати покладаються на вміння та знання цих фахівців, коли йдеться про кіберзмагання з Китаєм, який, як здається, завжди матиме вагому перевагу за кількістю хакерів.

Проблема АНБ у тому, що кібервоїни високого польоту не завжди залишаються на державній службі. Завдяки переходу в приватний бізнес вони можуть завиграшки потроїти прибутки, бо за-

раз на їхню роботу в приватному секторі такий самий попит, як і у державному.

Чарлі Міллер, колишній співробітник АНБ, відомий своїм умінням відшукувати найважкіші для виявлення помилки в продуктах компанії Apple, зокрема в ноутбуках MacBook Air і смартфонах iPhone, 2012 року пішов працювати у Twitter. Таких, як Міллер, у колах хакерів називають «білими капелюхами». Він зламує системи, щоб виправити помилки, перш ніж «чорні капелюхи» зможуть скористатися недоліками системи й заподіяти шкоду. Що популярнішою ставала соціальна мережа Twitter, то привабливішою була для шпигунів і злочинців. Міллер використовує досвід, набутий в АНБ, і свій уроджений хист, захищаючи Twitter і сотні мільйонів користувачів компанії, яка 2013 року стала відкритим акціонерним товариством.

Джастін Шух пішов аналогічним шляхом. Він почав свою кар'єру в середині 1990-х як інформаційний аналітик, програміст і системний адміністратор у Корпусі морської піхоти США. У 2001 році Шух почав працювати в АНБ, де навчався в рамцях Міждисциплінарної програми вивчення систем і мереж (SNIP), метою якої є підготовка кібервоїнів. «Випускники цієї програми стають [для агентства] безцінними працівниками, здатними вирішувати всі проблеми [управління комп'ютерними мережами]», – написано в брошурі АНБ, яке вдається до технічних термінів, коли йдеться про кібератаки. Менш ніж два роки потому Шух перейшов до відділу технічних операцій ЦРУ, який допомагав АНБ інсталювати обладнання для стеження у важкодоступних місцях. Проте він також пішов у приватний сектор і незабаром вигулькнув у компанії Google на посаді фахівця з інформаційної безпеки.

Компанія Google створила команду (частиною якої став і Шух), покликану знаходити вразливості у системі безпеки й експлойти нульового дня, що загрожували клієнтам компанії та її продуктам, наприклад системі електронної пошти та браузерові. Компанія неодноразово опинялася під прицілом спритних хакерських кампаній, найпомітнішу з яких 2010 року провела китайська група, що зламала сховище програмних кодів. Хакери вкрали текст програми для системи управління паролями, яка дозволяла користувачам одночасно заходити в різні додатки Google. Аналітики називали цю програму «коштовним каменем у короні» інтелектуальної власності компанії. Крадіжка викликала паніку серед вищого керівництва Google –

компанії, яка пишається власною системою безпеки користувачів та їхніх персональних даних і яка вибудувала собі репутацію, гарантуючи цю безпеку.

Зараз у Google є власна команда нишпорок (деякі з яких працювали в АНБ та інших розвідувальних організаціях), яка відстежує потенційні загрози. «Жодного секрету немає. Володіння величезним каталогом підозрілого або доведено шкідливого ПЗ справді допомагає захистити сотні мільйонів користувачів», – написав Шух у своєму твіттері 2012 року, після купівлі Google невеличкої компанії, яка розробляла антивіруси для перевірки електронної пошти та сайтів. Нині Google сканує пошту користувачів Gmail, вишукуючи загрози, і навіть попереджає їх повідомленням на червоному тлі, якщо система підозрює у листі вірус, імовірно надісланий хакерами, що працюють на державу. У попередженні не йдеться про Китай, але це очевидне припущення.

Навіть компанії Google бракує працівників, щоб знайти всі вразливості та експлойти нульового дня, які можуть загрожувати компанії і сотням мільйонів її користувачів. Тому компанія платить премії незалежним хакерам – тим самим, які продають свої відкриття оборонним підрядникам. Співробітники Google кажуть, що їхній найбільший конкурент на тіньовому ринку вразливостей нульового дня – це АНБ. Агентство купує інформацію про вразливості швидше за всіх інших і платить найвищу ціну.

Компанія також співпрацює з мережею власних посередників, які постачають її інформацією про вразливості нульового дня. Згідно з даними двох джерел, знайомих із програмами контролю безпеки Google, компанія купує інформацію про вразливості систем і експлойти у спеціалізованої фірми Endgame, розташованої в передмісті Вашинґтона. Невідомо, що саме Google робитиме зі своїми набутками, але можна сказати абсолютно напевно: по-перше, колекція експлойтів нульового дня дозволяє компанії вести власну кібервійну, по-друге, це незаконно. Лише уряд Сполучених Штатів може проводити наступальні кібероперації, що заподіюють шкоду комп'ютерним системам.

Проте хакери цілять не лише в державні структури, і в США це чудово відомо. І справді, до створення кіберармії уряд підштовхнула масштабна шпигунська кампанія, скерована проти оборонних підприємств. Натомість приватні американські підприємства почина-

ють розуміти, що ця армія ніколи не буде достатньо численною та сильною, щоб захистити всіх. Тому бізнес вимушений захищатися самостійно.

І одне з тих місць, де компанії шукають захисту передусім, – та сама тіньова мережа хакерів, які продають свої вміння та зброю клієнтам, що пропонують найбільше.

6
НАЙМАНЦІ

Веселі 20–30-літні молодики в сорочках поло і джинсах невимушено сидять у червоних кріслах Herman Miller перед сріблястими ноутбуками Apple і глянсовими пласкими моніторами. Хтось жує обід, який привозять щотижня, або перекуски з офісної кухні, інші домовляються заграти увечері в софтбол. Їхній офіс – розкішний індустріальний лофт із відкритим плануванням, високими стелями і виведеними назовні комунікаціями. За всіма зовнішніми ознаками Endgame Inc. нагадує типовий технологічний стартап.

Однак це зовсім не так. Endgame – один із провідних гравців на глобальному ринку кіберзброї. Серед іншого, компанія збирає інформацію про вразливості нульового дня та продає її урядам і корпораціям, і, якщо зважити на ціни, що виставляє компанія, справи йдуть непогано. Маркетингові документи свідчать про те, що Endgame просить $2,5 млн за річну підписку, в яку входить пакет із 25 нових експлойтів нульового дня. За $1,5 млн клієнти отримують доступ до бази даних, в якій зберігається інформація про фізичне місце розташування та інтернет-адреси сотень мільйонів уразливих комп'ютерів у цілому світі. Озброєний цією інформацією, клієнт компанії Endgame може знайти у власних системах вразливі для атаки місця й вибудувати захист від атак. У базі даних він також знайде відомості про комп'ютери, уразливі для експлойтів. Зокрема, комп'ютери, які містять важливу інформацію, наприклад урядові документи або корпоративні комерційні секрети. Компанія Endgame може обирати, з ким мати справи, але не диктує клієнтам, як саме використовувати придбану інформацію, і може перешкодити протизаконним діям клієнтів не більше, ніж виробник зброї Smith&Wesson може запобігти скоєнню злочину з боку своїх покупців.

Основу бізнесу компанії Endgame становить обробка величезного обсягу інформації про незахищені комп'ютери, вразливість мереж і подання її у графічному вигляді. Для цього Endgame використовує

власне програмне забезпечення, яке в компанії називають «Хірургічною пилою» (Bonesaw) і описують як «додаток для визначення кіберцілей».

«“Хірургічна пила” – це інструмент для створення схеми практично всіх пристроїв, під’єднаних до інтернету, із зазначенням їхнього програмного й апаратного забезпечення», – розповів журналістам співробітник Endgame у 2013 році. Програма показує системи, які внаслідок зараження вірусами стають уразливими для атак.

За словами аналітиків у сфері безпеки і колишніх держпосадовців, одним із найбільших клієнтів компанії Endgame є АНБ. Відомо, що компанія також співпрацює з ЦРУ, Кіберкомандуванням США, британськими розвідувальними службами і великими американськими корпораціями. Компанія Endgame має чотири офіси, один з яких розташований у престижному районі Кларендон у місті Арлінґтоні (штат Вірджинія) і до якого з Пентаґону можна дістатися за десять хвилин автомобілем або проїхавши на метро чотири зупинки.

Компанія Endgame пропонує клієнтам перелік комп’ютерів, якими користуються деякі з найбільших стратегічних противників США. У 2010 року компанія склала список із 18 державних структур і великих державних компаній Венесуели, комп’ютери яких вразливі для атак. У цьому переліку виявилися водопровідна станція, банк, Міністерство оборони, Міністерство закордонних справ і адміністрація президента. У таблиці, яка, за словами представників компанії, становить «не повний перелік», були зазначені інтернет-адреси кожної зараженої комп’ютерної системи, перелічені міста, в яких розташовані ці системи, і названі запущені у них небезпечні додатки. В останній колонці таблиці, позначеній як EGS Vuln, було зазначено, чи вразливі ці додатки для атак. Практично напроти кожного з перерахованих в цій колонці комп’ютерів стояло слово «так».

Компанія Endgame також розшукувала цілі в Росії. Внутрішня документація показує, що відкриті для атаки комп’ютери є в Міністерстві фінансів, на нафтопереробному заводі, в банку і на атомній електростанції. Компанія також виявила низку вразливих для атак об’єктів у Китаї, країнах Латинської Америки і Близького Сходу.

Раніше складання таких переліків підпадало під компетенцію державних розвідслужб. Лише вони мали доступ до подібної інформації і навички для розшуку вразливих комп’ютерів із такою точніс-

тю. І лише вони мали мотивацію і засоби для придбання кіберзброї, призначеної для атак на ці системи. Нині це змінилося.

Компанія Endgame належить до небагатьох вузькопрофільних компаній-найманців, які спеціалізуються в так званому активному захисті, але кількість подібних фірм стрімко зростає. Активний захист – це евфемізм, що ним послуговуються фахівці з інформаційної безпеки, щоб збити з пантелику інших, позаяк під «захистом» мають на увазі не лише блокування мереж і встановлення антивірусів. Це поняття охоплює превентивні удари і відповідь на атаки. Сама компанія Endgame атак не здійснює, проте її клієнти, озброєні придбаною інформацією, можуть завдавати кібердари самостійно. Загалом законодавство забороняє приватним компаніям проводити кібератаки, дозволені державним агентствам. За даними трьох інформаторів, знайомих із бізнесом Endgame, переважна більшість клієнтів компанії – це американські державні структури. Однак з 2013 року компанія почала співпрацювати з провідними технологічними компаніями і банками й досягла справжнього комерційного успіху.

Компанію Endgame заснував 2008 року Кріс Роуланд, першокласний хакер, який уперше потрапив на радари Міністерства оборони ще 1990 року – після проникнення у комп'ютерну систему Пентаґону. Відомо, що влада Сполучених Штатів відмовилася від його переслідування в обмін на згоду попрацювати на державу. Роуланд заснував Endgame, узявши до спілки знайомих хакерів із репутацією «білих капелюхів», що працювали аналітиками в компанії Internet Security Systems, яку 2006 року за $1,3 млрд придбала IBM. Формально компанія повинна захищати комп'ютери й мережі клієнтів. Проте навички та досвід хакерів дозволяють компанії не лише захищати, а й атакувати.

Деспотичний і запальний (за словами колишніх колег) Роуланд став активним прибічником того, щоб дозволити компаніям здійснювати контратаки проти окремих людей, груп і навіть цілих країн, які наважились атакувати першими. «Врешті-решт, нам необхідно дозволити корпораціям цієї країни завдавати удари у відповідь, – сказав Роуланд під час круглого столу в рамках конференції з етики і зовнішньої політики в Нью-Йорку у вересні 2013 року. – Вони втрачають мільйони доларів, і позаяк держава не може їм допомогти, гадаю, потрібно дозволити їм захищатися самостійно». Роуланд озвучив розчарування і невдоволення керівників багатьох корпорацій, які стали

мішенями кібершпигунів і злочинних угруповань. Пентаґон вирішив захищати своїх підрядників, вочевидь, непокоячись передусім про критично важливі об'єкти інфраструктури, як-от електромережі, а не про менш важливі для економіки США компанії.

Контратаки можуть мати різні форми. Компанія здатна скерувати величезний потік мережевого трафіку на шкідливий комп'ютер і «викинути» його в офлайн. Або залізти у жорсткий диск китайського кібершпигуна, знайти вкрадені документи й видалити їх. Звісно, після отримання доступу до комп'ютера шпигуна компанія може видалити геть усю інформацію, що зберігається в ньому, ба навіть запустити вірус. Один-єдиний акт самозахисту може швидко перерости у повномасштабний конфлікт. А зважаючи на те, що китайських кібершпигунів підтримують їхні військові, американська фірма здатна розв'язати власну кібервійну проти суверенної держави.

Ані компаніям, ані приватним особам не дозволено зламувати комп'ютери у відповідь на кіберагресію. Проте немає нічого протизаконного в тому, щоб пропонувати продукти і послуги, які надає Endgame. Ця компанія залучила понад $50 млн інвестицій від провідних венчурних фондів, зокрема від Bessemer Venture Partners, Kleiner Perkins Caufield&Byers і Paladin Capital. Це величезні гроші для стартапу, що спеціалізується у кібербезпеці, особливо в таких сумнівних методах.

Роуланд пішов із посади генерального директора Endgame 2012 року, після скандального оприлюднення хакерською групою Anonymous* внутрішніх маркетингових документів компанії. В Endgame спробували уникнути публічного розголосу і навіть вимкнули свій сайт. Проте Роуланд знову виступив на конференції з провокаційною заявою про те, що американські компанії ніколи не позбудуться кібератак, якщо не почнуть завдавати ударів у відповідь. Однак Роуланд зауважив, що висловлює лише особисту думку: «У кіберпросторі нині відсутня концепція заборони. Це глобальна зона вільного вогню». Здається, принаймні один учасник дискусії підтримав Роуланда. Роберт Кларк, професор права з Військово-морського академічного центру вивчення кібербезпеки, заявив перед аудиторією таке: якщо

* Anonymous – міжнародне угруповання інтернет-користувачів без постійного розташування чи складу, яке здійснює хакерські акції на знак протесту проти обмеження свободи в мережі інтернет.

компанія, що її атакують, проникне в комп'ютер злодія і видалить викрадену в неї інформацію, це не буде порушенням закону. «Це найбезглуздіша річ, яка спадає мені на гадку, – сказав Кларк. – Це мої дані, ось тут, і я повинен мати можливість їх видалити».

За кілька місяців після нью-йоркської заяви Роуланда компанія Endgame представила нового генерального директора. Їм став Натаніель Фік, 35-річний колишній капітан морської піхоти, який служив у Іраку й Афганістані, а згодом отримав диплом MBA у Гарвардській бізнес-школі та брав участь у роботі відомого наукового центру в Нью-Йорку. Фік видав спогади про свій бойовий досвід і став героєм книжки «Покоління вбивць», за сюжетом якої телеканал HBO зняв міні-серіал.

За словами двох осіб, які знають Фіка і знайомі із бізнес-стратегією компанії Endgame, новий генеральний директор намагався розірвати контракти з розвідувальними структурами і покласти край бізнесу, пов'язаному з уразливостями нульового дня. Він вважав цей напрям дуже сумнівним і не надто прибутковим, адже вартість одного-єдиного експлойта може сягати ста тисяч доларів. Чистий прибуток від торгівлі кіберзброєю був дуже низьким.

Проте піти з цього бізнесу було непросто. Інвестори компанії Endgame були пов'язані з державними замовниками, які мали глибокі кишені та планували витратити мільярди доларів на кібероборону й атаки протягом найближчих декількох років. Радники Endgame також були віддавна пов'язані з вигідними клієнтами, зокрема з відставним діячем Пентаґону, що обіймав за різних часів впливові управлінські посади в сфері технологій, а також із менеджером відділу управління інформаційними системами ЦРУ. Сам голова ради директорів Endgame обіймав посаду генерального директора компанії In-Q-Tel – венчурного фонду ЦРУ, а один із членів ради директорів раніше очолював АНБ.

Проте, як зауважив Фік невдовзі після призначення, що відбулося 2012 року, час величезних військових витрат, що почався після терактів 11 вересня, добігав кінця: США згортали військову присутність в Іраку й Афганістані, наближався період суворої ощадливості, а в Конгресі почастішали заклики до збалансованого бюджету й зменшення державних витрат. «Оборонний бюджет опиниться під тиском, але так і повинно бути, – сказав Фік. – Надмірні витрати за окремими

статтями впродовж останніх десятиліть уже не виправдовують себе». Однак він додав: «Гадаю, фінансування деяких напрямів збільшуватиметься й надалі».

Це зростання витрат спостерігаємо у приватному секторі. Двоє знайомих із Фіком осіб розповіли, що компанія Google стала одним із найбільших покупців пакетів вразливостей нульового дня у компанії Endgame. Якби Google завдала удару по тим, хто намагався викрасти її інтелектуальну власність, це було б порушенням закону. Проте Google була однією з найпомітніших і, поза сумнівом, найвпливовіших компаній, які наполегливо закликали Конгрес і адміністрацію президента Обами засудити Китай за кібершпигунство й піти на дипломатичні кроки, якщо ця країна не може приборкати власних хакерів. Особливо після того як Google став об'єктом масштабної шпигунської кампанії, внаслідок якої Китай викрав дещо його інтелектуальної власності, та почав ділитися з АНБ інформацією про атаки на власні мережі.

Роуланд – не єдиний працівник Endgame, який заявляв, що компанії мають право захищатися, якщо держава не може або не хоче захистити їх. Після публікації хакерами з групи Anonymous презентації компанії, в якій ішлося про те, як саме клієнти Endgame можуть використовувати кластери інфікованих комп'ютерів (так звані ботнети) для атак на сайти або викрадення паролів та іншої конфіденційної інформації, партнер одного з основних інвесторів Endgame виступив на захист цієї ідеї. «Якщо ви прогнозуєте, що війни майбутнього відбуватимуться у кіберпросторі, хіба не варто мати власну кіберармію? – заявив в інтерв'ю агентству Reuters Тед Шлейн, член ради директорів Endgame.

Більшість приватних компаній, що працюють у сфері кібербезпеки, просто зі шкіри пнуться, наголошуючи на тому, що не проводять контратак, уламуючись у комп'ютери хакерів, бо в США це незаконно. Проте компанії стежать за хакерами, які проникають у мережі їхніх клієнтів. Один із провідних гравців у цьому бізнесі, компанія CrowdStrike, спокушає шпигунів так званими горщиками з медом – фальшивими клієнтськими мережами, які насправді є стерильною зоною, недоступною для працівників і комп'ютерів важливих клієнтів. Суть пастки в тому, щоб виграти час для спостереження за хакерами й визначити, що саме їх цікавить (до прикладу, шукають вони технічні схеми або хочуть дізнатися подробиці угод), а відтак змусити пока-

зати інструменти та техніки, якими вони користуються для крадіжки інформації. Наприклад, компанія може захистити документ особливо складним паролем, сподіваючись, що хакер скористається новим способом зламування. Щойно клієнт зрозуміє, яким інструментарієм послуговується крадій, CrowdStrike зможе спрогнозувати, як саме хакер намагатиметься проникати в інші системи. Якщо клієнт хоче збити хакера зі шляху, він може подати оманливу або неправдиву інформацію в документах, які хакер вважатиме бізнес-стратегією або планами з випуску нової продукції.

CrowdStrike також аналізує профілі жертв хакера, щоб зрозуміти, які саме галузі або види технологій його цікавлять. Потім компанія складає досьє, і інколи навіть дає хакерові ім'я. Аналітики CrowdStrike понад рік відстежували кіберзлодія, якого назвали Anchor Panda, він шпигував за компаніями, пов'язаними із виробництвом супутників, аерокосмічною й оборонною галуззю, а також цікавився програмами космічних досліджень іноземних держав. Озброєні специфічною інформацією про цілі хакера та його методи зламування, клієнти CrowdStrike теоретично можуть застосовувати надійніші захисні заходи. Це наче розсилка точного опису зовнішності та поведінки злочинця по всіх поліцейських відділах, що значно ефективніше, ніж заклики до громадськості бути пильними під час зустрічі з підозрілими людьми.

Ця діяльність дуже нагадує роботу правоохоронних органів. І це не дивно, бо двоє керівників CrowdStrike – колишні агенти ФБР. Шон Генрі, генеральний директор CrowdStrike Services, підрозділу компанії, який вистежує та ідентифікує хакерів, служив у бюро 24 роки і лише 2012 року залишив посаду, на якій відповідав за всі міжнародні кіберпрограми й розслідування. (Колишній заступник директора кіберпідрозділу ФБР працює головним консультантом компанії.) Генрі стверджує, що CrowdStrike відрізняється від інших аналогічних компаній тим, що коли «ми реагуємо на втручання, то влаштовуємо справжнє полювання на ворога». Він каже, що компанія застосовує методи комп'ютерної криміналістики та перепрограмування шкідливого ПЗ, щоб зрозуміти тактику хакерів, методи їхньої роботи й мотивацію. Він уникає будь-яких згадок про вторгнення в комп'ютери противників компанії, адже колишній агент ФБР і сам упродовж років переслідував інших за порушення антихакерських законів. Проте слово «полювання» натякає на агресивнішу форму аналізу, ніж визнає

більшість компаній, що працюють у цій сфері. CrowdStrike встановлює сенсори в мережах клієнтів і залучає добровольців для збору інформації про методи хакерських атак, щойно вони починаються, а не лише збирає докази після завершення атаки. Компанія використовує отримані дані, щоб визначити належність хакера до певної групи або країни. Це одна з найскладніших проблем кіберкриміналістики, бо хакери зазвичай приховують власне розташування, послуговуючись для атак інфікованими комп'ютерами в інших країнах. CrowdStrike обіцяє повідомляти своїх клієнтів не лише про методи атак, а й про те, хто і навіщо це робить. Компанія приділяє чільну увагу виявленню шпигунів і хакерів, що працюють на інші держави, зокрема на Іран, Китай і Росію. (Група аналітиків з підрозділу «стратегічної розвідки» володіє китайською, фарсі та російською.) У своїх маркетингових матеріалах компанія CrowdStrike повсякчас наголошує, що використовує методи збору розвідданих для ідентифікації хакерів і передає специфічну, корисну інформацію про них клієнтам.

Ця методика також запозичена з арсеналу ФБР. Бюро «брало в оточення» хакерів, найвідоміші з яких належали до групи Anonymous, стежачи за тим, як вони викрадають дані в компаній і приватних осіб. Згодом ця інформація ставала підставою для кримінального переслідування. Проте CrowdStrike та її клієнтам не завжди йдеться про висунення звинувачень. І ось тут виявляється агресивна природа бізнес-моделі компанії.

За словами Генрі, ще одна відмінність CrowdStrike від конкурентів полягає в «здатності атакувати».

«Ідеться не про зустрічні хакерські атаки, – говорить Генрі, відмітаючи будь-які натяки на те, що компанія порушує закон. – Ідеться про забезпечення клієнта певними можливостями для створення й організації ворожого робочого середовища» в його мережі. Керівники CrowdStrike знають, що деякі компанії створюють це «вороже середовище», інсталюючи шкідливе ПЗ у пастках, розкиданих ними у власних мережах. Коли зловмисник завантажує документ або файл на свій комп'ютер і намагається його відкрити, активується вірус, який може знищити дані на жорсткому диску або встановити шпигунське ПЗ чи бекдор, що дозволить жертві атаки зайти до комп'ютера хакера. Компанія CrowdStrike заявляє, що не використовує хитрощів для зараження комп'ютерів. Проте співзасновник CrowdStrike Дмітрій Альперович в інтерв'ю 2013 року розповів, що влада Грузії схвалила

подібні дії і внаслідок цього російський хакер завантажив шпигунське ПЗ, яке дозволило правоохоронним органам сфотографувати його за допомогою його ж власної веб-камери. Цю фотографію долучили до офіційного звіту. «Приватний сектор повинен набути права на такі дії», – заявив Альперович.

У лютому 2014 року, після того як компанія Target повідомила про хакера, який украв понад 100 млн номерів кредитних і платіжних банківських карт, CrowdStrike створила навчальний онлайн-семінар на тему боротьби з кіберзлочинністю. «(Від)плати: не будь мішенню!» – було написано в рекламі, яку компанія розіслала своїм потенційним клієнтам електронною поштою. Навчальний курс повинен був навчити компанії «застосовувати проактивний підхід для захисту власних мереж» і показати, «як використати інформацію про загрози для того, щоб бути готовим до будь-якої несподіванки». Можливо, компанія CrowdStrike не завдавала контрударів власноруч, але попередження, надіслані клієнтам, і послуги, які вона рекламувала, натякають, що клієнти можуть освоїти необхідні навички на випадок, якщо вирішать «відплатити» самостійно.

Відшукування противника – це величезний поступ, якщо порівнювати з простим спостереженням за його діями, як із технічного, так і з правового погляду. Проте тут також існує ринок для кібернайманців, які розробляють і продають шпигунське ПЗ і хакерські інструменти, що не поступаються державним розробкам США кількарічної давності. Потужність розподілених обчислювальних систем, таких як хмарні сховища, дозволяє невеликим групам створювати щораз складніше програмне забезпечення, і невдовзі маленькі компанії зможуть створювати потужну кіберзброю, яка донедавна була доступною лише державним структурам. Найманці вже зараз допомагають представникам влади залякувати й переслідувати активістів і дисидентів. Пристрої, розроблені найманцями, – серед найстрашніших і найнебезпечніших у кіберпросторі.

Маркетингові документи фірми Gamma, розташованої у Великій Британії, містять пропозицію продажу шпигунської програми FinFisher, яка ховається всередині «фальшивих оновлень для популярного програмного забезпечення». Шпигунська програма, здатна контролювати комп'ютер, копіювати файли та записувати кожне слово, набране користувачем, замаскована під оновлення популяр-

ного застосунку iTunes. Користувач запускає оновлення, вважаючи, що отримує нову версію музичної програми, а насправді інсталює на комп'ютер програму FinFisher. Єгипетські поборники демократії звинуватили компанію в постачанні шпигунської програми режимові президента Хосні Мубарака, але компанія відкинула ці звинувачення. Мубарак віддав наказ силового розгону протестувальників у 2011 році, незадовго до того, як його усунули від влади. Дослідники в сфері безпеки стверджують, що копії програми FinFisher були знайдені в електронних листах, надісланих на адреси борців за демократію в Бахрейні.

Кібершпигуни та наймані хакери відкрито пропонують свої послуги правоохоронним органам і службам розвідки. Італійська компанія Hacking Team, розташована у Мілані, пропонує «повний контроль над об'єктами» за допомогою «невидимих» методів, які «не піддаються виявленню й не залишають слідів».

«Переможи шифрування! – говориться в одній презентації на сайті компанії, що наслідує стиль АНБ. – Тисячі зашифрованих онлайн-комунікацій щодня. Отримай їх!» У 2011 році компанія відкрила офіс в Аннаполісі (штат Меріленд), щоб працювати з американськими клієнтами.

Компанія Hacking Team розповідає про свій бізнес відверто. «Інколи важлива інформація захована всередині пристрою, ніколи не передається та зберігається під надійним захистом… аж поки ви не проникнете у цей пристрій», – написано в брошурі, що описує один із шпигунських продуктів компанії – «Систему віддаленого управління» (Remote Control System).

> «Питання в тому, чи існує простий спосіб проникнути в цей пристрій?.. Усе, що вам треба зробити, – це обійти шифрування, витягнути потрібну інформацію з пристрою та продовжувати стежити за об'єктами, хоч би де вони були, навіть за межами області моніторинґу. Remote Control System робить саме це. Отримайте контроль над вашими цілями і стежте за ними, незважаючи на шифрування і мобільність. Хакніть цікаві вам об'єкти за допомогою найзаразливішого програмного забезпечення. Увійдіть у безпровідну мережу і проведіть тактичні операції за допомогою спеціального обладнання, розробленого для віддаленої ро-

боти. Простежте за усіма цілями і управляйте ними віддалено, з одного-єдиного екрана».

Відомо, що програма може вмикати камеру і мікрофон ноутбука, перетворюючи його на підслухувальний пристрій.

Лише наприкінці брошури компанія Hacking Team згадує, що її продукт призначений лише для «санкціонованого прослуховування». (Компанію заснували два хакери, які розробили шпигунську програму на замовлення місцевої італійської поліції.) Hacking Team наголошує, що продає свій продукт лише державним правоохоронним органам і розвідслужбам, а також не постачає його в «країни, внесені до чорного списку» Сполученими Штатами, Європейським Союзом, НАТО або членами Асоціації держав Південно-Східної Азії (ASEAN). Компанія також обіцяє аналізувати кожного потенційного клієнта, щоб переконатися, чи технологія не буде «використана для порушення прав людини».

Проте в жовтні 2012 року дослідники з Citizen Lab Торонтського університету повідомили, що програма Remote Control System компанії Hacking Team була використана для зараження комп'ютера відомого поборника демократії з Об'єднаних Арабських Еміратів Ахмеда Мансура – 44-річного інженера-електрика, якого ув'язнили за підписання онлайн-петиції із закликом до чесних виборів у країні з династичною монархією. Мансур мимохіть завантажив шпигунську програму, сховану в «звичайному» електронному листі. Шпигунське ПЗ проникнуло в глиб персонального комп'ютера, аналізуючи всі файли й записуючи геть усе, що Мансур набирав на клавіатурі. Він зауважив, що комп'ютер почав працювати повільніше, а коли дізнався, що активістів у Бахрейні вистежили за допомогою програми FinFisher, зв'язався з фахівцями у сфері інформаційної безпеки, і ті підтвердили, що його комп'ютер хакнули. Шпигунське ПЗ було таким сильним, що навіть після зміни пароля електронної пошти невидимий хакер надалі читав листування Мансура. Зловмисник отримав повний контроль над комп'ютером, відстежував усі онлайн-комунікації Мансура і його зв'язки з іншими активістами. Сліди вели до інтернет-адреси в Об'єднаних Арабських Еміратах.

Місяць потому, як фахівець допоміг Мансурові позбутися шкідливого ПЗ, на активіста напали на вулиці.

Нападник знав ім'я Мансура, і той підозрював, що його могли вистежити через мобільний телефон. У цій бійці йому не завдали серйозних пошкоджень. Проте не минуло й тижня, як на Мансура знову напали і кілька разів ударили по голові. Чоловік пережив і цей напад.

Мансур – не єдиний активіст, комп'ютер якого, на думку дослідників, заразили шпигунським ПЗ компанії Hacking Team. Він став одним із багатьох громадських активістів, проти яких застосовувалися комерційні шпигунські програми під час заворушень на території Північної Африки та Близького Сходу. Немає жодних доказів того, що Hacking Team знала або була якимсь чином причетна до нападів на Мансура, і документальні докази того, що її продукт використали протизаконним способом, компанія називає «випадковим збігом обставин».

Компанія самостійно визначає законність власних операцій. І не одна вона. Не існує жодного міжнародного органу або закону, який контролює продаж шпигунського ПЗ і хакерських інструментів лише на законних підставах або лише тим державам, які не порушують прав громадян і не переслідують активістів. Також не існує жодних процедур контролю за поширенням такої кіберзброї, як Stuxnet. Протягом кількох останніх років політичні верхівки США, Росії, Китаю та низки інших країн почали обговорювати проблему відсутності законодавства щодо кіберзброї, але жодна країна досі не підійшла впритул до ухвалення закону, який міг би стримати її від створення зброї нового покоління. Як має виглядати закон про кіберзброю, докладно невідомо. На заводах зі збагачення ядерного палива можна провести інспекцію. Танки, кораблі й літаки видно здалеку. Натомість кіберзброю можна просто вбудувати у комп'ютер. І вона практично непомітна, поки хтось не скористається нею.

Звинувачення компаній зі сфери кібербезпеки у співпраці із владою під час так званої Арабської весни прозвучали не вперше. Восени 2010 року, приблизно тоді, коли сайт WikiLeaks готувався оприлюднити викривальну інформацію про Bank of America, що містила внутрішні звіти й документи банку, представники Міністерства юстиції США зв'язалися з юристами банку та рекомендували їм вдатися до послуг юридичної фірми з Вашинґтона Hunton & Williams. Остання об'єднала три невеличкі технологічні компанії для проведення про-

пагандистської кібероперації проти опонентів Торговельної палати США – провідного лобіста бізнес-інтересів у Вашинґтоні. Група планувала проаналізувати сайти та соціальні мережі за допомогою особливої технології аналізу даних і скласти досьє на опонентів Палати. Компанія Hunton & Williams звернулася до групи, що працювала під назвою Team Themis, з проханням учинити так само з людьми, що підтримують WikiLeaks, а також визначити, де саме організація зберігає секретну інформацію, отриману з анонімних джерел.

«Вочевидь, якщо вони зможуть довести, що WikiLeaks зберігає дані в певних країнах, це спростить судове переслідування цієї організації», – написав в електронному листі колегам один із членів групи. Міністерство юстиції шукало інформацію, за допомогою якої можна було дискредитувати засновника WikiLeaks Джуліана Ассанжа, який оприлюднив секретні звіти військової розвідки та телеграми Держдепу. А зараз федерали хотіли доручити частину розслідування найманцям, спонукаючи Bank of America до співпраці з групою Team Themis, названою на честь героя грецької міфології Титана, який утілював «божественний закон» на противагу законові людському.

До групи Team Themis входила компанія Palantir Technologies, стартап із Кремнієвої долини, яка швидко потоваришувала з такими важковаговиками національної безпеки, як Річард Перл, колишній голова Ради з питань оборонної політики і впливовий республіканець, а також Джордж Тенет, колишній директор ЦРУ, що пішов працювати до Герба Аллена, інвестора компанії Palantir і очільника загадкового інвестиційного банку Allen & Company, що проводить щорічні конференції в Сан-Валлі (штат Айдахо), збираючи під одним дахом відомих журналістів, спортсменів і бізнесменів. Компанія Palantir отримала початкові інвестиції від венчурного фонду ЦРУ In-Q-Tel, голова якого очолював компанію Endgame.

До групи Team Themis входили ще дві фірми зі сфери кібербезпеки: HBGary Federal, генеральний директор якої відчайдушно намагався навести контакти з АНБ, і Berico Technologies, в якій працював ветеран іракської війни з досвідом використання кіберзброї у польових умовах. З пропозиції, розробленої групою, випливає, що Team Themis планувала створити аналітичний підрозділ, покликаний забезпечувати юристів інформацією про «організації опонентів і мережі, що викликають зацікавлення». Гендиректор HBGary Аарон Барр сказав, що команда збиратиме інформацію про «фоловерів і

волонтерів із різних країн світу», що підтримують WikiLeaks, а також про спонсорів організації з метою залякування їх. «Потрібно втовкмачити цим людям: у разі, якщо вони підтримують цю організацію, ми їх переслідуватимемо», – писав Барр в електронному листі. Він запропонував надсилати WikiLeaks недостовірні документи, сподіваючись, що сайт оприлюднить їх і дискредитує себе. Барр також переконував узяти на гачок «таких людей, як Ґленн Ґрінволд» (блогер і активний прибічник WikiLeaks), і хотів розпочати «кібератаки» на шведські сервери WikiLeaks, щоб «отримати дані» про анонімні джерела організації та розкрити їх.

Компанія Team Themis не мала шансу розпочати свою шпигунську та пропагандистську кампанію. У лютому 2012 року в одній зі статей Financial Times навели слова Барра, який вихвалявся, що в змозі проникнути у внутрішню структуру хакерської групи Anonymous. Хакери відповіли тим, що зламали електронну пошту Барра й оприлюднили всі листи за минулий рік, зокрема й комерційні пропозиції і листування Team Themis. Звільняючись із компанії, Барр заявив журналістам: «Я хочу приділяти більше часу своїй родини й узятися за відновлення власної репутації». Компанія Berico продовжує працювати. Вона продає державним організаціям послуги з аналізу даних і геолокаційне ПЗ. Компанія Palantir залишається однією з найперспективніших технологічних компаній у сфері національної безпеки, а серед її клієнтів – ЦРУ, Командування спеціальних операцій і Корпус морської піхоти США. Усі вони використовують програмне забезпечення, розроблене компанією для стеження за терористами, і так само чинить Розвідувальне управління збройних сил США, Національний антитерористичний центр, Міністерство внутрішньої безпеки та ФБР. Кіт Александер, колишній директор АНБ, сказав, що Palantir здатна допомогти «бачити» хакерів і шпигунів у кіберпросторі і що програмний продукт, пропонований компанією, в агентстві схвалили. Серед клієнтів Palantir – департаменти поліції Лос-Анджелеса і Нью-Йорка, в яких створені розвідувальні й антитерористичні підрозділи, які, на думку багатьох експертів, діють ефективніше, ніж ФБР і ЦРУ.

Хоча група Team Themis зазнала поразки, американська влада звернулася до інших кібершпигунів для стеження за WikiLeaks і надання допомоги в інших розслідуваннях. 2011 року компанія Tiversa з Пітсбурґа потрапила на шпальти газет, звинувачуючи WikiLeaks у використанні піринґової файлообмінної системи (штибу тих, що

використовуються для скачування музики) для здобуття секретних військових документів. WikiLeaks, яка заявляла, що оприлюднює лише документи, отримані від інформаторів, назвала ці звинувачення «абсолютно брехливими». Tiversa передала свої знахідки державним слідчим, які спробували відкрити судову справу проти Ассанжа. Членами консультативної ради компанії Tiversa були відомі експерти зі сфери інформаційної безпеки й колишні американські держслужбовці, як-от генерал Веслі Кларк, колишній очільник Вищого штабу союзних держав Європи та кандидат у президенти від Демократичної партії, і Говард Шмідт, колишній радник Барака Обами з питань кібербезпеки.

Компанія Tiversa виявила у файлообмінних мережах низку секретних і вкрай важливих державних документів. Компанії та державні структури, збентежені витоками інформації, отримали стимул для посилення заходів безпеки й захисту ключової та секретної інформації. Tiversa оголосила, що її аналітики знайшли креслення президентського ґвинтокрила Marine One на комп'ютері, розташованому в Ірані. Ймовірно, якийсь працівник оборонного підприємства в місті Бетесда (штат Меріленд) скористався файлообмінною системою і користувач з Ірану отримав доступ до жорсткого диска його комп'ютера. У 2009 року Tiversa розповіла комітету Конгресу, що під час розслідування були виявлені: документи таємних служб щодо розташування конспіративної квартири для першої леді у разі виникнення надзвичайної ситуації; електронні таблиці, що містять персональні дані тисяч американських військовослужбовців; перелік ядерних об'єктів із зазначенням місця їхнього розташування; персональна медична інформація тисяч приватних осіб, зокрема дані про медичну страховку та платіжні документи, а також результати діагностичних процедур.

Але, доводячи слабкий захист систем, сама компанія Triversa стала причиною конфліктів. У 2013 році компанія з Атланти LabMD, що займається діагностикою раку, звинуватила Tiversa в крадіжці інформації про пацієнтів як в самої LabMD, так і в інших медичних компаній за допомогою піринґових мереж. Федеральна торговельна комісія провела розслідування після того, як у результаті витоку інформації була розкрита інформація про пацієнтів LabMD. Компанія заявила, що влада найняла Tiversa для того, щоб отримати документи без згоди й інформування LabMD. Згідно з документами судової

справи, компанія Triversa виявила інформацію про пацієнтів LabMD у піринґовій мережі, а потім невпинно телефонувала й надсилала електронні листи медичній компанії, намагаючись продати свої послуги із забезпечення кібербезпеки. Згодом LabMD відкликала свій позов (або ж його відхилили), натомість Tiversa подала зустрічний позов за наклеп.

У кіберпросторі немає визначених кордонів. Проте географія відіграє не останню роль у тому, як далеко ладні зайти кібернайманці задля вирішення проблем клієнтів. Деякі європейські компанії мають менше упереджень проти атак у відповідь, позаяк тамтешні антихакерські закони не суворі або взагалі відсутні. Наприклад, Румунія, що стала одним із розплідників хакерів і онлайн-аферистів, готових поширювати шкідливе ПЗ за винагороду. Ще одне місце, де можна найняти хакерів, – це тіньовий ринок уразливостей нульового дня. У 2013 році федеральна влада прикрила онлайн-ринок постачальників хакерських послуг під назвою «Шовковий шлях» (Silk Road), доступ до якого був відкритий через анонімну систему-маршрутизатор Tor.

Донині жодна американська компанія не зізналася в тому, що здійснює агресивні кібероперації, спрямовані на викрадання інформації або знищення електронних систем противника. Однак колишні працівники розвідки стверджують, що хакерські атаки трапляються, хоча й не афішуються. «Це протизаконно. Проте це відбувається, – зізнається колишній високопосадовець з АНБ, який нині працює корпоративним консультантом. – Це відбувається з поради юристів. Але я б не порадив клієнтові робити це».

Колишній офіцер військової розвідки розповідає, що найактивніші хакерські контратаки здійснюються в банківській сфері. За останні кілька років банки втратили мільярди доларів через кіберзлодіїв, головно зі Східної Європи і Росії, які використовують хитромудре шкідливе ПЗ для викрадання імен і паролів клієнтів і спустошення їхніх банківських рахунків.

У червні 2013 року корпорація Microsoft об'єдналася з кількома найбільшими фінансовими організаціями, серед яких були Bank of America, American Express, JPMorgan Chase, Citigroup, Wells Fargo, Credit Suisse, HSBC, Royal Bank of Canada і PayPal, задля знешкодження величезного кластера зламаних комп'ютерів, використовуваних для здійснення кіберзлочинів. Вони націлилися на сумнозвісну групу

Citadel, яка заразила тисячі комп'ютерів у всьому світі і таємно від господарів перетворила їх на армію «ботнетів»*, яку злочинці використовують для викрадання персональних даних, а отже, і грошей у мільйонів людей. Під час контратаки, яку в Microsoft назвали «Операція b54» (Operation b54), відділ цифрових злочинів компанії розірвав лінії зв'язку між понад 1400 ботнетами групи Citadel і приблизно п'ятьма мільйонами персональних комп'ютерів, інфікованих шкідливим ПЗ. Крім того, Microsoft перебрала контроль над серверами, які Citadel використовувала для проведення операцій.

Компанія Microsoft хакнула Citadel. Ця операція була б незаконною, якби компанія не отримала судовий дозвіл – «благословення» на контратаку. Microsoft дістала контроль над жертвами групи Citadel, які й гадки не мали, що їхні комп'ютери інфіковані, і змогла попередити їх про необхідність інсталяції захисту вразливого програмного забезпечення. По суті, Microsoft зламала комп'ютери користувачів, намагаючись їх урятувати. (І врятувати саму себе, бо комп'ютери були заражені передусім через вразливості продуктів Microsoft, які, ймовірно, атакують найчастіше в світі.)

Це був перший випадок співпраці Microsoft і ФБР. Але вже сьома атака компанії на ботнети з 2010 року. Юристи компанії знайшли нові правові підстави для судових позовів, зокрема звинуватили злочинців, що зламували продукти Microsoft, у незаконному використанні товарного знаку компанії. Це був новий юридичний рубіж. Навіть юристи Microsoft, серед яких колишній федеральний прокурор США, визнали, що ніколи не розглядали можливості застосування сумнівних методів, що порушують чинне законодавство, задля отримання дозволу на початок кібератак. Готуючись до «Операції b54», перш ніж звернутися до ФБР, компанія Microsoft і банківські організації впродовж шести місяців стежили за групою Citadel. Урешті-решт нишпорки з антихакерської групи Microsoft увійшли у дві бази даних служб інтернет-хостингу в Пенсильванії та Нью-Джерсі, де спільно з федеральними маршалами** зібрали кримінальні докази, які до-

* Ботнет – це мережа комп'ютерів з таємно запущеним у них автономним програмним забезпеченням (ботами), яке дозволяє зловмисникам виконувати певні дії з використанням ресурсів інфікованого пристрою.

** Федеральні маршали – співробітники Служби федеральних маршалів США, підрозділу Міністерства юстиції, яке забезпечує діяльність федеральних судів, розшукує й арештовує державних злочинців, а також бореться з тероризмом.

зволили компанії отримати дозвіл на кібератаку. Військові назвали б цю операцію збором даних про ціль. І, за багатьма ознаками, «Операція b54» нагадувала військову кібероперацію. З технічного боку вона не надто відрізнялася від атаки американського кібервійська на мережу Obelisk, яку використовували члени «Аль-Каїди».

Щоб завдати удару по групі Citadel, компанія Microsoft співпрацювала з правоохоронними органами 80 країн світу. Керівник Відділу розслідування кіберзлочинів Європолу, правоохоронної організації Європейського Союзу, заявив, що «Операція b54» успішно вибила Citadel майже з кожного зараженого групою комп'ютера. А юрист відділу цифрових злочинів компанії Microsoft проголосив: «Погані парубки дістали копняка».

Компанія Microsoft продовжує атакувати ботнети, і її успіх надихає державних діячів і керівників корпорацій, які бачать на власні очі, що співпраця між поліцією та корпоративними хакерами може бути дієздатним методом боротьби з кіберзлочинністю. Проте узгоджені контрудари, як-от атака на групу Citadel, потребують часу на схвалення та планування, а також залучення команди юристів для отримання дозволу на їхнє проведення. Але що трапиться, якщо компанія не захоче чекати півроку на дозвіл завдати удару у відповідь або якщо за її плечима не стоять офіцери правоохоронних органів?

Відставного офіцера військової розвідки непокоїть той факт, що порівняно прості у технічному виконанні контрудари спонукають організації, і насамперед банки, відмовитися від співпраці з компаніями штибу Microsoft і розпочати власні атаки у відповідь, без дозволу суду. «Банки відчули смак ударів у відповідь, бо їм остогиділи тимчасові заходи, – сказав він. – Ми починаємо усвідомлювати, що підприємницький сектор не готовий миритися з подібним ризиком. І якщо уряд не може або не хоче вжити необхідних заходів, єдиний логічний вихід – вдатися до них самотужки». Він говорить, що хакерські контратаки не будуть прерогативою лише великих корпорацій. «Якщо ви знаменитість, то хіба не заплатите комусь, щоб знайти того, хто збирається оприлюднити деякі ваші пікантні фото? Чорт забирай, так!»

Безсумнівно, вони знайдуть талановитих хлопців, ладних виконати цю роботу. Опитування 181 респондента, проведене 2012 року під час конференції Black Hat USA у Лас-Веґасі, показало, що

36 % «фахівців у сфері інформаційної безпеки» брали участь у хакерських контратаках. Наразі це меншість, проте можна припустити, що не всі опитані були щирими. Але працівники компаній, що займаються кібербезпекою і поки що не проводили хакерських контратак, володіють вміннями й навичками, необхідними для розв'язування приватної кібервійни.

Колишній службовець АНБ розповідає, що кращими, на його думку, приватними фірмами зі сфери кібербезпеки керують колишні фахівці служб радіотехнічної розвідки. Ці фірми не лише використовують методи електронної розвідки, а й залучають звідти людські ресурси. З досвіду роботи в АНБ ці працівники виснували, що потрібно відстежувати дискусії на тематичних хакерських інтернет-форумах і вдавати потенційних злочинців, що бажають придбати шкідливе ПЗ.

Один керівник приватної охоронної фірми стверджує, що частина актуальної та корисної інформації про новітнє шкідливе ПЗ, хакерські методи й потенційні об'єкти надходить, що й не дивно, з найбільшого джерела шпигунів і кіберграбіжників, що діють проти США, – з Китаю. Рік Говард, до того як стати приватним кібершпигуном, очолював групу інформаційного реагування на надзвичайні ситуації. Рік розповів, що під час роботи у розвідці приватної комп'ютерної компанії iDefence він підтримував постійний зв'язок із хакерами і продавцями кіберзброї з Китаю. Його джерела розповідали iDefence про новітнє шкідливе ПЗ у наявності (так само як у США, в Китаї воно продається на тіньовому ринку), про основних гравців на цьому ринку і про цікаві для хакерів цілі. Зрештою, хакерство – це бізнес, в якому задіяні люди.

До 2013 року Говард очолював підрозділ інформаційної безпеки компанії TASC – великої IT-фірми із власним «центром операцій із забезпечення кібербезпеки». Офіс TASC розташований у бізнес-центрі міста Шантіллі (штат Вірджинія), поруч з іншими технологічними компаніями, які зробили Вашинґтон одним із найзаможніших міст Сполучених Штатів. Компанія TASC розташована в трьох будівлях і нагадує базу АНБ. Уздовж коридорів безліч дверей з табличками «Таємно», а вхід захищають кодові замки та пристрої для зчитування карт доступу. Якщо ви потрапите всередину цих захищених приміщень, навряд чи зрозумієте, де ви: у Шантіллі чи у Форт-Міді.

Чимало хакерів, що працювали колись на АНБ, не бояться говорити про співпрацю із владою. Насправді вони цим навіть пишаються. Брендон Конлон, який раніше працював у елітному підрозділі TAO і мав за плечима «10-річний досвід роботи в сфері наступальних операцій у комп'ютерних мережах у АНБ», згідно з його профілем у мережі LinkedIn, заснував IT-компанію Vahna. Конлон почав кар'єру з розробки ПЗ для імплантатів, потім перейшов працювати в TAO, де очолив гавайське відділення. Також він працював у відділі розшуку АНБ, де вистежував китайських хакерів. Випускник Військово-морської академії США, він брав участь у трьох операціях АНБ в Афганістані, а також співпрацював із ЦРУ, допомагаючи у проведенні хакерських операцій. Компанія Vahna пишається тим, що її співробітники мають «багаторічний досвід роботи в розвідувальних і оборонних кіберспільнотах», і проголошує власні «безпрецедентні можливості доступу до вразливостей у системах вашої інформаційної безпеки, зменшення ризику в зоні роботи ваших технологій і забезпечення тактичних ударів у відповідь на появу дір у системі безпеки». Інакше кажучи, все, чого Конлон учився в АНБ, він тепер може робити для корпорацій.

Упродовж кількох останніх років великі оборонні підприємства активно поглинали невеликі технологічні фірми й спеціалізовані групи, що працювали в сфері кібербезпеки, збираючи персонал, спеціалізоване ПЗ, а також укладаючи контракти з розвідувальними службами, військовими відомствами і корпораціями. У 2010 році компанія Raytheon, один із найбільших оборонних підрядників США, погодилася придбати за $490 млн IT-фірму Applied Signal Technology, що працювала у сфері кібербезпеки, обслуговуючи військові та державні організації. Цілком виправдана висока ціна компанії Raytheon, обороти якої минулого року становили $25 млрд, здавалася жалюгідними копійками. У 2013 році компанія Cisco, гігант у галузі виробництва мережевого устаткування, придбала за $2,7 млрд готівкою фірму Sourcefire. Видання New York Times назвало цю угоду свідченням «лихоманкового зацікавлення» компаніями, які спеціалізуються на кібератаках і шпигунстві. Після оприлюднення деталей угоди відставний офіцер військової розвідки сказав, що його вразила сума, яку Cisco заплатило за компанію, флагманський продукт якої збудований на відкритій для загального доступу системі виявлення вторгнень Snort, яку може використовувати будь-хто. Ця угода доводила хіба

що зростання ціни на послуги із забезпечення кібербезпеки або ж свідчила про появу чергової величезної «бульбашки» на ринку, зазначив колишній офіцер.

Проте компанії роблять ставки на виграшну карту – державні витрати на кібербезпеку. Бюджет Пентаґону на статті, пов'язані з кібербезпекою, у 2014 році становив $4,7 млрд, що на $1 млрд більше, ніж попереднього року. Армія вже не купує дорогі ракетні системи. Після появи дронів чимало керівників переконані, що нинішнє покоління винищувачів із пілотом у кабіні стане останнім. Величезні кошти, виділені за часів холодної війни на дорогі системи озброєнь, колись набили капшуки вашинґтонських підрядників, а нині вони скеровуються на кіберринок, що розвивається у швидкому темпі.

7
ПОЛІЦЕЙСЬКІ СТАЮТЬ ШПИГУНАМИ

Шпигунське програмне забезпечення стало тріумфом програмування та підступу. Ці програми непомітно працювали на комп'ютері жертви і записували все, що набирав користувач. Електронні листи. Документи. Але насамперед полювали на паролі. Зокрема, один особливий пароль – фразу або послідовність літер і цифр, використовувану жертвою для запуску програми шифрування під назвою «Доволі висока конфіденційність» (Pretty Good Privacy, PGP). На відміну від інших програм шифрування, PGP проста у використанні навіть для користувачів-початківців. Програму можна вільно завантажити з інтернету, а наданий нею рівень безпеки раніше був доступний лише державним агентам і шпигунам. Тепер, клікнувши мишкою кілька разів і ввівши пароль, будь-який користувач міг перетворити свої повідомлення на абракадабру, розшифрувати яку здатен лише той, кому призначався лист. Однак шпигунська програма перехоплювала паролі й надсилала їх своєму господареві, який міг розкодувати зашифровані повідомлення, які жертва вважала приватними. Розробники назвали своє творіння, що стало променем світла у темному царстві, «Чарівним ліхтарем» (Magic Lantern).

Творцями цієї шкідливої програми були не китайські хакери чи російські крадії особистих даних. Це були співробітники Федерального бюро розслідувань США. І працювали вони у відділі найсекретніших і технічно найскладніших операцій у тому самому бюро, яке сьогодні є незамінним партнером АНБ у проведенні шпигунських і військових кібероперацій.

Це відділ технологій перехоплення інформації (Data Intercept Technology Unit), який працівники називають DITU. Це ФБРівський аналог АНБ, який проводить операції радіотехнічної розвідки, про які навряд чи напишуть у газетах, а протягом останніх 15 років відділ згадували на слуханнях у Конгресі лише кілька разів. DITU розташований у величезній будівлі на військово-морській базі у Квонтіко

(штат Вірджинія), під дахом якої також працює академія підготовки агентів ФБР. Відділ DITU перехоплює телефонні дзвінки й електронні листи терористів і шпигунів на території Сполучених Штатів. Якщо АНБ хоче отримати інформацію від Google, Facebook, Yahoo та інших технологічних гігантів, вирушить за нею саме DITU. Відділ забезпечує технічне обслуговування програми Prism, яка збирає персональні дані в найбільших технологічних компаніях. А ще DITU стежить за тим, щоб усі американські компанії створювали комп'ютерні мережі та застосунки з дотриманням закону США про негласне спостереження на користь зовнішньої розвідки, тобто дозволяє владі шпигувати. А якщо вони відмовляться, DITU встановить пристрій стеження без їхньої згоди і виконає всю роботу за них.

АНБ не впорається без DITU. Відділ тісно співпрацює з найбільшими американськими телекомунікаційними компаніями – AT&T, Verizon і Sprint. «DITU – це основна сполучна ланка між провайдерами послуг і службами національної безпеки», – каже представник технологічної галузі, якому доводилося часто працювати із відділом. DITU слідкує за тим, щоб у величезній мережі оптоволоконних кабелів, використовуваних згаданими компаніями, можна було легко перехоплювати телефонні й інтернет-комунікації. Протягом останніх років відділ надавав ФБР допомогу в створенні комп'ютерних програм аналізу і фільтрування даних. Бюро планує встановлювати ці програми у телефонних і інтернет-мережах, збираючи щораз більше інформації, зокрема і дані про маршрути електронних листів, трафік, інтернет-адреси, номери портів, які обслуговують вхідні і вихідні повідомлення, і визначаючи, яка операційна система і які застосунки запущені на комп'ютерах.

Проект Magic Lantern став одним із перших досягнень відділу. Розроблена наприкінці 1990-х програма стала супутником відомішої програми аналізу електронних листів Carnivore, яка зчитувала інформацію із заголовка листів («кому», «від кого», дату надсилання), а слідчі аналізували комунікаційну модель, збираючи докупи розрізнені дані щодо членів кримінальної мережі. Обидві ці програми, як і інше шпигунське ПЗ, як наприклад CoolMiner, Packeteer і Phiple Troenix, були розроблені, щоб допомогти ФБР ловити наркоторговців, терористів і розповсюджувачів дитячої порнографії. Проте, коли про Carnivore заговорили в новинах, програму назвали засобом державного стеження у стилі «Великого брата», а захисники цивільних свобод

заявили, що методи ФБР дискредитують систему шифрування, яку використовують у законних цілях (наприклад, для захисту фінансової інформації чи особистих даних пацієнтів). Ті самі арґументи прозвучали по упливі десятиліття, коли стало відомо, що АНБ таємно ослаблює алгоритми шифрування.

ФБР почало використовувати шпигунські програми за декілька років до терактів 11 вересня і до перших спроб АНБ охопити шпигунською мережею цілу територію США. Агенти ФБР займалися внутрішнім кібершпигунством триваліший час, ніж їхні друзяки з Форт-Міда. Нині ці дві організації фактично об'єднали свої зусилля. Від Квонтіко до штаб-квартири АНБ тягнуться оптоволоконні лінії, тому інформація, зібрана DITU, миттєво передається за призначенням. Агенти ФБР і працівники Міністерства юстиції аналізують запити АНБ на збір електронної пошти в Google і відстежування постів у Facebook. Вони представляють агентство в секретному Суді спостереження за іноземною розвідкою, який також розглядає запити на стеження за американцями. Саме ФБР подало до суду прохання зобов'язати телефонні компанії передавати в АНБ записи всіх телефонних дзвінків, зроблених із території США. Коли журналісти та законотворці виголошують, що АНБ «шпигує за американцями», насправді вони мають на увазі, що ФБР допомагає АНБ, надаючи технічну й правову інфраструктуру для проведення внутрішніх розвідувальних операцій. Посередницька роль DITU дозволяє технологічним компаніям стверджувати, що вони не передають інформацію про клієнтів АНБ. І це правда. Вони передають її відділові DITU, який надсилає її в АНБ.

АНБ є найбільшим користувачем DITU. Але цей відділ аж ніяк не обмежується роллю хлопчика на побігеньках. Разом з іншими групами розвідки та кіберспостереження ФБР відділ DITU здійснює деякі з найскладніших державних розвідувальних програм. У академії ФБР у Квонтіко DITU ділить простір із відділом оперативних технологій (Operational Technology Division), який відповідає за технічний збір, обробку інформації та надсилання її до ФБР. Його девіз – «Пильність завдяки технологіям». Серед відомих можливостей відділу – шпигунські операції у наземних лініях зв'язку, безпровідних мережах, а також у комунікаціях комп'ютерних мереж, зокрема стеження за електронною поштою, комутаторами і маршрутизаторами, завантаження аудіофайлів, відеозаписів, зображень та інших цифрових доказів у розслідуваннях, а також дешифрування. Відділ спеціалізується

на нелегальному проникненні в приміщення, запуску комп'ютерних вірусів та інсталяції пристроїв стеження. Відділ DITU купує в провідних американських технологічних компаній привілейований доступ до їхніх систем. Наприклад, за дорученням АНБ відділ співпрацює з компанією Microsoft, припильновуючи, щоб нові функції програми Outlook, завдяки яким користувачі можуть створювати поштові адреси, не стояли на перепоні шпигунству. Угода з компанією допомогла урядові обійти процедуру шифрування Microsoft, відтак державні аналітики можуть читати повідомлення Outlook.

ФБР почало займатися кіберполюванням іще до того, як ця діяльність стала пріоритетом національної безпеки. Уперше ФБР використало хакерські методи у програмі «Кіберлицар» (Cyber Knight) – саме тоді бюро й створило шпигунську програму Magic Lantern. Програмісти ФБР розробили «маячки», тобто програми, які можуть вбудовуватися в електронні листи й визначати інтернет-адресу комп'ютера користувача. Перші маячки використовували для пошуку викрадених дітей. Коли викрадач зв'язувався з батьками дитяти (зазвичай викрадач був колишнім чоловіком або партнером), агент ФБР писав відповідь. І коли злочинець відкривав електронного листа, маячок починав працювати. Він не завжди вів агентів до будинку викрадача, але принаймні дозволяв визначити, звідки саме останній надіслав повідомлення. Це була чудова підказка. (Розробка цих маячків поклала початок розвиткові технології, за допомогою якої спецслужби склали схему мереж ядерного об'єкта в іранському місті Нетенз.)

ФБР використовувала маячки для вистежування дитячих порнографів. Бюро заражало їхні комп'ютери вірусами та шпигунським ПЗ, яке позначало дитячі фотографії, а потім відстежувало пересилання фото від одного користувача до іншого. Агенти збирали докази для кримінального переслідування й аналізували мережу обміну дитячою порнографією. У цьому сенсі це була операція зі збору розвідданих.

Згідно з американським законодавством, ФБР відповідає за розслідування всіх кіберзлочинів, шпигунства й атак на території США. Бюро підпорядковується Національній об'єднаній робочій групі із розслідування кіберзлочинів, створеній за наказом президента, до якої також входять Секретна служба, ЦРУ і АНБ. Окрім кібершпигунства і зондування мережевої інфраструктури, група запобігає злочинам у фінансовій сфері та онлайн-шахрайству, спостерігає за групами

так званих хактивістів, які проводять акції протесту проти компаній і державних агентств, а також контролює розвиток внутрішніх загроз, пов'язаних, наприклад, із просочуванням у пресу інформації від держслужбовців.

Зазвичай робота ФБР полягає в збиранні доказів для кримінальних справ. Але коли йдеться про кібербезпеку, ФБР відходить від правоохоронної місії й діє радше як служба розвідки, дбаючи насамперед про прогнозування та попередження кібератак, ніж про судове переслідування хакерів.

«Бюро зосереджується передусім на зборі інформації і передачі її АНБ, розвідувальному співтовариству та Міністерству оборони, – розповідає високопосадовець із правоохоронних органів, який працює над розслідуваннями внутрішніх і міжнародних кіберзлочинів, зокрема фінансового шахрайства та розповсюдження дитячої порнографії. Загалом, ФБР і не намагається довести справи до суду». Правоохоронець каже, що упродовж кількох останніх років ФБР перепрофільовує багатьох співробітників із питань протидії тероризму на проблеми кібербезпеки, що стали найвищим «пріоритетом національної безпеки», випереджуючи посадові злочини, корупцію в органах влади й порушення прав громадян. В антитерористичних відділах і контррозвідці – в бюро їх групують – завжди був величезний штат: майже 13 тисяч осіб у 2013 році. Від 2001-го до 2009 року кількість агентів у відділі протидії тероризму збільшилася вдвічі. Це зростання збіглося з різким зменшенням кількості кримінальних переслідувань у справах, не пов'язаних із терористичною діяльністю, зокрема тих, що стосуються посадових і економічних злочинів. (ФБР звинувачували у тому, що бюро не доклало необхідних зусиль для розслідування шахрайських операцій з іпотекою та цінними паперами напередодні фінансової кризи 2008 року.)

У 2012 році бюро витратило на різні кібероперації $296 млн. Наступного року його чільники попросили в Конгресу додаткові $86 млн для програми ФБР «Кіберініціатива нового покоління» (Next Generation Cyber Initiative), яка дозволяла збільшити розвідувальні можливості бюро за допомогою додаткового штату й створення нової системи аналізу шкідливого ПЗ і втручань у комп'ютерні системи. Бюро планувало найняти 152 нових співробітники, окрім уже наявних 1232 осіб, більшість яких була не агентами ФБР, а фахівцями з комп'ютерних наук, інженерами, криміналістами та інформаційними

аналітиками. Кіберпрограми поглинали більшу частину бюджету ФБР, який стрімко зростав. Незадовго до звільнення директор агентства Роберт Мюллер, який почав працювати за тиждень до терактів 11 вересня, заявив у Конгресі, що «в осяжному майбутньому кіберзагрози зрівняються або навіть перевершать рівень загрози поширення тероризму».

Переслідування кіберзлочинців та іноземних кібервоїнів – це майбутнє ФБР. Бюро дедалі більше нагадує ЦРУ або АНБ. Більшість нових співробітників – це інформаційні аналітики й хакери, а не правоохоронці. А урядовці говорять про те, що ФБР почало частіше посилатися на Акт про негласне спостереження на користь зовнішньої розвідки для збору інформації в межах розслідування кіберзлочинів, адже так простіше отримати дозвіл на стеження, ніж посилаючись на Кримінальний кодекс, який вимагає від правоохоронців надання обґрунтованих доказів скоєння злочину.

«Інформація, здобута у рамцях FISA, не використовується для кримінального переслідування. Тож навіщо ми її збираємо? Я й гадки не маю, – зізнався високопосадовець із правоохоронних органів. – Від певного часу ми більше не проводимо розслідувань. Ми просто збираємо розвіддані». Інакше кажучи, ФБР шпигує.

Це важлива зміна у політиці провідної правоохоронної структури США. Коли ФБР збирає інформацію для використання в суді, бюро доводиться дотримуватися суворіших процедур, що контролюють збір доказів, і триматися у визначених межах розслідування. Натомість коли бюро робить розвідку першочерговою місією, воно розкидає ширші тенета й зосереджується передусім на пошуку цілей для АНБ і військових кібервоїнів, а не на притягуванні злочинців до суду.

Китайські кібершпигуни, що викрадають об'єкти інтелектуальної власності, стали одними з найважливіших цілей для ФБР. «Ми збираємо великі об'єми інформації про діяльність Китаю проти американських компаній», – розповідає один із колишніх чільників ФБР, який займався кіберрозслідуваннями. Фахівці ФБР зламали комп'ютери китайських хакерів і вивантажили звідти перелік компаній, якими цікавилися хакери. «Ми знайшли ці компанії і надіслали їм повідомлення: "Ось цей комп'ютер у вашій мережі зламаний китайцями. Ось як ми дізналися про це"».

Кібероперативники ФБР також роздобули адреси електронної

пошти працівників, упольованих китайськими хакерами, які надсилали жертвам на перший погляд звичайні електронні листи, в яких насправді містилося шпигунське ПЗ. «Ми дізнались, які ключові слова та фрази містилися в тих листах, – розповідає колишній співробітник ФБР, – і повідомили компанії, на що саме варто звернути пильну увагу і які електронні листи відкривати не слід. Ми сказали їм: "Ви наступні у списку"».

Найбільше непокоїло те, що в переліках потенційних жертв опинилися співробітники американських нафтогазових компаній. Ці підприємства володіють найбільшими нафтопереробними заводами й трубопроводами, якими управляють за допомогою системи SCADA (система диспетчерського управління та збору даних) – обладнання того ж ґатунку, яке АНБ атакувало на іранських заводах ядерної промисловості, щоб вивести з ладу газові центрифуги. За словами колишнього працівника бюро, китайські спроби проникнути на підприємства нафтогазової галузі «тривали безперервно». Навесні 2012 року ця активність сягнула найвищого піку – хакери зламали комп'ютерні мережі 20 компаній, що володіли трубопроводами для перекачування природного газу або обслуговували їх. ФБР і Міністерство внутрішньої безпеки втрутились у справу й провели секретні наради з керівниками і співробітниками служб безпеки цих підприємств. Вони почали відстежувати активність і переміщення хакерів, намагаючись збагнути, як їм удалося проникнути в мережі і яку шкоду вони можуть заподіяти. Однак доказів того, що хакери здобули доступ до головних систем SCADA, не виявили – можливо, шпигуни розшукували стратегічно важливі документи або інформацію про енергоресурси США. Проте проникнення в мережі почастішали й так занепокоїли Міністерство внутрішньої безпеки, що те оприлюднило спеціальне попередження для енергетичної галузі, описуючи загрози й способи захисту систем.

Колишній держслужбовець розповів, що агенти ФБР також проникали в комп'ютери російських і східноєвропейських кримінальних угруповань, які спеціалізуються на викраденні грошей із банківських рахунків компаній, – ці суми сягають кількох мільярдів доларів на рік. ФБР ідентифікувало потенційних жертв шахраїв, а потім попередило їх про заплановані атаки. Також агенти проникли в комп'ютери хакерської групи Anonymous, знайшли списки осіб, що цікавили хакерів, і попередили цих людей.

Чи можуть такі розвідувальні операції запобігти хакерським атакам? «Я абсолютно чітко бачу перепони для атак», – заявив один колишній держслужбовець. Ідеться про встановлення програмних оновлень, блокування визначених IP-адрес у корпоративних мережах, суворе дотримання основних правил безпеки (наприклад, використання довших або складніших паролів), адже навіть передові компанії частенько ігнорують ці правила. Проте дати кількісну оцінку результативності цих заходів доволі складно. Компанії прагнуть замовчувати окремі ситуації, коли допомога державних структур придалася їм, бо не хочуть визнавати, що їм загрожувала небезпека.

Нинішні і колишні держслужбовці стверджують, що ФБР витрачає чималу частину свого бюджету й часу на відстеження проникнень китайських хакерів у американські комп'ютерні мережі та запобігання атакам на критично важливі об'єкти інфраструктури. Безсумнівно, це дуже важлива місія, але це складно назвати правоохоронною діяльністю, якою, власне, й покликане опікуватися ФБР. Чи варто проводити розслідування, визначає не бюро, а Міністерство юстиції, федеральні прокурори й, зрештою, генеральний прокурор. Однак дотепер Сполучені Штати не довели до суду жодної справи про крадіжку інтелектуальної власності або порушення американських антихакерських законів китайськими кіберзлочинцями.

«Коли йдеться про національну безпеку, американська влада ставить на чільне місце контррозвідку, яка, як сподіваються можновладці, допоможе сформувати принаймні якусь стратегію та перешкодити китайцям робити те, що вони роблять», – каже колишній держслужбовець. Адміністрація Обами вирішила не звертатися до суду, а оприлюднити інформацію про китайських хакерів і натиснути на тамтешній уряд, аби він посилив контроль над ними. Докази, зібрані ФБР і АНБ, допомагають у цьому. (Звісно, китайська влада майже напевно не буде співпрацювати з американцями у розслідуванні кримінальної справи проти одного зі своїх громадян. Китайські очільники навряд чи зізнаються, що їхня країна так зухвало шпигує проти США. Вірогідно, вони звинуватять американських хакерів (не без підстав) у шпигунстві проти Китаю.)

Поки влада шукає дипломатичного розв'язку проблеми шпигунства, отримана ФБР інформація повинна допомогти корпораціям захиститися від майбутніх атак. Так само як АНБ надає інформацію оборонним підприємствам, ФБР передає звіти власникам і опера-

торам критично важливих об'єктів інфраструктури, а також банкам і фінансовим структурам – організаціям, які влада вважає життєво важливими для забезпечення економічної безпеки та нормального повсякденного життя в США.

ФБР не завжди попереджає компанії про проникнення у комп'ютерні мережі. Інколи бюро використовує зламані комп'ютери як пастку, однак ці методи можуть призвести до катастрофи.

На початку грудня 2011 року Джорджу Фрідману, генеральному директорові приватної розвідувальної компанії Stratfor, зателефонував Фред Бартон, перший віце-президент компанії інформаційної розвідки, у минулому фахівець із протидії тероризму в Держдепі. Бартон розповів Фрідману, що сайт компанії зламаний, а інформація про кредитні карти клієнтів, які платили за підписку на різні інформаційні матеріали й звіти компанії щодо міжнародних відносин, украдена. Номери кредитних карт не були зашифровані, тобто компанія не дотримувалася найпростіших заходів безпеки. Згідно зі звітом Фрідмана, наступного ранку він зустрівся з агентом ФБР, «який чітко дав зрозуміти, що ведеться розслідування, і запропонував співпрацю».

ФБР саме проводило операцію проти членів хакерської групи Anonymous, які націлилися на Stratfor, звинувачуючи компанію у тісних зв'язках з американською владою та службами розвідки. (Згодом один хакер звинуватив компанію в «шпигунстві за цілим світом» і за групою Anonymous зокрема.) У компанії Stratfor працювали колишні держслужбовці, однак це приватна установа, яка готує аналітичні звіти й заледве відрізняється від інших консалтинґових фірм, ба навіть інформаційних агентств. Щоденний аналіз світових подій читають держслужбовці, серед яких і співробітники військових і розвідувальних організацій, проте ці звіти призначені не лише для них.

За шість місяців до згаданих подій у Stratfor виявили «крота» – ФБР заарештувало відомого хакера Гектора Ксавьє Монсеґера, який називав себе Сабу, і зробило його своїм інформатором. Монсеґер очолював хакерську групу LulzSec, цілями якої були комп'ютерні системи корпорацій і державних агентств, зокрема й ЦРУ, сайт якого вони якось вивели в офлайн. Представники ФБР згодом розповідатимуть, що Монсеґер допоміг їм атакувати хакерів у Британії, Ірландії і Сполучених Штатах, а отримана від нього інформація допомогла

запобігти атаці хакерів на 300 державних агентств і компаній. Проте Stratfor не була однією з них.

ФБР дізналося про те, що група Anonymous цікавиться Stratfor у грудні 2011 року, коли Джеремі Гаммонд, якого звинувачують в очоленні операції, повідомив Монсеґерові, що він проник у мережу компанії й узявся за дешифрування конфіденційної інформації. Проте замість того, щоб попередити Stratfor, ФБР вирішило влаштувати засідку.

У бюро попросили Монсеґера переконати Гаммонда і його друзів-хакерів у необхідності вивантажити інформацію з мережі Stratfor на інший комп'ютер, який таємно контролювало ФБР. У матеріалах кримінальної справи згадано про те, що хакери завантажили «кілька гігабайт конфіденційних даних», зокрема номери 60 тисяч кредитних карт і особистих даних клієнтів компанії, а також адреси електронної пошти працівників. Протягом цієї двотижневої операції ФБР спостерігало, як хакери викрадають фінансову інформацію підписників і видаляють деякі приватні документи компанії Stratfor. Ба більше, хакери надіслали до WikiLeaks 5 млн електронних листів із внутрішньої мережі листування компанії. (Згодом ФБР виправдовувалося, що не мало можливості зупинити хакерів, бо ті зберігали електронні листи на своїх комп'ютерах.)

ФБР попросило Фрідмана не розповідати про витік інформації і проникнення в комп'ютерну мережу компанії, поки агенти не відстежать всі дії хакерів. Але ближче до вечора 24 грудня Фрідман довідався, що сайт компанії Stratfor знову зламаний. Цього разу хакери розмістили на головній сторінці компанії «радісне повідомлення» про те, що викрали номери кредитних карт і величезну кількість адрес електронної пошти, а також «практично знищили разом із даними і резервними копіями» чотири сервери Stratfor, – написав у своєму звіті Фрідман.

Це був нищівний удар по інфраструктурі компанії. На цих серверах зберігалися зібрані упродовж років звіти й аналітика, яку створювала і продавала своїм підписникам компанія. Це становило підґрунтя бізнесу Stratfor. Електронні листи були конфіденційними, а оприлюднення приватного листування між деякими співробітниками компанії викликало скандал. Як-от, кілька листів Бартона з расистськими висловлюваннями щодо арабів.

Згодом Гаммонд розповідав, що знищення серверів було зви-

чайною практикою. «Спочатку ви підміняєте головну сторінку сайту, потім викачуєте інформацію і, зрештою, знищуєте сервер – просто заради розваги, і вони вже не зможуть відновити систему. Ми не хочемо, щоб вони її відновлювали. І потрібно знищити інформацію, яка допоможе виявити тих, хто це зробив, і те, як саме вони це зробили».

Знищення архівів Stratfor і оприлюднення приватного листування поклало кінець бізнесу компанії та її репутації.

ФБР могло попередити Stratfor про заплановану атаку й у компанії вдалися б до екстрених методів захисту. Бюро могло спробувати зупинити хакерів завчасно. Але його чільники постановили, що важливіше змусити Гаммонда і його колег завантажити інформацію на комп'ютер ФБР, щоб використати її як доказ у кримінальній справі. Компанія Stratfor потрапила під перехресний вогонь під час полювання ФБР на групу Anonymous.

Та сама доля спіткала клієнтів компанії. Протягом декількох днів після зламу хакери оприлюднили номери кредитних карт підписників, з яких, як стало відомо, було вкрадено $700 тисяч. Деякі з цих транзакції, зокрема ті, які проходили як доброчинні пожертви, компанії, що обслуговували кредитні карти, змогли скасувати Але хакери також розкрили електронні адреси підписників, які згодом були використані для атак. Серед підписників Stratfor були колишні офіцери розвідки, науковці, учасники міжнародних проектів і фахівці з корпоративної безпеки. Серед відомих підписників компанії були колишній держсекретар Генрі Кіссінджер, колишній радник із питань національної безпеки Джон Пойндекстер і віце-президент Джеймс Квейл.

За оцінкою Stratfor, хакерська атака завдала компанії $2 млн збитків, якщо зважити на втрату потенційних прибутків і витрати на відновлення системи. Ба більше, компанії довелося задовольнити груповий судовий позов, поданий колишніми підписниками, і це, за оприлюдненою інформацією, коштувало Stratfor не менше $2 млн, адже довелося надати колишнім і поточним клієнтам відшкодування у формі безкоштовної підписки, а також сплатити судові витрати і послуги фінансового аудиту для клієнтів, які вимагали цього.

Історія, яка сталася із Stratfor, показує розмір збитків, які можуть спіткати компанію у разі хакерської атаки під спостереженням ФБР. Звісно, бюро мусить збирати докази злочину, якщо планує заареш-

товувати злочинців. Згодом офіційні особи заявили, що Монсеґер допоміг їм фактично знищити групу LulzSec, відповідальну за низку вторгнень і нищення сайтів. Справді, бюро попередило чимало компаній про небезпеку для їхнього бізнесу. Але операція, пов'язана з атакою на Stratfor, виявила небезпечну та неприємну правду про антихакерську стратегію ФБР. Якщо завдання цієї структури полягає в збиранні інформації, зокрема такої, що стосується китайських і російських хакерських груп, ФБР може допомогти попереджувати атаки й уникнути збитків. Але якщо бюро намагається працювати в традиційному стилі, тобто полює на поганих хлопців і веде їх до суду, жертвами можуть ставати невинні люди.

Монсеґер довів, що він надійний союзник ФБР. У 2013 році Міністерство юстиції вимагало від судді відкласти винесення вироку, оскільки хакер допомагав завершити інші розслідування. «Від першого дня арешту обвинувачуваний активно співпрацював із владою, – писав федеральний обвинувач до судді в Нью-Йорку. – Інколи він цілу ніч спілкувався з іншими хакерами, що допомогло розпочати кримінальне переслідування». Якби Монсеґера засудили на максимальний термін, він провів би залишок свого життя у в'язниці.

Джеремі Гаммонд стверджує, що співпраця Монсеґера з владою сягнула значно далі, ніж наведення агентів на хакерські групи штибу Anonymous. «Багатьом невідомо, що Сабу використовував своїх маріонеток для зламування визначених владою об'єктів, зокрема численних сайтів іноземних держав. Якщо Сполучені Штати не могли діяти згідно із законом, вони використовували Сабу, а також мене й моїх співвідповідачів, для протизаконної діяльності». Гаммонд, якого засудили до десяти років ув'язнення за зламування комп'ютерів компанії Statfor, не міг надати доказів сказаного, а ФБР ніколи не зізналось у тому, що вдавалося до послуг хакерів для проникнення в комп'ютерні системи іноземних держав.

Інколи здається, що держава та компанії, які вона нібито намагається захистити, працюють одне проти одного. Проте, попри деякі розбіжності у методах, у кіберпросторі держава і бізнес стають спільниками. Цей союз народжується завдяки взаємному розумінню, що національна безпека й економічний добробут Сполучених Штатів наражаються на серйозну небезпеку через нестримне кібершпигунство та реальну загрозу кібератак на критично важливі об'єкти інф-

раструктури. Держава вбачає у захисті всіх галузей промисловості кращий спосіб захисту кіберпростору. Але вона не може впоратися з цим завданням власноруч. Приблизно 85 % комп'ютерних мереж у Сполучених Штатах належать приватним структурам і особам, і будь-яка з них може виявитися слабкою ланкою в ланцюзі кібербезпеки. Серед них і великі телекомунікаційні компанії, що контролюють основні мережі інтернету. Це і техногіганти, як-от Google, відповідальні за величезну частину інтернет-трафіку, які вже починають прокладати в деяких американських містах власні кабелі для надання доступу в інтернет і телевізійних послуг. І фінансові організації, через приватні мережі яких щодня здійснюються транзакції на трильйони доларів, а гроші миттєво потрапляють з одного рахунку на інший. І традиційні союзники держави – оборонні підприємства, у мережах яких безліч креслень надсекретної зброї та іншої секретної інформації. Держава оголосила захист кіберпростору найвищим пріоритетом нації. Однак компанії висловлюють власну думку щодо того, як здійснюється цей захист. Союз держави та бізнесу – це підґрунтя розвитку військово-мережевого комплексу, і саме він визначатиме характер кіберпростору й те, як ми працюватимемо та існуватимемо в ньому зараз, у XXI столітті.

ЧАСТИНА II

8
ЩЕ ОДИН «МАНГЕТТЕНСЬКИЙ ПРОЕКТ»

Травень 2007 року
Овальний кабінет

Майку МакКоннеллу вистачило 15 хвилин, щоб переконати Джорджа Буша санкціонувати кібервійну в Іраку. МакКоннелл просив про годинну зустріч із президентом і його головними радниками з питань національної безпеки, вважаючи, що саме стільки часу піде, щоб переконати їх у доцільності такого ризикового кроку. І що йому робити з 45 хвилинами, що залишилися?

– Ще щось? – запитав Буш.

– Ну, насправді, так, – відповів МакКоннелл.

Після повернення на державну службу у лютому МакКоннелл шукав нагоди обговорити з Бушем одну проблему національної безпеки, яка серйозно його непокоїла: Сполучені Штати вразливі до нищівних кібератак національного масштабу. МакКоннелл боявся, що в комунікаційні системи країни можна проникнути, як це було в Іраку, і вивести їх із ладу або знищити. Особливо його непокоїло те, що фінансові компанії не дбають про достатній захист інформації про рахунки, фондові операції та грошові перекази, а також не працюють над запобіганням злочинів, пов'язаних із розкраданням мільярдів доларів з особових і корпоративних банківських рахунків.

Але у небезпеці опинилася й критично важлива інфраструктура. Два місяці тому Міністерство внутрішньої безпеки звернулося до Національної лабораторії Айдахо, яка проводить дослідження в галузях ядерної промисловості та енергетики для федеральної влади, з проханням перевірити, чи зможуть хакери отримати віддалений доступ до електростанції і розкрутити генератор до таких обертів, щоб він став некерованим. Результати експерименту лякають. На відеозаписі, який просочився у пресу, можна побачити велетенський зелений генератор, що трясся наче під час землетрусу, аж поки із нього не вирвалася пара й чорний дим. Ефект здавався майже анімаційним,

проте був абсолютно реальним, а експеримент виявив критично слабке місце в самому серці американських електромереж. Офіційні особи боялися, що хакери можуть вивести з ладу енергетичне обладнання і це призведе до аварійного вимкнення струму, яке триватиме тижні або й місяці, аж поки обладнання не замінять.

Кіберзагроза вже не була гіпотетичною. Міністерство оборони мусило відреагувати на вторгнення в комп'ютерні мережі підрядників. Окрім креслень і секретних розробок систем озброєння, які хакери викрали або збиралися викрасти, були: креслення Єдиного ударного винищувача, гвинтокрила Black Hawk і безпілотного літального апарата віддаленого стеження Global Hawk; інформація про відеосистеми й канали передавання даних безпілотників; креслення ракетної системи Patriot, реактивних двигунів компанії General Electric і протиракетної системи Aegis; інформація про методи аналізу розвідданих; креслення сонара для підводного картографування і бойового корабля ВМС прибережної зони; схеми легких торпед; креслення бойових машин Корпусу морської піхоти; інформація про плани екіпірування армії новітніми приладами для ведення спостереження і розвідки; креслення вантажного літака C-17 Globemaster, а також інформація про армійську глобальну систему управління вантажоперевезеннями; системні креслення літака-розвідника RC-135; опис технології перехоплення радіосигналів і схеми радіоантен, використовуваних військово-морськими силами. Кожен підрозділ американських збройних сил опинився під прицілом, так само як технології та озброєння, які Сполучені Штати використовували для війни у кожному вимірі – на землі, на воді, у повітрі та в космосі.

Але як переконати Буша у необхідності негайних дій? МакКоннеллові було відомо, що президент не знався на техніці. Якось він сказав, що користується «ґуґлом» украй рідко, здебільшого, щоб поглянути на супутникові знімки свого ранчо в Техасі. Було б складно пояснити йому технічними термінами, як хтось, сидячи за клавіатурою за тисячі кілометрів од США, може вчинити хаос за допомогою пристрою, майже незнайомого президентові. Тому МакКоннелл звернувся до теми, яка володіла увагою Буша впродовж практично всього терміну його президентства, – до тероризму.

МакКоннелл запропонував Бушу уявити такий гіпотетичний сценарій: що сталося б, якби терористи «Аль-Каїди» не захоплювали комерційні авіалайнери й не скеровували їх у будівлі 11 вересня

2011 року, а натомість зламали бази даних провідних фінансових організацій і знищили їх, стерши на порох світову фінансову систему? Не можна було б проводити транзакції. Не можна було б здійснювати торгові операції. Через комп'ютерні мережі світу щодня перекачуються трильйони доларів. Ці «гроші» насправді просто інформація. Баланси рахунків. Розподілені мережі електронних бухгалтерських книг, які зберігають інформацію про те, хто і що купив чи продав, хто, кому і куди переказав гроші. Варто лише пошкодити частину цієї інформації або знищити її, і масова паніка неминуча, доводив МакКоннелл. Економіки країн можуть упасти лише через брак довіри, а що вже казати про те, що банки й фінансові організації навряд чи зможуть відновити втрачені дані.

Здавалося, Буш не повірив. Як злодій, озброєний лише комп'ютером, зможе проникнути у святилище американської фінансової системи? Хіба ж ці компанії не вдаються до запобіжних заходів, щоб захистити свої цінні активи? Чи є інші вразливі місця? Буш хотів знати про них. Чи загрожує небезпека Білому дому? Буш показав на телефон захищеної лінії зв'язку на своєму робочому столі, яким користувався для спілкування з членами кабінету міністрів і іноземними керівниками.

– Чи може хтось прослуховувати? – запитав Буш.

В Овальному кабінеті запанувала тиша. Радники президента з питань національної безпеки нервово перезиралися. МакКоннелл зрозумів, що президентові досі ніколи не розповідали, яким заслабким був електронний захист органів влади, та й держави загалом.

– Пане президенте, – сказав МакКоннелл, – якщо можливість зламати пристрій зв'язку існує, ми повинні вважати, що наші вороги неодмінно спробують нею скористатися.

А після цього МакКоннелл перелічив Бушу всі способи, за допомогою яких США можуть використати телекомунікаційну систему Іраку. Президент почав усвідомлювати: те, що він може зробити з іншими, інші можуть зробити з ним.

Повертаючись до гіпотетичної кібератаки на фінансову систему, МакКоннелл навів іще одне порівняння з тероризмом:

– Економічні наслідки такої атаки будуть значно гіршими, ніж від атак 11 вересня, – запевнив МакКоннелл Буша, який знав про те, що удар по вежах-близнюках посилив економічний спад США.

Буш здавався приголомшеним. Він повернувся до міністра фінансів Генрі Полсона, який раніше обіймав посаду генерального директора інвестиційного банку Goldman Sachs:

– Генку, те, що говорить Майк, – це правда?

Полсон відповів:

– Навіть більше, пане президенте, і коли я працював на Goldman, цей сценарій не давав мені спати ночами.

Буш підвівся.

– Інтернет – наша конкурентна перевага, – звернувся він до своїх радників і членів кабінету міністрів. – Ми повинні зробити все необхідне, щоб захистити його. Якщо доведеться, ми запустимо новий мангеттенський проект, – сказав президент, натякаючи на секретну програму зі створення першої атомної бомби за часів Другої світової війни.

МакКоннелл ніколи не сподівався на таку сильну реакцію. Він понад десять років очікував, аж поки президент – якийсь із президентів – встромить спис у небезпеки, які, на його думку, лежали просто на поверхні повсякденного життя.

Буш звернувся до МакКоннелла:

– Майку, ти окреслив проблему. У тебе є тридцять днів на її вирішення.

Ніхто не зміг би «вирішити» цю проблему за 30 днів, якщо її взагалі можна розв'язати. Але президент Буш лише попросив розробити комплексний план посилення державного кіберзахисту, поклавши початок вирішенню одного з найважливіших технічних завдань в американській історії. МакКоннелл побачив рідкісну можливість і вхопився за неї. Проте він не міг упоратися самостійно. Тому начальник шпигунів звернувся до джерела технічної майстерності, яке знав найкраще.

Від самого початку державний план кіберзахисту розробляло АНБ. До цього плану ставились як до військової та розвідувальної програми, тому тримали його у суворій таємниці. Він був офіційно засекречений президентським наказом, який Буш підписав у січні 2008 року. Адміністрація планувала витратити $40 млрд на реалізацію програми протягом перших п'яти років – величезна сума для одного напряму. Не лише МакКоннелл, а й Кіт Александер очікував миті, коли президент покладе весь свій авторитет і вплив на підтрим-

ку державних зусиль із протидії невидимим ворогам, які, на думку Александера, становили справжню загрозу для Сполучених Штатів. Александер також вважав, що зловмисні хакери, які, вірогідно, працюють на ворожі держави або терористичні угруповання, врешті-решт оберуть за мішень фінансові організації на Волл-стріт, електромережі та інші критично важливі об'єкти інфраструктури.

На першому етапі державного контрнаступу потрібно було скоротити кількість потенційних цілей. Міністерство оборони обмежило виходи до загальнодоступного інтернету до 18 шлюзів. Це був надзвичайний захід, зважаючи на те, що вільний інтернет-доступ був у кожному віддаленому кутку перебування збройних сил, аж до більшості штаб-квартир у зонах бойових дій. (Ось чому технологія вистеження повстанців у Іраку працювала так бездоганно.) Міністерство оборони впоралось із завданням краще, ніж будь-яке інше державне відомство, запобігши вторгненням у власні мережі, хоча ворогам інколи таки вдавалося проникнути всередину. У червні 2007 року хакери зламали відкриту систему електронної пошти, якою користувалися міністр оборони Роберт Ґейтс і сотні інших офіційних осіб. Цей випадок став важливим нагадуванням про те, що на часі підняти віртуальні розвідні мости, суворо обмеживши доступ у зовнішній світ.

Водночас АНБ почало пильно моніторити шлюзи у пошуках ознак зловмисної діяльності. Цю активну складову комп'ютерної оборони високопосадовець із Пентаґону згодом опише як «почасти наглядову, почасти сторожову і почасти снайперську». Якщо хакери або їхні ботнети намагалися вдертися до мереж Міністерства оборони, військові могли заблокувати інтернет-адресу для запобігання шкідливого трафіку, а потому попередити військові та розвідувальні організації, щоб ті простежили за трафіком з атакованого вузла. Ідея полягала в тому, щоб забезпечити кращий захист мереж Міністерства оборони, використовуючи напрацьовані АНБ методи збору інформації, а також створити щось подібне до системи миттєвого попередження компаній, спостерігаючи за будь-яким шкідливим ПЗ у мережах іще до початку атаки на важливі промислові об'єкти. Першими в списку одержувачів попереджень були енергетичні та фінансові компанії.

Проте всі ці заходи не можна було вважати повноцінним планом захисту держави. Намагання відстежити в інтернеті шкідливе ПЗ через нечисленні точки доступу – це те саме, що шукати муху на стіні, дивлячись через соломинку. (Немає жодних доказів того, що завдяки

згаданій стратегії спостереження за власними мережами АНБ бодай раз запобігло масштабній кібератаці.) Александер заявив, що для ґрунтовного захисту країни АНБ потрібно прокласти більше стежок у мережах американських компаній. Деякі з них АНБ уторувало завдяки секретній контррозвідувальній операції під назвою «Візантійська опора» (Operation Byzantine Foothold), у рамцях якої хакери АНБ вистежували китайських та інших іноземних шпигунів, що проникли в мережі військових підрядників. АНБ намагалося визначити джерело поширення фішинґових електронних листів, що містили шкідливе ПЗ. Зібрана по нитці інформація про методи хакерів допомогла посилити кіберзахист компаній. Проте лише кілька підприємств погодилися співпрацювати з Пентаґоном – ділитися інформацією з власних мереж і дозволяти АНБ зиркнути бодай одним оком усередину. Александер хотів, аби влада розширила програму, охопивши компанії за межами воєнно-промислового комплексу. Але на це були потрібні час і певна політична воля, яких Буш наприкінці президентського терміну вже не мав. Натомість МакКоннелл вважав: якщо стане відомо про керівну роль АНБ у забезпеченні внутрішньої кібербезпеки, це призведе до політичної катастрофи. Не минуло й двох років після публікації в New York Times гучної статті, присвяченої програмі АНБ із незаконного прослуховування телефонів і перегляду електронної пошти всередині країни. Участь агентства в кіберзахисній програмі означала розширення такої діяльності, а також поєднання функцій збору розвідувальної інформації і кіберборотьби – аж до відсічі хакерам. Деякі члени Конгресу хотіли обмежити розвідувальну діяльність АНБ, яка стала невід'ємною частиною його кіберзахисної місії. МакКоннелл вважав, що агентству наразі потрібно стишитись і зосередитися на менш сумнівних методах кіберзахисту, спостерігаючи за державними мережами і мережами оборонних підрядників.

Відтак МакКоннелл почав працювати у цивільному полі. Міністерство внутрішньої безпеки, яке мало законні повноваження для забезпечення безпеки домену .gov, що ним користувалася більшість державних установ (за винятком військових і розвідувальних структур), наглядало за виконанням ініціативи зі скорочення кількості інтернет-шлюзів у невійськових державних структурах: із понад 1000 до 50. Це завдання виявилося масштабнішим і розпливчастішим, ніж у Міністерства оборони, позаяк ці цивільні мережі не мали централізованого управління і їх було значно більше. Реалізація проекту

потребувала більше часу, ніж залишалося до кінця президентського терміну Буша, а отже, МакКоннеллу теж бракувало часу.

Натомість Александера терміни не обмежували. Він обійняв посаду лише 2005 року, і хоча традиційний термін на цій посаді не перевищує чотирьох-п'яти років, майбутній президент чи міністр оборони завиграшки міг його продовжити. Справді, попередник Александера пропрацював на цій посаді шість років – довше за всіх керівників у 56-річній історії агентства. Що помітнішою ставала участь АНБ у розвідувальних операціях, зокрема в антитерористичних, то впливовішим ставав директор агентства і то складніше було його замінити. Александер розумів, що панівне становище агентства в розвідувальній ієрархії надалі залежатиме від зміцнення лідерських позицій АНБ у забезпеченні кіберзахисту та веденні кібервійни. Це було наступне масштабне завдання, яке уряд проголосив одним із пріоритетів державної безпеки. За побіжними оцінками, час протидії тероризмові минув, а кібербезпеки – настав. Александерові потрібно було лише дочекатися моменту, коли більшість лідерів країни це збагне й звернеться до нього за допомогою. Йому потрібна була криза.

9
«АМЕРИКАНСЬКА КАРТЕЧ»

П'ятниця 24 жовтня 2008 року стала несподівано метушливим днем у штаб-квартирі АНБ. Того дня президент Буш приїхав до Форт-Міда, щоб зустрітися з керівниками агентства, і це був його останній запланований візит перед складанням президентських повноважень у січні наступного року. У 16:30, коли більшість співробітників АНБ уже збиралася вирушати додому на вихідні, високопосадовець Річард Шаффер, що відповідав за комп'ютерну безпеку, увійшов до кабінету Кіта Александера з терміновим повідомленням.

Молодий аналітик однієї з «мисливських» команд АНБ, що стежили за зловмисними вторгненнями, виявив у військовій комп'ютерній мережі шкідливу програму. Це був маячок, який надсилав сигнали розташованому невідь-де головному комп'ютерові, запитуючи інструкції для дій – можливо, скопіювати файли або стерти всі дані. Ця ситуація сама по собі не була аж надто тривожною. Однак сигнали виходили із секретної мережі, яку використовувало Центральне командування США, що вело війни в Іраку й Афганістані. Усі вважали, що проникнення в цю мережу неможливе, позаяк вона не під'єднана до інтернету.

У жодну секретну ізольовану мережу досі ніхто не проникав. Такі мережі не під'єднували до глобальної мережі інтернет, позаяк через них проходили важливі надсекретні військові повідомлення, зокрема плани воєнних дій і накази підрозділам на полі бойових дій. Протягом кількох наступних днів аналітики працювали не покладаючи рук – намагалися визначити, як саме шкідлива програма потрапила до мережі, припускаючи, що, найімовірніше, вона проникла всередину випадково, із зараженого USB-носія, яким скористався якийсь солдат в Афганістані. Саме там спостерігалася найбільша кількість заражень комп'ютерів. І це становило ще одну проблему – програма була заразливою і швидко поширювалася, самовідтворюючись і проникаючи в інші комп'ютери мережі через USB-носії. Аналогічне ПЗ виявили також у двох інших секретних мережах.

Керівники АНБ запідозрили роботу ворожої розвідки, яка намагалася викрасти секретну військову інформацію. Аналітики вважали, що заражений USB-носій могли підкинути, приміром, на автостоянці, де він чекав на якусь довірливу людину – такого собі «пацієнта нуль», – яка би підібрала знахідку й вставила у захищений комп'ютер Центрального командування або на військовій базі. Шкідлива програма не могла під'єднатися до інтернету, щоб отримати інструкцію. Проте шпигун міг керувати нею, перебуваючи на відстані кількох кілометрів від зараженого комп'ютера, за допомогою радіосигналу – АНБ також використовувало подібне обладнання, інсталюючи шпигунське ПЗ у локальні мережі. Існували ознаки того, що «хробак» проникав також у несекретні системи, які мали з'єднання із зовнішнім світом, і міг стати для іноземних шпигунів точкою входу в мережі Пентаґону.

Це проникнення було безпрецедентним в історії військових і розвідувальних служб. Александер вирішив, що час оголошувати тривогу.

Генерал ВПС Майкл Басла працював у Пентаґоні в п'ятницю ввечері, коли надійшов тривожний дзвінок із Форт-Міда. Басла обіймав тоді посаду заступника директора Об'єднаного комітету з питань командування, контролю, зв'язку і комп'ютерних систем. Він миттєво збагнув небезпеку, про яку повідомили керівники АНБ. «Так багато слів, – згадував Басла згодом, – щоб повідомити: "Г'юстон, у нас проблема"»*.

Колесо державної військової машини почало обертатися. Тієї ночі Басла разом із керівниками АНБ провів нараду з адміралом Майклом Малленом – головою Об'єднаного комітету і старшим військовим радником президента Буша. Агентство проінформувало заступника міністра оборони Ґордона Інґленда, який разом із лідерами Конгресу брав діяльну участь у впровадженні «Ініціативи оборонної промисловості».

---

* Це фраза, яку вимовив командир американського космічного корабля «Аполлон-13» Джеймс Ловелл під час експедиції на Місяць у 1970 році, повідомляючи космічний центр у Г'юстоні про вибух кисневого балону і виведення з ладу двох із трьох батарей паливних елементів. Фраза стала популярною після виходу фільму «Аполлон-13» у 1974 році.

Ніхто не знав напевно, коли саме шкідливе ПЗ спробує виконати свою місію, хоч би у чому вона полягала. Проте члени пошукової групи АНБ, які виявили «хробака», вважали, що знають спосіб його нейтралізації. «Хробак» надсилав запит головному серверові, вимагаючи інструкцій. Чом би не дати «хробакові» те, чого він хоче? Фахівці пошукової групи хотіли підмінити сервер управління, зв'язатися з «хробаком» і наказати йому перейти в режим сну і не робити наступних кроків. Цей план не був цілком безпечним. Якщо група порушить або зупинить роботу важливих мережевих програм, як-от секретного зв'язку між командирами на полі бою, це може зашкодити військовим операціям в Афганістані та Іраку. Секретна мережа повинна працювати без перешкод.

Однак Пентаґон погодився на план АНБ, якому дали кодову назву «Американська картеч» (Backshot Yankee). Фахівці пошукової групи провели ніч із п'ятниці на суботу за детальною розробкою плану, поглинаючи содову, щоб не заснути, і вгризаючись у піцу. В суботу зранку вони поставили сервер у вантажівку й вирушили в розташоване неподалік Агентство оборонних інформаційних систем, яке керувало глобальними телекомунікаційними системами Міністерства оборони. Сервер заразили шкідливим ПЗ, а потому активували комп'ютера-самозванця, який скомандував «хробакові» вимкнутися. План подіяв.

Тепер в АНБ з'явився спосіб деактивації «хробака». Проте спочатку потрібно було його знайти – причому геть усі копії, що розповзлися мережами Міністерства оборони. АНБ згуртувало своїх кращих хакерів з елітного Відділу особливого доступу, які почали шукати заражені «хробаком» військові комп'ютери. А відтак пішли далі і почали відстежувати його сліди у цивільних комп'ютерах, зокрема у тих, які працювали в урядових мережах США та інших країн. З'ясувалося, що «хробак» розповзся дуже широко.

Нічого дивного у цьому не було. Виявилося, що «хробак» не був надто новим. Уперше його виявили фінські фахівці з інформаційної безпеки у червні 2008 року, коли він проникнув у комп'ютер військових організацій країн – членів НАТО. «Хробака» назвали Agent.btz. Слово «agent» (агент) – загальна назва всіх виявлених зразків шкідливого ПЗ, а суфікс «btz» – це внутрішній маркер виду. Не було жодних доказів того, що зараження «хробаком» Agent.btz призвело до викрадання або знищення даних на американських комп'ютерах. Насправді

«хробак» був не надто складним, отож повставало запитання: навіщо іноземна розвідка витрачала зусилля на створення «хробака», який ховався в комп'ютерах усього світу і нічого не крав?

Проте військові керівники надалі боялися проникнень у мережі, вважаючи їх страшною загрозою державній безпеці. Тиждень потому, як АНБ попередило Пентаґон, Маллена запросили на нараду з президентом Бушем і міністром оборони Гейтсом. АНБ узяло на себе завдання із виявлення кожного зараженого Agent.btz комп'ютера та знешкодження цього «хробака» за допомогою підміненого сервера. У листопаді Стратегічне командування США, яке тоді відповідало за ведення кібервоєн, видало декрет: заборонити використання зовнішніх накопичувачів на комп'ютерах Міністерства оборони й усіх військових комп'ютерів. Така реакція була надмірною, але це свідчило про ступінь переляку й тривоги вищого військового керівництва.

Александер тривожився не так сильно. У цій паніці він убачав можливість зробити АНБ новим військовим лідером у кіберпросторі. Адже саме його пошукова група виявила «хробака», доводив він. Саме його експерти придумали, як його спритно вбити. Саме його елітні хакери, використовуючи свої шпигунські навички, вистежили «хробака» у схованках. Представники Пентаґону розмірковували: розпочати атаку й знищити «хробака» чи хитрістю змусити його виконувати команди підміненого сервера. (Процес очищення комп'ютерів тривав аж 14 місяців.)

У той час відповідальність за координацію воєнного удару – справжньої кібервійни – покладалася головно на Об'єднане командування функціональними частинами для ведення мережевої війни (Joint Functional Component Command for Network Warfare), підпорядковане Стратегічному командуванню. Проте цей підрозділ був нечисленним, якщо порівнювати його з АНБ, і не мав такого досвіду в інформаційному захисті та шпигунстві, який мало агентство. Влада вирішила, що нищівний удар по комп'ютерних системах, зокрема розташованих в інших країнах, був надто серйозним кроком у протидії «хробакові» Agent.btz, який, урешті-решт, не заподіяв жодної шкоди. Але операція «Американська картеч» показала, що у разі реальної загрози державі – кібератаки на електромережі або на банк – військовим доведеться згуртувати всіх найкращих снайперів під одним дахом.

«Було зрозуміло, що потрібно об'єднати всі наступальні та оборонні ресурси», – заявив Александер, виступаючи перед комітетом Конгресу в 2010 році, після розсекречення Пентаґоном деяких подробиць проведеної операції. Саме цього він завжди і хотів.

Операція «Американська картеч» стала каталізатором створення Кібернетичного командування США, – єдиного органу, який керував би всіма військовими операціями, покликаними захищати від віртуальних атак, а також ініціювати власні атаки. Цю ідею підтримував директор національної розвідки Майк МакКоннелл, а згодом схвалив і Боб Ґейтс. Вище військове керівництво збагнуло, що їм завдали удару нижче спини і що багато хто з них переоцінював власні можливості швидкого реагування на втручання у пентаґонівські комп'ютери. «Наші очі розплющилися», – зазнався Басла.

Кмітливість Александера та його команди кібервоїнів переконала пентаґонівську братію, Ґейтса і Білий дім, що саме АНБ спроможне й ладне очолити кібервійсько і повинно перебрати провідну роль. Александер керуватиме новим Кіберкомандуванням із Форт-Міда. Він отримає додатковий штат і фінансування. Але воїни та інфраструктура надаватимуться з АНБ.

Агентство надалі працювало над винищенням шкідливого «хробака» Agent.btz. Цей процес тривав понад рік, і агентство скористалося цим часом для розширення сфери впливу. Щойно з'являвся якийсь новий вірус, АНБ закривало всю інформацію про нього, залишаючи доступ лише тим, «кому потрібно» знати, що сталося. Кожен випадок ставав секретним проектом у рамцях масштабнішої операції. За словами колишнього інформаційного аналітика з Міністерства оборони, який мав доступ до інформації про «Американську картеч», така поведінка АНБ ускладнювала життя іншим агентствам, заважала їм реагувати на виявлені прогалини в захисті та збирати інформацію про те, що сталося, – саме цього, очевидно, прагнув Александер. Завіса таємниці покривала майже всі аспекти нової кібермісії АНБ. Колишній аналітик Міністерства оборони описує реакцію АНБ на операцію «Американська картеч» як «захоплення влади».

Потребу в секретності можна було б зрозуміти, якби «хробак» Agent.btz був частиною розвідувальної програми Росії, Китаю або іншої держави. Проте представники Пентаґону ніколи не заявляли, що втручання в мережу спричинило витік секретної або будь-якої

іншої життєво важливої інформації. Ніхто не з'ясував, чи заражений носій інформації, що став, на думку аналітиків, переносником інфекції, спеціально підкинули біля будівлі військового відомства або якийсь безтурботний військовослужбовець чи цивільний співробітник «підчепив» «хробака» Agent.btz за межами військової мережі, можливо, увійшовши до неї в інтернет-кафе з власного ноутбука, а потому мимохіть випустив шкідливу програму зі зовнішнього світу у внутрішню мережу. Цілком імовірно, що «пацієнт нуль» просто випадково підчепив «хробака» і іноземна держава тут ні до чого. Адже Agent.btz виявився різновидом практично нешкідливого «хробака» трилітньої давнини. Деякі офіційні особи, що працювали над операцією «Американська картеч», сумнівалися в причетності іноземних шпигунів. Адже якби шпигуни збиралися проникнути у святилище військового кіберпростору, то, мабуть, діяли б хитріше і бодай щось украли б. А, можливо, шпигуни просто зондували американську систему захисту й спостерігали за реакцією американців на вторгнення, щоб зрозуміти, як влаштована система безпеки.

Якби законодавці та чиновники з адміністрації Буша збагнули, що «хробак» Agent.btz був порівняно нешкідливим, вони б двічі подумали, перш ніж надавати АНБ такі широкі повноваження з управління кіберзахистом і кібератаками. Можливо, Александер і його підлеглі були зацікавлені в засекреченні подробиць вторгнення, щоб отримати важелі впливу й просунути АНБ на очолення Кіберкомандування. Це припущення вірогідне, якщо зважити на спроби Александера залякати державних службовців кіберзагрозами, а відтак переконати їх, що саме він і є та людина, яка «переможе чудовисько». «Александер, наче чарівник із країни Оз, створив ауру неймовірних можливостей, захованих за завісою у Форт-Міді, – каже колишній працівник адміністрації Обами, який тісно співпрацював із генералом у питаннях кібербезпеки. – Він використовував секретність, щоб упевнитися, що ніхто не зазирне за завісу».

Секретність була – і надалі залишається – потужним джерелом влади АНБ. Але агентство черпало силу також із параної, яка пустила паростки у душах чільників Міністерства оборони після операції «Американська картеч». Аби захиститися від потенційних вірусів, керівництво військових відомств заборонило використання зовнішніх носіїв у Міністерстві та всіх підрозділах збройних сил декретом, який викликав обурення військовослужбовців на полях бойових дій,

позаяк портативні носії інформації використовували для перенесення документів і карт з одного комп'ютера на інший. Заборона протрималася кілька років після закінчення операції «Американська картеч». «Якщо ви дістанете USB-накопичувач і вставите його в мій комп'ютер, за кілька хвилин у двері постукають і комп'ютер конфіскують», – розповів Марк Мейбері, старший науковий співробітник ВПС США, під час інтерв'ю у його пентаґонському кабінеті 2012 року. На представників адміністрації Буша накотила хвиля страху перед кіберзагрозами. Вона накрила їх із головою і вихлюпнулася на наступного президента.

10
«СЕКРЕТНИЙ СКЛАДНИК»

Щойно Барак Обама переступив поріг Білого дому, його почали бомбардувати поганими новинами щодо стану державного кіберзахисту. Він провів секретну нараду з Майком МакКоннеллом у Чикаґо, і директор розвідки розповів йому оновлену версію страшної історії, викладеної 2007 року Бушу. Під час передвиборної кампанії китайські шпигуни зламали електронні поштові скриньки членів виборчого штабу Обами і його конкурента, сенатора Джона МакКейна. Тепер, коли 44-й президент США посів своє місце в Овальному кабінеті, Центр стратегічних і міжнародних досліджень – шанований аналітичний центр у Вашинґтоні – оприлюднив докладний і песимістичний звіт про кібернебезпеки для США. Його автори провели щонайменше 16 зустрічей за зачиненими дверима із вищими військовими та державними керівниками й описали декілька розсекречених утручань у мережі так, що волосся ставало дибки. Серед іншого там були описи зламування електронної пошти міністра оборони Роберта Ґейтса; зараження комп'ютерів Міністерства торгівлі шпигунською програмою, яку, на думку кількох незалежних експертів, китайські хакери встановили на ноутбук міністра торгівлі Карлоса Ґутьєрреса під час його офіційного візиту до Пекіна; проникнення в комп'ютерні мережі Держдепартаменту, після яких зникли «терабайти» інформації. За словами одного з укладачів звіту, ці та інші проникнення в мережу, згадані у документі, становили лише 10 % від загальної кількості виявлених зовнішніх утручань у системи. Решта випадків були надто серйозними, або ж надто тривожними для публічного обговорення.

Учасники наради, серед яких були високопосадовці АНБ, керівники деяких найбільших технологічних і оборонних підприємств країни, члени Конгресу й експерти в сфері кібербезпеки, що продовжували працювати в новій адміністрації, схвалили ініціативу «нового мангеттенського проекту», розпочатого Бушем. Проте вони визнали, що великого поступу не було. Адміністрація Обами мусила врахувати

попередні досягнення й, спираючись на них, сформулювати нові вимоги до деяких галузей промисловості та критично важливих об'єктів інфраструктури задля посилення й підтримки їхньої кібербезпеки. «Це стратегічне питання одного рівня з проблемами зброї масового знищення та глобальним тероризмом, за розв'язок яких відповідає федеральний уряд, – писали учасники наради. – Нездатність Америки захистити кіберпростір – це одна з найневідкладніших проблем національної безпеки, що стоять перед новою адміністрацією… Це битва, в якій ми програємо».

Іноземні шпигуни невтомно намагалися дістати доступ до засобів комунікації, промов і політичних заяв найвпливовіших членів нової президентської адміністрації. У перший рік президентства Обами китайські хакери розпочали кампанію, скеровану проти службовців Держдепу, зокрема й проти держсекретаря Гілларі Клінтон. Хакери розіграли надзвичайно майстерний сценарій: п'ятеро співробітників Держдепартаменту, які вели перемовини щодо зниження викиду парникових газів із китайськими урядовцями, отримали фішинґові електронні листи нібито від знаменитого вашинґтонського журналіста Брюса Стокса. Останнього в Держдепартаменті знали добре, адже він писав про проблеми міжнародної торгівлі та кліматичні зміни. Ба більше, він був чоловіком посла Венді Шерман, яка свого часу працювала старшим політичним радником Білла Клінтона з питань Північної Кореї, а згодом обіймала третю за важливістю державну посаду й вела переговори з Іраном щодо згортання ядерної програми у 2013 році. Тодд Стерн, дипломатичний представник США у Китаї, що опікувався питаннями зміни клімату, доводився Стоксу давнім другом. У темі електронного листа було зазначено «Китай і кліматичні зміни», тож здавалося, що це звичайний лист із запитаннями від журналіста. А в самому повідомленні містилися коментарі щодо роботи одержувачів листа та їхніх поточних справ. Хоч би ким був відправник повідомлення, він знав Стокса і його друзів настільки добре, що міг скласти лист у його стилі. Досі невідомо, чи відкрив хтось із одержувачів повідомлення, що містило вірус, здатний вивантажувати документи зі службових комп'ютерів і відстежувати електронні комунікації їхніх власників.

У 2009 році один із підлеглих Гілларі Клінтон одержав листа нібито від колеги із сусіднього кабінету. У листі було вкладення, яке, за словами відправника, стосувалося нещодавньої наради. Одержувач не

міг пригадати нараду й не був упевнений, що вона взагалі відбувалася. Тому він пішов до сусіднього кабінету, щоб розпитати співробітника про щойно отриманий електронний лист.

– Який лист? – запитав колега.

Завдяки обачності молодого співробітника Державний департамент перешкодив встановленню програми для стеження на комп'ютерах в офісі Гілларі Клінтон. Ця історія стала черговим нагадуванням про те, якими майстерними стали шпигуни, і доказом того, що вони вибудовують схему взаємин членів адміністрації, імена яких украй рідко згадують у пресі. Китайські шпигуни вдосконалили цю техніку в наступні роки і донині користуються нею. Чарлі Крум, відставний генерал ВПС, який колись керував Агентством оборонних інформаційних систем, а нині обіймає посаду віце-президента з питань кібербезпеки в компанії Lockheed Martin, каже, що кібершпигуни ретельно вивчають сайт компанії, шукаючи у прес-релізах імена співробітників, занотовуючи публічні появи керівників та інші інформаційні крихти, які можуть допомогти проробити всі деталі підходу до потенційної мети атаки. Відтоді, як шпигунам доводилося порпатись у смітниках біля приватних будинків чи стежити за людьми на вулицях, аби роздобути такі подробиці, минули роки.

Перед обличчям загрози американській безпеці й іноземних шпигунських атак, спрямованих проти його власної команди, Обама вже на початках президентства дав зрозуміти, що має намір зробити кібербезпеку одним із найвищих пріоритетів держави. У промові, виголошеній у травні 2009 року в Східному залі Білого дому, він зазначив: «Ми знаємо, що кіберзлочинці зондують наші електромережі і що в інших країнах кібератаки занурювали в темряву цілі міста». Обама не сказав, де саме це сталося, проте розвідники та військові виснували, що йшлося про два аварійних знеструмлення в Бразилії, у 2005-му й 2007 році, влаштованих хакерами, що отримали доступ до систем контролю електромереж SCADA.

До виступу Обами офіційні особи США здебільшого лише натякали на проникнення в електромережі та рідко погоджувалися, щоб їхні імена згадували. Власники й оператори електромереж спростовували чутки про спричинені хакерами знеструмлення, зокрема й кілька таких випадків у США, відкидаючи подібні припущення як безглузді спекуляції, і цитували результати офіційних розслідувань, в яких аварії зазвичай пояснювали природними явищами, як-от па-

діння дерева на дроти або їхнє забруднення. Але тепер президент визнавав уразливість американських електромереж і те, що нічні жахіття про знеструмлення хакерами цілих міст уже стали реальністю в інших країнах.

«Моя адміністрація впровадить новий ефективний підхід до захисту американської цифрової інфраструктури, – проголосив Обама. – Цей новий підхід починається згори, з моєї особистої відповідальності: віднині ми ставимося до нашої цифрової інфраструктури – мереж і комп'ютерів, від яких ми щодня залежимо, – так, як це повинно бути, як до нашого стратегічного державного активу. Захист цієї інфраструктури стане пріоритетом державної безпеки. Ми повинні впевнитися, що ці мережі безпечні, надійні та безвідмовні. Ми виявлятимемо, запобігатимемо й стримуватимемо атаки проти об'єктів цієї інфраструктури та швидко відновлюватимемо їх після будь-якого пошкодження або знищення».

Захист кіберпростору, заявив Обама, перетворився на державне завдання.

Кіт Александер погоджувався з президентом. Як на нього, залишалося вирішити одне-єдине питання: хто саме в уряді візьметься за таке гераклове завдання?

Після призначення на посаду директора АНБ у 2005 році Александер відвідав штаб-квартиру Міністерства внутрішньої безпеки, розташовану в респектабельному передмісті Вашинґтона, у комплексі Cathedral Heights, де криптографи військово-морських сил США допомогли зламати шифр «Енігма», використовуваний нацистами під час Другої світової війни. Він привіз із собою згорнутий аркуш паперу, щоб передати його Майклові Чертоффу, колишньому федеральному прокуророві та судді, якого нещодавно призначили новим міністром внутрішньої безпеки. Згідно із законом, міністерство повинне координувати політику кібербезпеки на рівні уряду, захищати комп'ютерні мережі цивільних державних служб і співпрацювати з компаніями заради захисту критично важливих об'єктів інфраструктури. Це була величезна й нечітко визначена зона відповідальності та лише одне з безлічі завдань, доручених міністерству, створеному тільки два роки тому, яке також наглядало за патрулюванням кордонів США, перевіркою авіапасажирів і вантажів, удосконаленням не-

ефективної державної імміграційної системи, а також запобіганням новим несподіваним терористичним атакам на США.

У захищеному від прослуховування кабінеті Александер розгорнув на столі для проведення конференцій аркуш паперу. Це була велетенська діаграма, що демонструвала всю зловмисну діяльність в інтернеті, про яку вже знало АНБ. Наміри Александера можна трактувати по-різному. Можливо, він прийшов, щоб допомогти молодому міністерству впоратися зі своєю місією із забезпечення кібербезпеки. Або ж натякав, що Міністерство внутрішньої безпеки не впорається без АНБ, тому краще йому відійти вбік і дозволити фахівцям робити свою справу. Правда полягала у тому, що Міністерство внутрішньої безпеки було не в змозі скласти таку діаграму, яку щойно показав Александер. Щоб працювати на рівні АНБ, міністерству бракувало досвідченого персоналу, величезного бюджету, системи глобального стеження, а також бюрократичної та політичної підтримки Вашинґтона.

З погляду Александера та його підлеглих, було безвідповідально знехтувати можливістю допомогти міністерству всім, чим можна. Проте це не означало, що агентство зійде з орбіти, поступившись провідною роллю у кіберпросторі. Воно підпорядковувалося Міністерству оборони, і його повноваження поширювалися на захист держави від іноземних атак на землі, у повітрі, на воді й у комп'ютерних мережах.

За словами колишнього держслужбовця, якому доводилося працювати з обома, Чертофф і Александер швидко знайшли спільну мову. Здавалося, що міністр із радістю дозволив кібервоїнам з Форт-Міда узяти на себе керівництво. Наступні чотири роки Александер присвятив розбудові кіберармії АНБ, і кульмінацією його діяльності стали операція «Американська картеч» і створення Кіберкомандування. У 2009 році Обама призначив колишню губернаторку Арізони Дженет Наполітано міністром внутрішньої безпеки. Александер наказав своїм підлеглим надавати Наполітано та її команді всю можливу допомогу та консультації. Але він не мав наміру відступати з поля битви. Не тоді, коли він готувався почати свою найбільшу кампанію.

Александер вже бачив, як «Ініціатива оборонної промисловості» (Defense Industrial Base – DIB) дозволила урядові отримати доступ до інформації з корпоративних комп'ютерних мереж. Компанії пере-

творилися на цифрових розвідників у кіберпросторі, а інформація, яку вони постачали, допомагала АНБ поповнювати каталог з описами загроз – перелік відомого шкідливого ПЗ, хакерських методів і підозрілих інтернет-адрес. Александер називав цю ініціативу «секретним складником». Спочатку програма DIB охоплювала лише 20 компаній. Але Александер прагнув поширити модель DIB на підприємства інших галузей, зокрема енергетичної та фінансової, і залучити для участі в програмі щонайменше 500 компаній.

У АНБ цей план назвали «Транш 2» (Tranche 2). Оператори «критично важливих об'єктів інфраструктури» (під це визначення підпадали електростанції, підприємства атомної промисловості, банки, розробники програмного забезпечення, транспортні та логістичні компанії, ба навіть медичні установи й постачальники медичного обладнання, якщо його можна вивести із ладу віддалено), згідно із законом або регулятивним актом, повинні були дозволити провайдерові інтернет-послуг моніторити вхідний і вихідний трафіки. Послуговуючись переліком загроз АНБ, провайдер шукатиме шкідливі програми або ознаки іноземних кібервтручань. Так виглядала перша версія плану Александера з перетворення АНБ на головний розвідувально-аналітичний центр із виявлення кіберзагроз. АНБ не здійснюватиме сканування самостійно, але надасть усю необхідну інформацію для пошуку загроз провайдерам. Це допоможе агентству уникнути підозр у тому, що воно торує собі шлях у приватні комп'ютерні мережі, але не перешкодить керувати операцією. Щойно сканер виявить загрозу, аналітики АНБ утрутяться й отримають доступ до неї. Вони вирішать, пропускати трафік чи заблокувати його, і за потреби проведуть контратаку на джерело загрози.

Агентство вже розробило систему для сканування Tutelage, здатну ізолювати електронні листи з вірусами й переносити їх у цифровий аналог чашки Петрі, де аналітики могли б вивчати їх, не заражаючи інші комп'ютери. Ця система була тим самим «сенсором, вартовим і снайпером», що використовувало АНБ для спостереження за власними інтернет-шлюзами в 2009 році. Тепер Александер хотів зробити цю систему частиною програми Tranche 2, штовхаючи сотні компаній і операторів критично важливих інфраструктурних об'єктів на новий фронт кібернетичних воєн.

Деякі офіційні особи з адміністрації Обами занервували. Президент чітко заявив про свій намір захищати кіберпростір як важ-

ливий державний ресурс. Але він вагався щодо довжини повідця, на якому перебуватиме АНБ. Обама ніколи не мав теплих почуттів ані до агентства, ані до Александера. І хоча він цінував і використовував величезні можливості, які могло запропонувати АНБ, культура шпигунства здавалася йому чужою.

Улітку 2009 року офіційні представники Пентаґону розробили проект «виконавчого акту», який би дозволив військовим здійснювати контратаки на комп'ютери, звідки виходив шкідливий трафік, скерований не лише проти військових систем, а й проти мереж приватних підприємств критично важливої інфраструктури, як-от електростанції. Це був екстраординарний крок. Досі уряд лише надавав допомогу компаніям, забезпечуючи їх інформацією про хакерів і шкідливе ПЗ, і завдяки цьому вони могли посилювати власний захист. Тепер АНБ вимагало повноважень на проведення контратак проти кожного, хто атакує важливі підприємства Америки, якщо ці атаки могли призвести до людських жертв (скажімо, унаслідок аварії енергосистеми або виведення з ладу системи управління повітряними польотами) або якщо під загрозою опинялась американська економіка чи державна безпека. Ці нечітко сформульовані критерії дозволяли широку інтерпретацію повноважень. До прикладу, чи можна вважати масовану DDOS-атаку на американські банки, яка не руйнує банківську систему і не скерована на викрадення грошей, а лише призводить до збою в роботі, ворожим актом, що загрожує економіці США?

Адміністрація Обами підкорегувала законопроект, але зміни були несуттєвими. Обама не став перешкоджати АНБ наносити удари у відповідь. Він лише вимагав схвалення таких дій президентом або міністром оборони.

Можливо, відчуваючи, що не варто покладатися на безумовну підтримку Обами, Александер презентував свій план програми Tranche 2 законодавцям, які контролювали багатомільярдний бюджет його агентства. Александер розповів їм, що закон, який зобов'яже компанії передавати дані, не схвалює адміністрація президента, принаймні не в цій формі. Білий дім кілька разів (у 2011-му і 2012 році, під час розгляду законопроекту в Конгресі) попереджав Александера про неприпустимість виступів од імені президента й озвучення обіцянок, виконання яких адміністрація не могла дотримати.

«Люди з центру незадоволені мною», – боязко зізнався Александер під час зустрічі з конгресменами. Проте це не зупинило його від

просування своїх планів. Александер виявився жалюгідним промовцем, але у вузькому колі він міг бути вельми чарівним і переконливим. Він уклав союз із лідерами Демократичної та Республіканської партій і комітетом із питань розвідки у сенаті. Законодавці давали йому потрібні суми й схвалювали нові бюджети на забезпечення кібербезпеки. Нагляд Конгресу за діяльністю АНБ був мінімальним і ненав'язливим. Александер вигравав війну на Капітолійському пагорбі. Проте у нього з'явилися вороги в адміністрації президента.

Іще до початку роботи у міністерстві у перші дні 2009 року нова заступниця міністра внутрішньої безпеки Джейн Голл Лют виявила, що битва за контроль над кібербезпекою вже добігла кінця і Александер переміг. Чимало її колег давно висновували, що АНБ – це єдиний варіант, адже лише це агентство володіло розлогим каталогом комп'ютерних загроз, який містив описи шкідливого ПЗ, хакерських методів і підозрілих інтернет-адрес. Вони знали, що ця інформація зібрана по крихтах під час проведення секретних і дорогих розвідувальних операцій, що свідчило про надійність і важливість даних. Їм також було відомо, що Міністерство внутрішньої безпеки не мало подібного сховища інформації, а про персонал у сфері кібербезпеки годі й казати. У 2009 році у міністерстві працювали 24 фахівці-комп'ютерники, натомість у Міністерстві оборони таких службовців було понад 7 тисяч і більшість із них працювала в АНБ. Центр нагляду за надзвичайними мережевими ситуаціями Міністерства внутрішньої безпеки не міг відстежувати мережевий трафік у реальному часі, що робило його практично неужитковим для раннього виявлення кібератак. Міністерство могло розраховувати хіба що на роль PR-служби, яка переконує компанії дотримуватись ефективних практик «кібернетичної гігієни», краще стежити за власними мережами й ділитись інформацією з урядом. Але це були символічні жести, а не реальні дії.

Службовця, який відповідав за розвиток кіберзахисної місії міністерства, Лют побачила вперше, коли він простягнув їй заяву про звільнення. Род Бекстром звільнився у березні, протестуючи проти того, що він описав як втручання АНБ у політику, а це, згідно із законом, було прерогативою Міністерства внутрішньої безпеки. «АНБ контролює діяльність міністерства у сфері кібербезпеки», – з докором написав Бекстром. Співробітники агентства мали робочі місця

у штаб-квартирі міністерства й упровадили тут свої закриті методи праці. А нещодавно керівники АНБ запропонували перевести Бекстрома і його підлеглих – усіх п'ятьох – у штаб-квартиру агентства у Форт-Міді.

«Під час мого перебування на посаді директора ми опиралися підпорядкуванню [центра] АНБ», – писав Бекстром. Він попередив Лют, Наполітано і головних президентських радників із питань державної безпеки, зокрема й міністра оборони Роберта Ґейтса, що у разі, якщо попустити АНБ віжки, воно грубо потопчеться по недоторканності приватного життя й цивільних свободах і впровадить у міністерстві атмосферу секретності.

Лют не була експертом у сфері кібероперацій. Армійський офіцер у відставці, донедавна вона керувала миротворчими операціями ООН. Але, як де-факто головний операційний керівник міністерства, вона відповідала за виправлення його досі непрозорої кіберполітики. Очевидно, це означало продовження битви з АНБ. (Наполітано не хотіла обіймати керівну посаду, та й навряд чи мала потрібну кваліфікацію. Фактично вона була технофобкою, не мала особистого профілю в мережі та навіть на роботі не користувалася електронною поштою.)

Лют досить довго крутилася в колах розвідників, аби виснувати, що вони отримують владу почасти завдяки секретності та створенню такої собі видимості всезнання. Вона не погоджувалася з поширеною думкою, буцімто лише АНБ володіє технологіями, необхідними для захисту кіберпростору. «Уявіть, що телефонний довідник Мангеттена – це всесвіт шкідливого ПЗ, – якось сказала вона колегам. – АНБ має лише одну сторінку цього видання». Лют вважала, що чимало компаній уже володіють інформацією про найбільші загрози: вони змушені її збирати, бо хакери та іноземні держави щодня намагаються проникнути в їхні мережі. Приватні компанії з кіберзахисту, розробники антивірусних програм і навіть журналісти зібрали й проаналізували масив даних щодо шкідливих програми та інші кіберзагрози; вони продавали цю інформацію або оприлюднювали її на загальнодоступних ресурсах. Розробники програмного забезпечення випускали автоматичні оновлення для виправлення виявлених дір у системі безпеки власних програм. АНБ відстежувало цю інформацію. Чому ж нікому не спадає на гадку, що розвіддані агентства містять відому всім інформацію? «Інформація шпигунського агентства може бути корисною, проте компанії не завжди потребують її для зміц-

нення власного захисту», – говорила Лют. Потрібно, щоб компанії обмінювались одна з одною відомою їм інформацією та створили щось штибу інтернет-версії сусідського нагляду.

Лют була не єдиною, хто вважав, ніби Александер надто дорого продає свій «секретний складник».

«Є припущення, що коли інформація засекречена, вона правдива, але не у цьому випадку, – розповідає один керівник правоохоронних органів, який сперечався з керівниками АНБ на кількох нарадах із приводу того, чи повинно агентство відігравати провідну роль у захисті промислових комп'ютерних мереж. – Ми можемо надати політикам інформацію з грифом секретності (рівень нижчий, ніж "цілком таємно"), а вони скажуть: "Не треба, у нас є надсекретний звіт, і в ньому міститься геть уся правда". І заперечити тут важко, тому що АНБ не викладає на стіл усі карти щодо джерел інформації та її унікальності. Законотворці та громадяни не бачать усієї картини загроз».

Навіть зустрічаючись із чільниками найбільших технологічних компаній, зокрема Google, які досить багато знали про кібершпигунів і атаки й мали фінансову зацікавленість у тому, щоб їх зупинити, Александер, однак, намагався переконувати їх, що АНБ володіє достовірнішою й важливішою інформацією. «Його позиція виглядала так: "Якби ви знали те, що знаємо ми, ви б дуже злякалися. Я єдиний, хто може вам допомогти"», – розповідає колишній високопосадовець, що опікувався питаннями безпеки.

«Александер переконав багатьох законодавців і політиків, що АНБ є монополістом і лише у Форт-Міді можна знайти допомогу, – розповідав колишній представник адміністрації президента, який займався питаннями кібербезпеки. – І він використовував цю фразу про "секретний складник". Я перебував тоді по інший бік таємничої завіси; "секретного складника" не існує. Це повна нісенітниця».

Перші два роки роботи Лют у Міністерстві внутрішньої безпеки панувала незначна напруга. Але в лютому 2011-го вона переросла у відкриту війну за сфери впливу. На конференції з питань безпеки оборонної промисловості, що відбулася у Колорадо-Спрінґс, домівці Академії ВПС США, Александер проголосив, що саме АНБ повинно відгравати роль лідера у захисті кіберпростору. Він вимагав нових повноважень для забезпечення захисту від нищівних кібератак на

Сполучені Штати. «У мене немає повноважень для припинення атак на Волл-стріт або промислові підприємства, і цю прогалину потрібно ліквідувати», – сказав він. Александер кинув виклик, оголосивши американський кіберпростір мілітаризованою зоною.

Александер планував виступити з подібною промовою за вісім днів на одній з найбільших щорічних конференцій з комп'ютерної безпеки у Сан-Франциско. Найвпливовіші газети і профільні ЗМІ готувались її відвідати. Але Лют перетасувала всі карти. 14 лютого, за три дні до запланованого виступу, вона разом з іншим керівником Міністерства внутрішньої безпеки оприлюднила на сайті Wired, впливового журналу про технології, статтю. «Останнім часом деякі спостерігачі наполегливо б'ють у барабан війни, закликаючи готуватися до битви, і навіть стверджують, що Сполучені Штати вже ввійшли у стан кібервійни, фактично програючи бій, – писала Лют. – Ми з цим не згодні. Кіберпростір – це не зона військових дій».

Це був прямий удар по Александеру. «Безсумнівно, тут існують конфлікти й зловживання, але кіберпростір – це цивільний простір, – писала Лют, – громада, бібліотека, ринок, шкільний двір, майстерня – і нова чудова епоха в людському досвіді, освіті та розвитку. Лише частина цього простору припадає на американську оборонну інфраструктуру, яку належним чином охороняють солдати. Проте основна частина кіберпростору – це простір цивільний».

Александер не вгамувався. Він виступив із запланованою промовою та повторив ті самі тези. А за кілька днів завдав удару у відповідь. «Багато народу говорить, що їм до вподоби технічні можливості АНБ… але вони не хочуть, щоб АНБ лізло до них», – сказав Александер у Вашинґтоні, під час виступу на конференції, присвяченій внутрішній безпеці, яка залишалася прерогативою Міністерства внутрішньої безпеки. Він знехтував порадою відійти вбік і допомагати із захистом, лише коли про це просять, а не рватися на лінію фронту. Александер навіть пригадав лінію Мажіно – довгу смугу залізобетонних укріплень, збудованих Францією на кордоні з Німеччиною в 30-х роках XX століття, натякаючи, що Сполучені Штати можуть програти, якщо зосередяться лише на стратегічному підході до власної оборони й недооцінюватимуть підступність ворогів. (Нацисти здолали лінію Мажіно, обійшовши її, чого Франція аж ніяк не очікувала, і завоювали країну за шість тижнів.)

Війна за сфери впливу набирала обертів. Білий дім рішуче відкинув план Александера Tranche 2, і не тому, що Обама вважав, ніби АНБ не впорається із захистом кіберпростору, а тому, що цей план вельми нагадував масштабну державну програму стеження за громадянами. Адміністрація не відмовлялася від основної ідеї Александера. Але вирішила натомість скористатися вже наявною програмою DIB, яка також була державною програмою стеження, і перевірити, чи зможуть інтернет-провайдери моніторити трафік за допомогою секретної розвідувальної інформації – того самого «секретного складника» АНБ. Ось такий компроміс: АНБ не отримає доступу до мереж компаній, але надаватиме їм розвідувальну інформацію через інтернет-провайдерів.

Навесні 2011 року 17 оборонних підприємств добровільно погодилися взяти участь у тестуванні програми. АНБ надалі передавало інформацію про загрози трьом інтернет-провайдерам – компаніям CenturyLink, AT&T і Verizon. Останні дві були добре знайомі зі системою стеження АНБ, позаяк брали участь у масовому зборі інформації про телефонні комунікації американців незабаром після терактів 11 вересня. І всі три компанії без питань передавали електронні листи й онлайн-дані клієнтів на запит ФБР і АНБ.

Пілотна програма зосереджувалася на двох контрзаходах: «карантині» вхідних електронних листів, заражених шкідливими програмами, і запобіганні вихідному трафіку з інтернет-адрес потенційних зловмисників методом нейтралізації ботнетів. Більшість організацій відстежувала лише вхідний трафік та ігнорувала дані, які виходили з їхніх систем. Хакери користувалися цією прогалиною в захисті та часто маскували документи компаній, що викрадалися, під звичайний вихідний трафік, перш ніж надіслати їх на контрольований сервер.

Тестування програми засвідчило її ефективність. Незалежний аналіз, виконаний Університетом Карнегі-Меллон, одним із провідних науково-дослідних інститутів країни, показав, що інтернет-провайдери здатні відстежувати й надійно зберігати секретну інформацію про кіберзагрози. Але для надміру возвеличених кібервоїнів із Форт-Міда це стало поганою новиною: практично жодна отримана від АНБ інформація не містила нічого, чого досі не знали компанії, і це підтвердило здогади Лют та інших експертів, які сумнівалися в існуванні «секретного складника» Александера.

Більшість інформації від АНБ вже не була актуальною на час отримання. З 52 випадків шкідливої активності, виявленої під час тестування програми, лише дві нейтралізували завдяки допомозі АНБ. Усі інші загрози компанії виявили самостійно, адже впродовж останніх кількох років вони власноруч вибудовували свої системи моніторинґу мереж і зводили стіну кіберзахисту.

АНБ могло б утішатися тим, що ці компанії вдосконалили свій захист завдяки приєднанню до програми DIB у 2007 році, коли їх примусили передавати інформацію про загрози і приймати державну допомогу, якщо вони хотіли й надалі мати справи з військовими. Проте пілотна програма перекреслила арґументи Александера на користь того, що лише його агентство має унікальну кваліфікацію для захисту нації.

Щоб зрозуміти це, університетська освіта не була потрібна. Керівники корпорацій ще 2010 року почали запитувати, чи справді АНБ аж така передова організація, як проголошував Александер. Під час наради з генеральними директорами підприємств у штаб-квартирі Міністерства внутрішньої безпеки Александер виступив із презентацією каталогу кіберзагроз, укладеного АНБ. Як розповідав один з учасників наради, генеральний директор компанії Google Ерік Шмідт нахилився до свого сусіда і прошепотів: «Тобто, вони намагаються нам сказати, що витратили всі ці гроші та здобули лишень оце? Ми давно це знаємо». Компанія Google, як і чимало інших великих компаній, часто атакованих хакерами, мала власні джерела інформації і збирала базу інформації про китайських хакерів. Її джерелами могли виступати приватні компанії зі сфери комп'ютерної безпеки, як-от Endgame, що продають інформацію про вразливості нульового дня. Водночас Google застосовувала й інші підходи: наприклад, впровадила складніші алгоритми шифрування даних користувачів і рухалася до впровадження так званого протоколу SSL, який забезпечує наскрізне шифрування за замовчуванням для всіх, хто користується сервісами Google. Збір інформації про загрози «більше не працює», запевняв Шмідт. Загрози не з'являються саме там, де АНБ розставляє сенсори. Хакери повсякчас змінюють методи роботи й шукають нові способи входу. Вони знають, що влада стежать за ними, – ось чому змінюють тактику.

Для Google, так само як і для інших великих компаній, ішлося не про один-єдиний «секретний складник», а про технологічне рагу

з багатьох складників, рецепт якого постійно змінюється. Загалом, компанії дуже серйозно ставилися до безпеки, вкладаючи власні кошти у захист важливої інформації та наймаючи незалежних експертів, аби надолужити там, де не могли впоратися самостійно.

Проте Александер наполягав на своєму. У 2011 році він вирушив до Нью-Йорка, де зустрівся з керівниками кількох найбільших фінансових організацій країни. Там, у конференц-залі у Мангеттені, йому поблажливо пробачили те, що він поводився так, наче знову опинився у 2007 році, у тому захищеному від зовнішніх загроз кабінеті Пентаґону, коли ось-ось мав повідомити промислових титанів, яке величезне лихо їх усіх спіткало.

АНБ уже ділилося деякою інформацією про кіберзагрози з банками через некомерційну організацію, яку ці ж банки створили, – так званий Центр аналізу й обміну інформацією. Ця система не відстежувала загроз у реальному часі, проте допомагала банкам не відставати від сучасних тенденцій у сфері безпеки й інколи отримувати своєчасні попередження про види шкідливого ПЗ і нові методи проникнення в мережі. Компанії з інших галузей так само створювали подібні центри для об'єднання колективних знань, проте банки досягли кращих результатів, тому що їм було що втрачати (кіберзлодії щороку викрадають мільярди доларів) і тому що їхня робота залежала від мереж передачі даних.

Александер розповів банкірам, що хоче поширити програму обміну інформацією DIB на банківський сектор, але цього разу використати одну хитрість. Александер пояснив, що буде значно легше забезпечити захист компаній, якщо вони дозволять АНБ встановити обладнання для стеження у своїх мережах. Викинути посередника. Дозволити аналітикам із Форт-Міда заходити безпосередньо на Волл-стріт.

У кімнаті запанувала тиша. Спантеличені керівники лише поглядали один на одного. *Цей парубійко говорить серйозно?*

«Вони вирішили, що він несповна розуму, – розповідає директор фінансової організації, який був присутній на тій нараді та зустрічав Александера раніше. – Адже він говорив про приватні мережі. Атаки, які траплялися в нашій галузі, зазвичай цілили у користувацький інтерфейс – сайти онлайн-банків або у сайт Nasdaq». Упродовж останніх років ці сайти піддавалися так званим DDOS-атакам, які перенавантажують сервери інформаційними запитами, що призводить

до порушення їхньої роботи, але це не знищує дані про рахунки, бо вони зберігаються у внутрішній банківській мережі. І ця інформація здебільшого передається мережами, які взагалі не мають з'єднання з інтернетом або ці з'єднання вкрай обмежені. «Це неправда, що банки відкриті для атак з інтернету. А Федеральна резервна система, Міністерство фінансів, біржові брокери, платіжні системи – усі вони по-справжньому добре знають усю інфраструктуру фінансових послуг і те, як вона працює. Александер і гадки про це не мав».

Компанії, що надають фінансові послуги, не нехтують кіберзагрозами. Згідно з одним запитуванням, дві третини американських банків повідомили, що зазнавали DDOS-атак. Проте Александер пропонував компаніям піти на невиправданий ризик. Він намагався впровадити в їхні комп'ютери власних шпигунів. Якби про таку операцію стало відомо, політичні наслідки були б жахливими. Ба більше, якби агентство інсталювало своє обладнання без попередження або судового дозволу, компанії могли притягнути його до відповідальності за незаконну шпигунську діяльність.

Навіть якщо б банки впустили АНБ у свої мережі, навряд чи агентство могло повідомити їм більше, ніж вони знали із власних джерел. Чимало провідних американських банків створили служби безпеки для попередження шахрайства з кредитними картками і банківських крадіжок. Суми грошей, які фінансові організації втрачають щороку внаслідок кіберзлочинів, варіюють від сотень мільйонів до мільярдів доларів залежно від виду й масштабу злочину. ФБР вистежує хакерські банди, які намагаються проникнути в банківські мережі та вкрасти гроші або здійснити шахрайські транзакції з кредитних карт, і ділиться здобутою інформацією з фінансовими організаціями. Проте федерали частенько виявляють, що колеги з корпоративних служб безпеки вже випередили їх.

У 2009 році близько 30 представників правоохоронних органів і розвідслужб і співробітники служб безпеки провідних американських банків зустрілися в штаб-квартирі ФБР у Вашинґтоні. «Десь посередині зустрічі ми запитали, як відбувається обмін інформацією між фінансовим сектором і державою, – розповідає Стів Чабінські, який колись був помічником заступника директора ФБР із питань кібербезпеки, а згодом почав працювати в приватній компанії CrowdStrike. – Усі лише скрушно зітхнули».

«Ви хочете, щоб ми були чесними? – запитав представник міжбанківської ради з питань обміну інформацією, створеної для спілкування між банками та владою. – Це не найкращий обмін. Ми добровільно передаємо вам усю нашу інформацію і нічого не отримуємо натомість». Представники ФБР зауважили, що передали банкам перелік загроз, зокрема й список підозрілих інтернет-адрес, що можуть належати кіберзлочинцям. Створення цього звіту потребувало неабияких зусиль. Деяка інформація була призначена тільки для використання правоохоронними органами або взагалі була секретною.

«Гаразд, – відповів представник банку, – якщо це все, на що ви здатні, у нас проблеми. Тому що нам усе це відомо». Банки обмінюються інформацією та купують її у приватних розвідувальних компаній. Урядовці почали усвідомлювати, що не мають монополії на збір інформації. ФБР вирішило поділитися з банками звітами про поточні розслідування, щоб ті могли оцінити глибину його знань, розповів Чабінські. Однак виявилося, що банки відстежували кожну справу з цього переліку, крім однієї. Хакери націлювалися на мережу автоматичного клірингового центру – електронної системи, яка обробляла масив транзакцій, зокрема й прямі депозити, платежі по кредитних і дебетових картах, а також електронні перекази між рахунками. Крадіжка особистих даних і паролів людей, які використовували мережу, дозволила б злодіям зняти з численних рахунків близько $400 млн. Банки вже здогадувалися, що хакери полюють на клірингову мережу, проте не уявляли масштабів і не знали про методи викрадання особистих даних, виявлені ФБР. Банки були вдячні за інформацію та змогли залатати вразливі місця у системах безпеки. Але це був той рідкісний випадок, коли ФБР знало щось таке, чого не знали банки.

Спецслужби рідко переслідують кіберзлочинців, особливо якщо шахраї живуть у країнах з недосконалим законодавством у сфері кіберзлочинів, які не мають домовленості із США про екстрадицію підозрюваних. «Росіяни попередять хакерів, що ми за ними стежимо, і запропонують тим змінити імена, щоб було важче їх знайти», – розповідає один із керівників правоохоронних органів, який працював над розслідуванням кіберзлочинів. І це ставить банки у складне становище, адже їм доводиться наодинці протистояти хвилі криміналітету, масштаби й амбіції якого постійно зростають, натомість правоохоронні органи довели своє безсилля у стримуванні загроз.

Керівники фінансових організацій не підтримали план Александера зі встановлення шпигунського обладнання в їхніх мережах. Проте не зупинили його інших масштабніших планів. Після повернення до Вашинґтона він проштовхнув рішення щодо передачі АНБ повноважень із захисту інших критично важливих галузей економіки. Чільне місце у списку належало енергетиці, за якою йшло водопостачання. «Він хотів звести стіну довкола найуразливіших організацій Америки… і встановити в їхніх мережах обладнання для стеження», – розповідає колишній представник адміністрації президента. Програма Tranche 2 померла, а пілотна програма DIB підірвала осяйну репутацію АНБ, проте Александер продовжував натискати на всі важелі, головно спираючись на підтримку адміністрації президента. Пілотну програму не назвали цілковитою поразкою. Деякі представники адміністрації, зокрема й з Міністерства внутрішньої безпеки, зауважували, що програма довела ефективність передачі секретної інформації компаніям через обраних владою посередників. Хоч би як було складно, але вони можуть працювати в тандемі. І хоча дані АНБ дозволили виявити лише дві унікальні загрози, це таки краще, ніж зовсім нічого, додавали держслужбовці.

Міністерство внутрішньої безпеки отримало номінальний контроль над розширеною програмою DIB, доступ до якої дістали ті підприємства поза оборонною сферою, добробут яких був важливим для державної та економічної безпеки США. Уряд вибирав компанії, що потребували особливого захисту, навмання. Натомість збір інформації про загрози й більша частина технічного аналізу шкідливого ПЗ і методів проникнень надалі залишалися за АНБ, що часто співпрацює з ФБР, діяльність якого (а також бюджет) була спрямована з антитерористичної діяльності на кібербезпеку. У 2013 році в АНБ працювало понад тисячу математиків (більш ніж у будь-якій іншій організації США), 900 кандидатів наук і 400 комп'ютерних фахівців. Мізки й м'язи для забезпечення державного кіберзахисту продовжують надходити з АНБ, і, можливо, так буде завжди.

Виникло бюрократичне непорозуміння, але, врешті-решт, влада надалі контролює захист кіберпростору й розглядає інтернет як стратегічний державний ресурс – саме це й обіцяв Обама у промові, виголошеній у Білому домі в травні 2009 року. Александер знав, що агентство не спроможне відстежити кожну загрозу в інтернеті; йому надалі була необхідна інформація від компаній. Тому він почав тис-

нути на суспільство. Під час промов і виступів у Конгресі він попереджав, що хакери вдосконалюють власну майстерність, що кількість кіберзлочинів зростає і що компанії не мають технічного ресурсу, щоб захистити себе. Александер вимагав посилення державного контролю в цій сфері, щоб спонукати компанії підвищити стандарти безпеки й гарантувати відсутність кримінального переслідування тим, хто передає в АНБ інформацію про комунікації своїх клієнтів без судового дозволу. Александер називав кіберзлочинність і шпигунство «найбільшим перерозподілом багатства в історії» і попереджав, що поки американський бізнес не посилить кібероборону, державі надалі загрожує «кібернетичний Перл-Гарбор».

«Ми бачимо зростання рівня активності в мережах, – застерігав Александер на конференції з безпеки 2013 року в Канаді, через два роки після зустрічі з керівниками фінансових організацій. – Я стурбований тим, що незабаром ситуація вийде з-під контролю, приватний сектор надалі не зможе протистояти загрозі, і державі доведеться вступити у гру».

Деякі компанії прислухалися до попередження. Але не так, як розраховував Александер. Вони знали, що загроз побільшало. Вони бачили, як хакери пускають коріння в їхніх мережах і щодня викрадають дані. Але виснували, що, попри гучні заяви АНБ, держава не в змозі їх захистити. Компаніям доведеться захищатися самостійно.

11
КОРПОРАТИВНА КОНТРАТАКА

У середині грудня 2009 року програмісти зі штаб-квартири Google, розташованої в містечку Маунтін-В'ю в Каліфорнії, почали підозрювати, що хакери з Китаю отримали доступ до приватних облікових записів поштового сервісу Gmail, зокрема й до тих, які використовують китайські правозахисники, що перебувають в опозиції до влади Пекіна. Як і більшість інших відомих інтернет-компаній, Google та її користувачі часто ставали мішенями для кібершпигунів і злочинців. Але коли фахівці придивилися до атаки пильніше, то виявили, що це не звичайна хакерська операція.

Під час цієї операції, яку Google згодом назве «хитромудрою і цілеспрямованою атакою Китаю на нашу корпоративну інфраструктуру», кіберзлодії змогли отримати доступ до системи паролів, яка дозволяла користувачам входити в низку служб Google водночас. Ця система була найважливішим об'єктом інтелектуальної власності, яку розробники вважали «коштовним каменем у короні» вихідних кодів компанії. Google хотіла отримати конкретні докази зламування, щоб поділитися ними з правоохоронними органами та розвідкою США. Отож фахівці компанії відстежили джерело зламу – сервер у Тайвані, з якого висмоктували системну інформацію. Вірогідно, цей сервер контролювали хакери з материкового Китаю.

«Google зламала цей сервер», – розповідає колишній старший офіцер розвідки, який знав про дії компанії. За його словами, у цьому рішенні крився певний правовий ризик. Чи була це справді контратака? Позаяк не існує закону, що забороняє домовласникові простежити за грабіжником до місця його проживання, компанія Google не порушила жодних законів, відстеживши джерело вторгнення в свої системи. Хоча невідомо, як саме фахівці компанії дістали доступ до сервера, попри отримання контролю над ним, вони б переступили межу закону лише тоді, коли б видалили або знищили дані. Але Google

нічого не знищувала. Натомість компанія зробила дещо неочікуване й безпрецедентне – поділилася здобутою інформацією.

Компанія Google розкрила подробиці однієї з наймасштабніших кібершпигунських кампаній в американській історії. Докази свідчили про те, що китайські хакери проникли в системи близько тридцяти різних компаній, серед яких виявилися технологічні гіганти Symantec, Yahoo, Adobe, оборонний підрядник Northrop Grumman і виробник обладнання Juniper Networks. Широта кампанії не дозволяла визначити її головну мету. Чи було це промислове шпигунство? Стеження за правозахисниками? Або ж Китай намагався створити щось штибу плацдарму для шпигунів у основних секторах американської економіки, ба більше, інсталювати шкідливе ПЗ у системи управління критично важливими об'єктами інфраструктури? Єдине, у чому компанія Google, як здавалося, була упевнена, то це те, що хакерська операція була масштабною і тривалою і за нею стояв саме Китай. Це були не просто незалежні хакери, а китайська влада, яка мала засоби й мотиви для такої масованої атаки.

Google поділилася своїми знахідками з іншими атакованими компаніями, а також із правоохоронними органами та розвідувальними службами. Протягом останніх чотирьох років керівники корпорацій потай тиснули на урядовців, закликаючи їх оприлюднити інформацію про китайське шпигунство, присоромити цю країну й змусити її припинити цю хакерську кампанію. Але для заяв, у яких вони могли б тицьнути пальцем в обвинувачену державу, президентові Обамі чи держсекретарю Гілларі Клінтон були потрібні докази того, що атаки виходять саме з Китаю. Переглядаючи матеріали, надані компанією Google, державні аналітики не були впевнені у неспростовності цих доказів. Американські урядовці вирішили: якщо вони оприлюднять те, що дізналася Google, зважаючи на нестабільні взаємини між двома найбільшими економіками світу ризик конфлікту дуже великий.

Компанія Google з цим не погодилася.

Заступник держсекретаря Джеймс Штейнберґ розважався на коктейльній вечірці у Вашинґтоні, коли його асистент приніс термінове повідомлення: Google збирається оприлюднити заяву щодо китайської шпигунської кампанії. Штейнберґ, друга за рангом особа у справах зовнішньої політики, миттєво збагнув масштабні наслід-

ки цього рішення. Американські корпорації досі не бажали публічно звинувачувати Китай у шпигунстві або крадіжці інтелектуальної власності. Компанії боялися втратити довіру інвесторів і клієнтів, а тому запрошували незалежних хакерів, щоб ті латали найуразливіші місця в корпоративній системі безпеки, і розлючено лаяли китайських чиновників, у владі яких негайно закрити доступ до одного з найбільших і найдинамічніших ринків для американських товарів і послуг. Для будь-якої компанії виступ проти Китаю мав би вагомі наслідки. Але для Google, найвпливовішій компанії епохи інтернету, це було історичне рішення.

Наступного дня, 12 січня 2010 року, головний фахівець юридичного відділу Google Дейвід Драммонд оприлюднив розлогу заяву в блозі компанії, звинувачуючи китайських хакерів у атаці на інфраструктуру Google, і розкритикував китайську владу за цензуру в інтернеті та переслідування правозахисників. «Ми пішли на незвичний крок, поділившись інформацією про ці атаки з широкою аудиторією, не лише тому, що виявили порушення безпеки та цивільного права, а й тому, що ця інформація стане основою для масштабнішої глобальної дискусії з приводу свободи слова», – заявив Драммонд.

Представники Держдепартаменту побачили рідкісну можливість натиснути на Китай, звинувативши його у шпигунстві. Того ж вечора Гілларі Клінтон виступила з власною заявою. «Ми отримали інформацію про звинувачення Google, які порушують дуже серйозні питання й проблеми. Ми чекаємо пояснень від китайського уряду, – сказала вона. – Для сучасного суспільства й економіки довіра до кіберпростору вкрай важлива».

Ці дипломатичні заяви мали неабияке значення. Завдяки сміливості Google адміністрація Обами отримала змогу звинуватити Китай у шпигунстві, не висуваючи власних арґументів, а просто посилаючись на факти, виявлені компанією під час власного розслідування. «Це була слушна нагода обговорити ці питання без викриття секретних джерел або делікатних методів [збору інформації]», – підкреслив Штейнберґ. Компанія Google не попереджувала адміністрацію про власне рішення, яке йшло врозріз із нехіттю деяких офіційних осіб до громадських обговорень шпигунства. Але тепер, коли все сталося, ніхто не нарікав. «Це було їхнє рішення. Звісно, у мене не було жодних заперечень», – розповідав Штейнберґ.

Адміністрація Обами змінила тон спілкування з Китаєм на суворіший, а почалося все з промови Клінтон щодо започаткування ініціативи сприяння свободі в інтернеті (Internet Freedom initiative), виголошеної через дев'ять днів після заяви Google. Вона закликала Китай припинити цензуру пошукових запитів у інтернеті та блокування доступу до сайтів, які публікують критику державних лідерів. Клінтон порівняла ці віртуальні бар'єри з Берлінським муром.

Натомість компанія Google заявила, що припинить фільтрувати результати пошуку за словами й темами, забороненими державною цензурою. А якщо Пекін заперечуватиме, Google ладна піти ва-банк і полишити китайський ринок, навіть утративши при цьому мільярди доларів потенційного зиску. Ця заява посадила інші американські технологічні компанії на «розпечений стілець». Чи готові вони й надалі миритися з державним утручанням і придушенням свободи слова, щоб зберегти свій бізнес у Китаї?

Після заяви Google іншим компаніям стало простіше визнати, що вони також піддавалися хакерським атакам. Урешті-решт, якщо з цим стикнулася Google, це могло статися з будь-ким. Шпигунські атаки Китаю могли стати навіть ознакою важливості компанії, на яку звернула увагу наддержава. Один-єдиний пост у блозі Google змінив риторику глобальної дискусії на тему кіберзахисту.

Компанія Google також задекларувала, що багато знає про китайських шпигунів. АНБ хотіло знати, наскільки багато.

Google сповістила АНБ і ФБР про те, що її мережі зламали хакери з Китаю. Як правоохоронне агентство, ФБР могло почати розслідування цього проникнення як кримінального злочину. Проте АНБ був потрібний дозвіл Google на участь у розслідуванні та аналіз прогалини в захисті. Того самого дня, коли юрист Google написав свій пост у блозі компанії, головний юрисконсульт АНБ почав готувати проект «Угоди про спільне дослідження та розвиток» – правового акту, розробленого на підставі закону 1980 року задля прискорення комерційного розвитку нових технологій, в яких були зацікавлені не лише компанії, а й держава. В угоді йшлося про спільне створення нових пристроїв чи розробку технологій. Компанія не отримувала грошей, але могла розраховувати на те, що держава профінансує витрати на дослідження й розробку та дозволить використовувати державне обладнання й за-

лучати фахівців із держструктур для проведення досліджень. Кожна зі сторін зберігала результати співпраці у таємниці, поки обидві не погоджувались їх оприлюднити. Як наслідок, компанія отримувала ексклюзивний патент на те, що було створене спільними зусиллями, натомість держава могла використовувати будь-яку інформацію, набуту в рамцях цієї співпраці.

Не відомо, що саме спільно створили АНБ і Google після китайської хакерської заяви. Проте під час написання угоди представниця агентства зробила кілька натяків. «Загалом, у рамках місії із забезпечення інформаційної безпеки АНБ працює з низкою комерційних партнерів і дослідницьких об'єднань, аби запевнити доступність безпечних особливих рішень для Міністерства оборони та клієнтів системи національної безпеки», – сказала вона. Інтригує фраза про «особливі рішення», яка вочевидь стосується чогось створеного на замовлення агентства для збору інформації. Зі слів офіційних осіб, знайомих із деталями угоди між Google і АНБ, компанія погодилася надавати АНБ інформацію про трафік у своїх мережах в обмін на розвіддані щодо іноземних хакерів. Послуга за послугу, інформація за інформацію. А з перспективи АНБ – інформація в обмін на захист.

Ця спільна угода та згадка про «особливе рішення» дозволяють упевнено припустити, що Google і АНБ розробили пристрій або технологію виявлення вторгнень у мережі компанії. Завдяки цьому АНБ могло б отримувати цінну інформацію для своєї так званої системи активного захисту, яка використовує комбінацію автоматичних сенсорів і алгоритмів для виявлення шкідливого ПЗ або ознак запланованої атаки і протидіє їм. Одна система під назвою «Паніка» (Turmoil) розпізнає потенційно небезпечний трафік. Потому інша автоматична система «Турбіна» (Turbine) ухвалює рішення, пропустити цей трафік чи заблокувати його. Остання система також може запропонувати програму для атаки або хакерську методику, яку оператор зможе застосувати для нейтралізації джерела шкідливого трафіку. Він може скасувати інтернет-з'єднання джерела трафіку або скерувати трафік на контрольований АНБ сервер. А там джерело можна інфікувати вірусом або шпигунською програмою, за допомогою якої АНБ надалі спостерігатиме за ним.

Для роботи систем Turbine і Turmoil АНБ потребувало інформації, зокрема про дані, які передаються в мережі. Компанія Google, що

має мільйони клієнтів у всьому світі, – це наче каталог користувачів інтернету. Компанія має адреси їхньої електронної пошти. Знає їхнє фізичне розташування під час входу в мережу. Знає, що саме вони шукають у мережі. Влада може наказати компанії надати цю інформацію, як робить це в рамках програми Prism, в якій компанія Google брала участь протягом року ще до того, як підписала угоду про співпрацю з АНБ. Однак саме цей інструмент використовують для розшуку людей, яких влада підозрює в терористичній діяльності або шпигунстві. Місія АНБ із забезпечення кіберзахисту передбачає ширше охоплення мереж у пошуках потенційних небезпек, інколи ще до того, як стане відомо, де саме розташоване джерело загроз. У користувацькій угоді компанія Google повідомляє своїх клієнтів про те, що може передавати їхні «персональні дані» стороннім організаціям, зокрема й державним агентствам, для «виявлення, запобігання або інших заходів у разі шахрайських дій, проблем безпеки або технічних питань», а також для «захисту прав, власності або безпеки Google». За словами людей, знайомих із деталями угоди між АНБ і Google, влада не має дозволу на читання електронних листів користувачів Google, утім може робити це в рамках програми Prism. Натомість угода дозволяє АНБ аналізувати апаратне й програмне забезпечення Google у пошуках уразливостей, якими можуть скористатися хакери. Зважаючи на те що АНБ є єдиним найбільшим охоронцем інформації про вразливості нульового дня, ця інформація може зробити Google безпечнішою за інші компанії, які не дають доступу до своїх найбільших секретів. Угода також дозволяє агентству аналізувати втручання, які вже відбулися, щоб відстежити джерело атак.

Компанія Google пішла на ризик, співпрацюючи з АНБ. Корпоративний девіз компанії «Не будь злим», здається, суперечить роботі з прикриття розвідувального кібервоєнного агентства. Але внаслідок цієї співпраці Google отримала корисну інформацію. Незабаром після викриття китайського втручання Сергію Бріну, співзасновникові компанії Google, надали тимчасовий допуск до секретної інформації, що дозволив йому брати участь у закритих нарадах, де обговорювалась операція проти його компанії. Державні аналітики виснували, що вторгнення координував підрозділ Народно-визвольної армії Китаю. Це була найдокладніша інформація про джерело вторгнення, яку компанія Google отримала. Ці дані допомогли їй посилити захист систем, заблокувати трафік для кількох інтернет-адрес і ухвалити

зважене рішення про те, чи варто продовжувати працювати в Китаї. Керівники Google зневажливо відгукувалися про «секретний складник» АНБ. Але коли компанію атакували, по допомогу вона звернулася до Форт-Міда.

Компанія Google розповіла у блозі, що в рамцях операції, яка згодом отримала назву Aurora за іменем файлу на комп'ютері нападників, китайські хакери атакували понад 20 компаній. А невдовзі одна компанія зі сфери інформаційної безпеки вирахувала, що об'єктів атаки було близько тридцяти. Насправді масштаби китайського шпигунства були і є значно більшими.

Експерти з безпеки, державні і незалежні, дали спеціальну назву хакерам, які стоять за такими атаками, як Aurora, націленими на тисячі різних компаній, що працюють практично в кожному секторі економіки США. Вони назвали таких хакерів «підвищеною постійною загрозою» (Advanced persistent threat – APT). Ця назва звучить загрозливо й має певний підтекст. Коли держслужбовці говорять про APT, найчастіше вони мають на увазі Китай, а якщо конкретніше, то хакерів, які працюють під керівництвом чи на замовлення китайської влади.

Слово «підвищена» у цьому описі почасти стосується хакерських методів, які анітрохи не поступаються за ефективністю методам АНБ. Китайські кібершпигуни використовують застосунки для спілкування та надсилання миттєвих повідомлень на зараженому комп'ютері, щоб з'єднатись із сервером, що контролює операцію. Вони інсталюють шкідливі програми, а потім віддалено вдосконалюють їх, додаючи нові можливості зі збору інформації. Державний апарат, що підтримує всю цю шпигунську діяльність, також «просунутіший» за розрізнені групи кібервандалов або таких активістів, як група Anonymous, які шпигують за компаніями в політичних цілях, або навіть за російські кримінальні групи, які найчастіше зацікавлені у викраданні банківських даних і номерів кредитних карт. Китай готовий до довготривалої операції. Керівники країни прагнуть, щоб економіка та промисловість сягнули максимального розвитку в досяжному майбутті, і ладні викрадати знання, необхідні для досягнення цієї мети. Ось що говорять американські можновладці.

В описі цієї загрози також варто звернути увагу на слово «постійна». Збір величезних обсягів інформації з багатьох джерел потребує максимальної концентрації, політичної волі й фінансових ресурсів, адже потрібно випробувати безліч різноманітних методів зламу, зокрема й дорогі експлойти нульового дня. Шпигуни, що знайшли плацдарм і облаштувалися в корпоративній мережі, не підуть самостійно, поки їх не викинуть силоміць. Але невдовзі вони повертаються. «Загроза» американській економіці полягає в утраті потенційних прибутків і стратегічних позицій. Водночас існує небезпека, що китайські військові знайдуть точки входу в системи управління критично важливими об'єктами інфраструктури США. Американські розвідники вважають, що китайські військові вже мають схему інфраструктурних мереж, тож, якщо дві держави зійдуться колись у двобої, китайці зможуть завдати удару по таких американських об'єктах, як електричні мережі або газові трубопроводи, не вдаючись до запуску ракет або відправки флотилії бомбардувальників.

Операція Aurora дозволила побіжно оцінити сферу використання експлойтів APT. Уперше, коли йшлося про китайські шпигунські операції, були названі конкретні компанії. «Масштаб цієї діяльності значно більший, ніж хтось будь-коли уявляв», – зізнався Кевін Мандіа, генеральний директор і президент розташованої неподалік Вашинґтона компанії Mandiant, що займається комп'ютерною безпекою і кримінальними розслідуваннями. APT – це хакерська діяльність стратегічного державного рівня. «Шкода була завдана не лише п'ятдесятьом компаніям. Тисячі компаній опинились у небезпеці. У справжній небезпеці. Прямо зараз», – сказав Мандіа, ветеран кіберрозслідувань, у минулому офіцер комп'ютерної безпеки ВПС, який розслідував кіберзлочини. Компанія Mandiant – це професійна організація, до якої звертаються компанії, коли виявляють, що в їхні комп'ютерні мережі проникли шпигуни. Незабаром після зламу Google під час закритої зустрічі з представниками Міністерства оборони компанія Mandiant оприлюднила деталі власного розслідування, яке відбулося за декілька днів до атаки.

APT – це не одна організація, а кілька хакерських груп, до яких входять не лише команди, що працюють на Народно-визвольну армію Китаю, а й так звані хакери-патріоти – ініціативні, підприємливі ентузіасти комп'ютерів, які хочуть служити своїй країні. У китайських університетах безліч студентів комп'ютерних спеціальностей, які по

закінченні навчання йдуть працювати у військові організації. Хакери APT вважають найбільшими чеснотами крутійство та терплячість. Вони використовують уразливості нульового дня й установлюють бекдори. Присвячують свій час ідентифікації співробітників у організації, на яку націлилися, відтак надсилають їм старанно складені фішинґові електронні листи, нашпиговані шпигунським ПЗ. Вони проникають в організацію і часто працюють там місяці або навіть роки, перш ніж хтось їх виявить, і весь цей час викачують схеми та креслення, читають електронні листи й переглядають вкладення, стежать за працівниками, що звільнилися, і новачками – своїми майбутніми цілями. Інакше кажучи, китайські шпигуни поводяться так само, як і їхні американські колеги.

Жодна розвідувальна організація не виживе, якщо не знатиме свого ворога. З такою розлогою мережею спостереження, якою є АНБ, інколи простіше отримати докладну інформацію про хакерські кампанії від самих об'єктів атаки. Ось чому АНБ співпрацює з Google. Ось чому представники влади вислухали приватних нишпорок компанії Mandiant, коли ті прийшли з інформацією про APT. Захист кіберпростору – складне завдання, навіть для найкращого в світі шпигунського агентства. Подобається це комусь чи ні, але АНБ і корпорації повинні боротися з ворогом спільно.

Сергій Брін з Google – лише один із сотень гендиректорів, допущених у таємне коло АНБ. З 2008 року агентство пропонує керівникам компаній тимчасовий допуск до секретної інформації, інколи лише на один день, щоб дозволити їм потрапити на закриті наради на тему кіберзагроз. «Вони пускають когось на один день і показують безліч розвідданих, пов'язаних із небезпеками, що загрожують бізнесу в Сполучених Штатах», – розповідає керівник телекомунікаційної компанії, якому доводилося відвідати кілька таких заходів, що відбуваються приблизно тричі на рік. Гендиректори мусять підписати угоду щодо нерозголошення будь-якої інформації, отриманої під час брифінґу. «Їм довго пояснюють: якщо порушуватимеш цю угоду, тебе заарештують, засудять і ти проведеш решту життя у в'язниці», – каже керівник.

Навіщо комусь погоджуватися з такими суворими вимогами? «На один-єдиний день вони ставали особливими й бачили те, про що мало кому відомо», – пояснює керівник телекомунікаційної компа-

нії, який завдяки регулярній роботі над секретними проектами мав високий рівень доступу до засекреченої інформації, зокрема й про найтаємніші операції АНБ, як-от незаконну програму стеження, яка запрацювала після терактів 11 вересня. Саме завдяки цим закритим зустрічам «Александер близько потоваришував із багатьма директорами компаній, – додає джерело. – Я був на деяких із цих зустрічей і якось сказав: "Генерале, ви розповідаєте цим хлопцям такі речі, витік інформації про які може загрожувати небезпеці країни". Але він відповів: "Я знаю. Але це зважений ризик. І якщо витік станеться, їм відомо про наслідки"».

Агентство залякувало керівників, щоб привернути їхню увагу до проблеми. Викриття агентства, що стосуються викрадених даних і ворожих уторгнень, жахають, і повідомляють їх навмисно. «Ми лякаємо їх до бісиків», – зізнався в інтерв'ю суспільній радіостанції один урядовець у 2012 році. Деякі з цих керівників після нарад про загрози виходили з таким самим відчуттям, як оті директори оборонних підприємств, які влітку 2007 року залишали Пентаґон «із сивим волоссям». Деякі розгублені директори, які не знали, як захистити підприємства, зверталися до приватних охоронних компанії, таких як Mandiant. «Я особисто знаю одного генерального директора, життя якого сильно змінилося після закритої наради в АНБ із питань кіберзагроз, – розповів Річард Бейтліч, старший офіцер безпеки Mandiant, в інтерв'ю суспільній радіостанції. – Генерал Александер посадив його в крісло і розповів, що відбувається. Саме цей генеральний директор, як на мене, повинен був знати про [загрози його компанії], але він не знав, і ця інформація змусила його переосмислити все, що він думав про цю проблему».

В АНБ і приватних охоронних компаніях склалися взаємовигідні відносини. Влада залякувала керівників, а ті бігли по допомогу до експертів, таких як Mandiant. Ці компанії, своєю чергою, ділилися з владою інформацією, отриманою в процесі розслідувань. Саме так учинила компанія Mandiant після проникнення в мережі Google у 2010 році. Натомість АНБ використовувало закриті брифінґи, щоб спонукати компанії зміцнювати системи захисту. Під час однієї зустрічі 2010 року представники агентства заявили, що виявили уразливі місця в біосі – вшитій пам'яті персональних комп'ютерів, яка керує її роботою. Цей недолік дозволяв хакерам перетворювати комп'ютер на «цеглину», зробивши його абсолютно неужитковим. Генеральних

директорів компаній, що виробляли комп'ютери, які були присутні на цій зустрічі, попередили своєчасно, отож вони виправили недолік.

Закриті наради на вищому рівні – це лише один зі способів, які використовувало АНБ для укладання союзів із корпораціями. Деякі секретні програми дозволяють компаніям ділитись інформацією про власні розробки з агентством, яке вишукувало в них потенційні вразливості, а іноді встановлювало бекдори або інші входи для доступу. Серед компаній, які розкривали АНБ інформацію про власні продукти, були виробники комп'ютерів, серверів і мережевих маршрутизаторів, розробники популярного програмного забезпечення (зокрема і Microsoft), постачальники послуг електронної пошти та інтернет-провайдери, телекомунікаційні компанії, виробники супутників, антивірусні компанії і розробники алгоритмів шифрування.

АНБ допомагало компаніям знайти вразливі місця в їхніх продуктах. Але також платило компаніям, аби ті не усували деякі з виявлених недоліків. Ці вразливості дозволяли агентству заходити в мережі й проводити там шпигунські операції або атаки на іноземні держави, які інсталювали ці продукти в комп'ютерах розвідувальних і військових організацій, а також на критично важливих об'єктах інфраструктури. За словами представників компанії й американських можновладців, Microsoft передавала АНБ звіти щодо вразливостей нульового дня в своїх програмних продуктах іще до оприлюднення офіційних попереджень і виходу програмних оновлень. Компанія Cisco, один із провідних світових виробників мережевого обладнання, залишала в маршрутизаторах бекдори, щоб американські агентства могли відстежувати роботу обладнання, як розповів фахівець у сфері кібербезпеки, який навчав співробітників АНБ технологій захисту. Компанія McAfee, що працює у сфері інтернет-безпеки, надсилала до АНБ, ЦРУ і ФБР потоки мережевого трафіку, результати аналізу ПЗ, а також інформацію про хакерські новинки.

Компанії, які обіцяють розкривати відомості про «діри» в безпеці власних продуктів лише шпигунським агентствам, отримують гроші за своє мовчання, як кажуть експерти й офіційні особи, яким ці угоди знайомі. Ба більше, оці шпарини, через які влада може стежити, – вимога законодавства. Скажімо, телекомунікаційні компанії зобов'язані проектувати своє обладнання так, щоб правоохоронні органи, які отримали дозвіл суду на стеження, могли прослуховувати розмови так само легко, як через лінії стаціонарного зв'язку. Але якщо

АНБ збирає інформацію за кордоном, ці закони вже не поширюються на агентство. Натомість спостереження за допомогою бекдорів і секретних уразливостей в обладнанні та програмному забезпеченні, до якого вдається АНБ, у багатьох країнах незаконне.

Звісно, бекдорами і вразливостями можуть скористатись і хакери. У 2010 році аналітик компанії IBM виявив недолік у системі безпеки операційної системи Cisco, завдяки якій будь-який хакер міг скористатися бекдором для правоохоронних органів. Хакер міг зламати обладнання Cisco і скористатись їм для відстежування всіх комунікацій, зокрема й вмісту електронних листів. Залишаючи вразливості у продуктах, у тому числі таких популярних, як програми Microsoft, компанії піддають небезпеці мільйони користувачів, а також електростанції, комунальні служби й транспортні системи.

Згідно з американським законодавством, влада зобов'язана щоразу попереджати компанії, якщо використовує їхні продукти, сервіси або обладнання для стеження та збору інформації. Деякі з цих угод щодо обміну інформацією відомі лише керівникам і кільком юристам. Вигода від такої співпраці може бути значною. Джон Чемберс, керівник Cisco, потоваришував із Джорджем Бушем за часів його президентських повноважень. У квітні 2006 року Чемберс і президент обідали в Білому домі разом із Генеральним секретарем Центрального комітету Комуністичної партії Китаю Ху Цзіньтао, а наступного дня Буш «підвіз» Чемберса президентським літаком до Сан-Хосе, де президент долучився до Чемберса у штаб-квартирі Cisco і взяв участь у панельній дискусії, присвяченій конкурентоспроможності американського бізнесу. До розмови також приєднався тодішній губернатор Каліфорнії Арнольд Шварценеґґер. Близькість до політичної влади – це вже нагорода. Але привілейовані компанії інколи також отримують від уряду завчасні попередження щодо небезпек, які їм загрожують.

Міністерство внутрішньої безпеки також проводить зустрічі з представниками компаній у рамцях власної ініціативи зі створення «міжгалузевих робочих груп». Ці зустрічі дозволяють керівникам із корпоративного світу, з якими влада ділиться інформацією, поспілкуватися один з одним і почути державних діячів. Учасники таких зустрічей часто мають допуск до секретної інформації й успішно пройшли перевірки на благонадійність. Міністерство оприлюднює

розклад і програму деяких зустрічей, однак не розкриває назви компаній-учасниць і зберігає в таємниці чимало подробиць обговорюваних питань. Від січня 2010 року до жовтня 2013-го, як стало відомо із відкритих джерел, влада організувала щонайменше 168 зустрічей із компаніями лише в рамцях ініціативи зі створення міжгалузевих робочих груп. А були ще сотні інших зустрічей за галузевим принципом: наприклад, енергетика, телекомунікації і транспорт.

Ці зустрічі виглядали так: «брифінґ про кіберзагрози» за участі влади, зазвичай представників АНБ, ФБР або Міністерства внутрішньої безпеки; останні новини щодо конкретних ініціатив, як-от підвищення безпеки банківських сайтів, спрощення процедури обміну інформацією між комунальними підприємствами або перелік шкідливого ПЗ; обговорення «інструментів» безпеки, розроблених державою та приватними компаніями, наприклад програм для виявлення в мережі хакерів. Одна з нарад у квітні 2012 року була присвячена «сценаріям обміну інформацією для активного кіберзахисту» – розробленому АНБ методу нейтралізації кіберзагроз іще до того, як вони призвели до збитків. І йшлося тут про інформаційний обмін не між державними службами, а між корпораціями.

На більшості зустрічей ішлося про захист промислових систем управління – під'єднаних до інтернету пристроїв контролю обладнання електростанцій, ядерних реакторів, банків та інших критично важливих інфраструктурних об'єктів. Ось чия вразливість у кіберпросторі найбільше непокоїла керівників розвідки. Ця саме та тема, яка так збадьорила Джорджа Буша у 2007 році, і саме її висвітлив у промові Барак Обама два роки потому. Розсекречені програми цих зустрічей дозволяють поглянути, як саме збираються захищати внутрішній кіберпростір компанії та держава.

23 вересня 2013 року Міжгалузева робоча група з питань безпеки обговорювала зміни, запропоновані в законопроекті «Зв'язок між оператором і оперативним центром уряду Сполучених Штатів» (Connect Tier 1 and USG Operation Center). Під Tier 1 мають на увазі провідних інтернет-провайдерів чи мережевих операторів. Деякі найвідоміші компанії США, ознаковані як Tier 1, – це AT&T, Verizon і CenturyLink. Абревіатура USG розшифровується як United States Government (уряд Сполучених Штатів). Вірогідно, ініціатива передбачала організацію каналу передачі даних між АНБ і цими компаніями й розширення пілотної програми DIB, санкціоноване в лютому

2013 року президентським наказом, покликаним підвищити рівень безпеки критично важливих об'єктів інфраструктури у країні. Влада передавала інформацію про загрози, здебільшого через АНБ, двом інтернет-провайдерам – AT&T і CenturyLink. А ті продавали «розширені послуги кіберзахисту» компаніям, визначеним як життєво важливі для національної та економічної безпеки держави. Цією програмою номінально керує Міністерство внутрішньої безпеки, але саме АНБ надає інформаційну підтримку й забезпечує технічну експертизу.

Завдяки обмінові інформацією держава створила бізнес на кіберзахисті. Компанії AT&T і CenturyLink фактично стали приватними охоронцями, які продають захист обраним корпораціям і промисловим підприємствам. AT&T має одну з найдовших історій співпраці з державою у сфері нагляду. Після терактів 11 вересня компанія однією з найперших зголосилася передавати АНБ записи про дзвінки клієнтів, щоб агентство могло проаналізувати їх задля пошуку потенційних зв'язків із терористами, – ця програма співпраці триває донині. Більшість телефонних дзвінків у Сполучених Штатах здійснюється за допомогою устаткування AT&T, хоч би з якої мережі виходив виклик. Інфраструктура компанії є одним із найважливіших сховищ електронної інформації, яку часто відстежує АНБ і американські правоохоронні органи.

Про компанію CenturyLink зі штаб-квартирою у місті Монро у розвідувальному співтоваристві тривалий час було відомо не надто багато. Проте 2011 року вона придбала телекомунікаційну фірму Qwest Communications, з якою АНБ було знайомо навіть дуже добре. Ще до терористичної атаки 11 вересня представники АНБ виходили на керівників Qwest і просили їх надати доступ до високошвидкісних оптоволоконних мереж для стеження та виявлення потенційних кібератак. Компанія категорично відмовилася, позаяк представники агентства не мали судового дозволу на отримання доступу до обладнання компанії. Після терористичної атаки АНБ знову звернулося до Qwest із проханням передати записи телефонних розмов клієнтів компанії без судової санкції, як це зробила AT&T. Але компанія знову відмовила. Лише 10 років потому, після продажу компанії, мережі Qwest стали частиною розширеного апарату безпеки АНБ.

Перелік корпоративних потенційних клієнтів на поширювану державою кіберрозвідувальну інформацію такий самий строкатий, як економіка США. Щоб отримати цю інформацію, компанія повинна

відповідати державному визначенню критично важливого об'єкта інфраструктури: «майно, системи й мережі, фізичні чи віртуальні, такі життєво необхідні США, що виведення їх із ладу або знищення матиме руйнівний вплив на безпеку, державну економічну безпеку, національну систему охорони здоров'я, безпеку громадян або їхню сукупність». Це визначення здається вузьким, проте категорії критично важливих об'єктів інфраструктури доволі численні й охоплюють тисячі різних напрямів діяльності. Офіційно існує 16 секторів: хімічна промисловість; комерційні підприємства, серед яких торговельні центри, спортивні заклади, казино та парки відпочинку; лінії зв'язку; основні промислові підприємства; греблі; індустріальна база військового комплексу; служби надзвичайних ситуацій, такі як служби оперативного реагування та пошуково-рятувальні служби; енергетичні підприємства; заклади охорони здоров'я; інформаційні технології; ядерні реактори, матеріали й відходи; транспортні системи; системи водопостачання та каналізації.

Важко повірити, що кожну компанію з цього переліку можна вважати аж такою «життєво необхідною для Сполучених Штатів», що збій в її роботі або її зупинення завдасть удару по національній безпеці та здоров'ю нації. Однак за роки, що минули після терактів 11 вересня, держава розкинула таку розлогу захисну мережу, що практично кожну компанію можна було назвати критично важливим об'єктом інфраструктури. Влада не розкриває інформації про те, які саме компанії попереджає про кіберзагрози. І участь у програмі досі залишається добровільною. Проте законодавці та деякі представники розвідслужб, зокрема Кіт Александер та інші співробітники АНБ, тиснули на Конгрес, вимагаючи врегулювати стандарти кібербезпеки для власників і операторів критично важливих об'єктів інфраструктури. Якби це сталося, влада могла б вимагати від будь-якої компанії – від Pacific Gas & Electric до Harrah's Hotels and Casinos – погоджуватися на державну допомогу, ділитися з розвідкою інформацією про клієнтів і вибудовувати кіберзахист згідно з державними стандартами.

У 2013 році головний радник Пентаґону з питань кібербезпеки, генерал-майор Джон Дейвіс заявив у своїй промові, що Міністерство внутрішньої безпеки і Міністерство оборони працювали пліч-о-пліч над планом розширення оригінальної програми DIB на інші сектори економіки. Планували почати з енергетики, транспорту та нафтогазової галузі – з секторів, «критично важливих для місії Міністерства обо-

рони, державної економіки та державної безпеки, які ми не можемо контролювати безпосередньо», – казав Дейвіс. Розкриття структури цих систем і потенційні хакерські атаки на них генерал-майор назвав «постійною загрозою». Держава ніколи не зможе охопити всі компанії всебічним захистом самостійно. Вона не здатна зробити цього зараз, ось чому покладається на співпрацю з AT&T і CenturyLink. Значно більше компаній звернеться по допомогу до держави, щойно та розширить периметр кібернетичного захисту. Потенційний ринок для послуг у сфері кібербезпеки практично безмежний.

12
ВЕСНЯНЕ ПРОБУДЖЕННЯ

Сполучені Штати ще жодного разу не потерпали від масштабних кібератак, які б призвели до серйозного збою в роботі критично важливих об'єктів інфраструктури. Але на початку 2012 року частина представників влади захвилювалася, вирішивши, що те, чого вони так довго боялися, ось-ось станеться.

У березні того самого року принаймні 20 компаній, що обслуговують газові трубопроводи в США, звернулися до Міністерства внутрішньої безпеки, щоб зголосити підозрілі електронні листи, надіслані співробітникам цих компаній. Здавалося, що це листи начебто від колег, яких вони добре знали або могли знати завдяки специфіці своєї роботи – стандартний фішинґ. Деякі співробітники – досі невідомо, скільки саме, – відкрили повідомлення й вивільнили шпигунське ПЗ у корпоративні мережі операторів трубопроводів. Хакери не отримали доступу до систем управління трубопроводами, проте підійшли небезпечно близько. Якби оператори користувалися внутрішньою системою без зв'язку з інтернетом, імовірно, небезпека їх би оминула. Звісно, ризик того, що співробітник може принести шкідливе ПЗ на USB-носієві, все-таки існує.

Вищі посадові особи з ФБР, АНБ і Міністерства внутрішньої безпеки забили на сполох. Хакер, який здобуде контроль над трубопроводами, може перешкодити потокові природного газу або вивести з ладу систему управління, що призведе до аварії, ба навіть вибуху. Мережа газових труб США має протяжність понад 300 тисяч кілометрів, а природний газ – це приблизно третина енергоресурсу для постачання країни. Досі не було жодної підтвердженої кібератаки, яка б пошкодила труби. Проте подейкують, що під час холодної війни ЦРУ встановило шкідливе ПЗ на обладнанні трубопровідної системи Сибіру, де 1982 року стався вибух. Теоретична можливість віддаленої зміни тиску в трубах існує – подібну атаку АНБ уже проводило на іранському атомному підприємстві.

Щойно газові компанії повідомили уряд про зондування, пред-

ставники влади надіслали на підприємства «леткі» команди й зібрали необхідну інформацію з жорстких дисків і системних логів*. Джерело електронних листів простежили до початків однієї операції, яка, за словами аналітиків, почалася ще в грудні 2011 року. Попередження від компаній щодо виявлення шпигунів «нескінченні», каже колишній співробітник правоохоронних органів, який опікувався цією проблемою. Проте аналітики не могли скласти цілісної картини операції. Чи то хакери хотіли зібрати інформацію про конкурентів у трубопровідному бізнесі, наприклад про пошук нових постачальників газу чи будівництво нових установок? А може, вони намагалися перешкодити безперервному постачанню природного газу, інсталюючи шкідливу програму, здатну у визначений день знищити трубопровід?

Аби це з'ясувати, державні слідчі вирішили не оприлюднювати заяв, а тихо спостерігати за «гостями», щоб дізнатися, за чим саме вони полюють. Це був ризикований хід. Хакери могли щомиті розпочати нищівну атаку на корпоративні мережі й украсти або стерти цінну інформацію. А був іще шанс, щоправда незначний, що об'єктом атаки стануть саме трубопроводи, а це спричинило б катастрофічні економічні наслідки і навіть могло б призвести до загибелі людей біля місця вибуху. Представники влади провели закриті зустрічі з обраними компаніями та повідомили їм те, що вже знали. Вони поділилися з персоналом, що опікується корпоративною безпекою, «стратегіями зменшення заподіяної шкоди», повідомляючи адреси електронної пошти, з яких були надіслані фішинґові повідомлення, і конкретні IP-адреса, доступ до яких слід було заблокувати. Проте влада не звільнила мережі від шпигунів і не сказала компаніям, як це зробити. 29 березня група екстреного реагування з Міністерства внутрішньої безпеки, що працює спільно з АНБ, оприлюднила на секретному урядовому сайті попередження для всіх операторів трубопровідних мереж, в якому наказувала дозволити шпигунам шукати інформацію, яка їх цікавить, і не втручатися, поки їхні дії не загрожують роботі трубопровідної системи. Державні діячі з Вашинґтона попередили торговельні асоціації, що представляють інтереси нафтогазових компаній, і наказали тримати деталі операції у таємниці.

Реакція на проникнення в систему контролю трубопроводів про-

* Лоґ – файл, в якому накопичується службова та статистична інформація про події в системі.

демонструвала новий, значно вищий рівень впливу влади на кібероборону в енергетичному секторі. Газові компанії та їхні лобісти у Вашинґтоні дотримувалися вказівок та інструкцій державної влади. Майже весь час розслідування владі вдалося успішно тримати інформаційну блокаду ЗМІ. Серйозна хакерська кампанія проти життєво важливих об'єктів інфраструктури тривала вже декілька тижнів, і майже ніхто про неї не знав. Новини про проникнення в мережу з'явилися лише у травні, через два місяці після початку державної розвідувальної операції.

Втручалася держава й в інші галузі енергетики. Того літа Міністерство внутрішньої безпеки і Міністерство енергетики провели секретний брифінґ із питань кіберзагроз для гендиректорів електроенергетичних підприємств, пропонуючи їм тимчасовий допуск до закритої інформації, щоб надати більше інформації про загрози для галузі. Енергетичні компанії знали про небезпеки, що чатують у мережах, значно менше за компанії з інших галузей економіки, як-от фінансові організації, які регулярно ділилися одна з одною інформацією та створили систему для обміну повідомленнями щодо вторгнення й нові методи атак секретних мереж. Натомість енергетичні компанії боялися здаватися слабкими в очах конкурентів і надавати тим інформацію про майбутні стратегії, зізнавшись у власних проблемах з кіберзахистом.

Але урядовці втрачали терпець. Прибічники нового закону, покликаного регулювати стандарти кібербезпеки для комунальних компаній, продовжували проштовхувати його у Конгресі, арґументуючи необхідність закону зливою хакерських атак на газові компанії. Восени їхні плани зазнали поразки, второвуючи шлях для наказів Обами, покликаних зміцнити всі можливі способи кіберзахисту. Влада заохочувала компанії дотримуватися стандартів безпеки та методів захисту, розроблених Національним інститутом стандартів і технологій після консультацій із величезною групою промислових експертів і розвідників. Компанії могли проігнорувати поради влади. Але якщо б превентивна кібератака призвела до пошкодження інфраструктури, керівників компанії могли б притягнути до цивільної, ба навіть кримінальної відповідальності і їм довелося б пояснювати у суді, чому вони вирішили відбивати удар самостійно.

2012 року, у розпалі кібератак на газопровідні компанії, влада провела закриті брифінґи для майже 700 працівників комунальних

підприємств. У червні 2013 року Міністерство внутрішньої безпеки, ФБР, Міністерство енергетики та Агентство безпеки транспорту почали так звану активну кампанію з ознайомлення підприємств «з контекстом загроз і стратегіями зменшення заподіяної шкоди», – ішлося в інформаційному бюлетені Міністерства внутрішньої безпеки. В рамцях кампанії закриті наради відбулися щонайменше в десяти американських містах, зокрема, у Вашинґтоні, Нью-Йорку, Чикаґо, Далласі, Денвері, Сан-Франциско, Сан-Дієґо, Сіетлі, Бостоні, Новому Орлеані та в «багатьох інших за допомогою захищеного відеозв'язку». Енергетичні підприємства почали навчати своїх працівників основ кібербезпеки. Shell, Schlumberger та інші великі компанії надсилали персоналові фальшиві фішинґові електронні листи з фотографіями милих котиків та іншими привабливими картинками. Експерти, що проводили навчання, кажуть, що майже всі працівники спочатку ловилися на такі повідомлення, але після тренінгу майже 90 % навчилися не відкривати посилання та вкладені файли, які зазвичай запускають установку шкідливого ПЗ.

Натомість представники АНБ продовжували наполегливо вимагати збільшення повноважень для розширення своєї оборонної мережі. У травні 2013 року, під час одного з небагатьох своїх публічних виступів у Вашинґтоні, Чарлз Берлін, директор Оперативного центру національної безпеки АНБ, озвучив поширену в колах американської розвідки думку, згідно з якою, якщо агентство зосередиться лише на захисті державних комп'ютерних мереж і інформації, це «майже аморально». «Місія Міністерства оборони… [полягає] у захисті Америки», – сказав Берлін, що очолював мозковий центр агентства із радіотехнічної розвідки та захисту комп'ютерних мереж. «Я багато років простояв на мурі фортеці, виливаючи киплячу олію на нападників, – говорив він. – Ми більше не здатні захистити Америку».

Тривожною весною 2012 року співробітники правоохоронних органів, розвідувальних і приватних охоронних служб майже не сумнівалися в походженні хакерів. Проте залишалося одне запитання: яка в них мета?

Колишній співробітник правоохоронних органів, що працював над цією справою, каже, що хакери перебували в Китаї і що ця атака була частиною масштабної стратегії Китаю зі складання карти критично важливої інфраструктури Сполучених Штатів. Досі не зрозумі-

ло, яке завдання виконували хакери: просто шпигували чи готували ґрунт для кібервійни. Проте ці дві діяльності пов'язані одна з одною: щоб здійснити атаку на об'єкт, треба спочатку скласти схему інфраструктури та зрозуміти її вразливі місця. За всіма ознаками китайці шукали саме такі вразливі місця. За кілька місяців після виявлення втручання в мережі газових підприємств, канадська технологічна компанія Telvent, яка виробляє системи управління промисловими об'єктами і SCADA-системи, використовувані в Канаді та США, заявила, що хакери, ймовірно з Китаю, відстежували її мережевий трафік.

Кібервійна зі Сполученими Штатами не лежить у площині зацікавлень Китаю. На відміну від економічної конкуренції. Країна відчуває нагальну потребу дізнатись якнайбільше про джерела енергії американських компаній і про те, як цю енергію планують отримувати. Почасти це підтримало б китайські амбіції в енергетичній сфері. Водночас країні також потрібно підтримувати стрімкий темп розвитку економіки, бо, хоч він і сповільнився протягом останніх кількох років, ВВП Китаю від 2009 до 2013 рік збільшився на 7,8 %.

Китай шукає заміну традиційним джерелам викопних видів палива. Країна здебільшого використовує поклади вугілля, і про це передусім свідчить погана якість повітря в багатьох китайських містах. Китай – це друга країна світу за обсягами споживання вугілля, на яку припадає близько половини світового обсягу споживаного вугілля. Виробництво нафти в Китаї досягло максимальної позначки, тож влада шукає додаткові підводні родовища, а також переходить на чистіші джерела палива з багатшими запасами.

Щоб у майбутньому забезпечити Китай джерелами енергії, державні компанії зацікавлені у видобутку природного газу, який досі становить мізерну частку в енергоспоживанні країни – лише 4 % у 2009 році. Проте, щоб здобути цей газ, Китаю потрібно опанувати технологію гідравлічного розриву пластів і методи горизонтального буріння, розроблені й уперше впроваджені американськими компаніями. Звіт за 2013 рік, складений аналітиками кібербезпеки з фірми Critical Intelligence, висновує, що «китайські опоненти» сканували мережевий трафік енергетичних компаній США з метою викрадання інформації про методи гідравлічного розриву й видобутку газу. Автори зауважили, що китайські хакери цілилися здебільшого у компанії, що виробляють такі нафтопродукти, як пластмаса, і використовують

як основну сировину природний газ. Проникнення у комп'ютери газових підприємств у 2011–2012 роках могло бути пов'язане з цими завданнями, наголошують аналітики.

Але Китай не планує відмовлятися від традиційних джерел енергії. За даними розробника антивірусів – компанії McAfee, 2009 року відбулася серія кібервторгнень у мережі американських нафтових компаній, метою яких було викрадання інформації про родовища нафти у різних куточках земної кулі. Китай є другим найбільшим споживачем нафти у світі після США, а з 2009 року – ще й другим найбільшим імпортером нафти. Принаймні одна американська енергетична компанія, що збиралася бурити у спірних водах, які Китай вважав своїми, зазнала атаки китайських хакерів.

Китай вступає у конкурентну боротьбу за природні ресурси й водночас намагається збудувати державну енергетичну індустрію. Саме тому китайці активно атакують американські енергетичні компанії та промислові об'єкти. У 2012 році Міністерство внутрішньої безпеки оприлюднило інформацію про 198 атак на життєво важливі об'єкти інфраструктури, що на 52 % більше, ніж попереднього року. 40 % цих атак були скеровані проти енергетичних компаній. Якщо б США опинилися в стані війни з Китаєм, безсумнівно, збройні сили цієї країни спробували б скористатися кіберплацдармами, створеними хакерами в мережах американських енергетичних компаній, і знищити або вивести з ладу критично важливі інфраструктурні об'єкти. Але в найближчому майбутньому Китай навряд чи буде сильно зацікавлений у тому, щоб завдавати збитків економіці США або знеструмлювати країну. Китай – один із найбільших іноземних кредиторів і найважливіший торговельний партнер США, тому безпосередньо зацікавлений у відмінному здоров'ї американської економіки та купівельній спроможності американських споживачів. Тому Китай шукає законні стежки до отримання інформації про пошуки джерел енергії в Сполучених Штатах і вивчення американських технологій: з 2010 року країна інвестувала понад $17 млрд у нафтогазовий бізнес США і Канади.

Отже, Китай веде подвійну гру – вкладає кошти в американські компанії й водночас краде в них інформацію. Цей шлях вельми сумнівний. Якщо китайські викрадачі американської інтелектуальної власності зроблять ці компанії менш конкурентоздатними на світовому ринку, американська економіка зазнає збитків, а отже, зазнає

їх і Китай. Фахівці американської розвідки виснували, що ця країна навряд чи припинить кіберкампанію, поки американці не чинять дипломатичного тиску й не вводять економічних санкцій. Тому уряд, намагаючись захистити критично важливу інфраструктуру, вдався до агресивніших політичних дій: наприклад, ухвалив рішення щодо захисту і моніторинґу газових трубопроводів у 2012 році. Єдине, що заспокоює фахівців із національної безпеки, – це те, що досі не виявлено жодних ознак того, що Китай прагне перейти від шпигунства до бойових дій.

Однак цього не скажеш про інших противників США.

Із вересня 2009 року американських банкірів регулярно турбують кібератаками певного виду. Хакери полюють не на гроші банків, а на сайти, за допомогою яких клієнти можуть управляти своїми рахунками, перевіряти баланс, оплачувати послуги й здійснювати грошові перекази. Хакери перенавантажують банківські сервери трафіком із підконтрольних комп'ютерів, надсилаючи безліч одночасних запитів, що «вбиває» сайти. Десятки банків зазнавали таких атак, що призводить до збою в роботі. Серед них Bank of America, Wells Fargo, Capital One, Citigroup, HSBC та інші відомі та менш знані фінансові інституції.

Банки, так само як безліч інших компаній, що ведуть бізнес у мережі, вже стикалися з DDOS-атаками і раніше. Більшість експертів у сфері безпеки вважають такі атаки лише прикрою неприємністю і аж ніяк не загрозою, наслідки якої зазвичай можна усунути впродовж кількох годин. Проте одна атака стала безпрецедентною за масштабом і складністю. Нападники створили величезні комп'ютерні мережі, з яких відправляли на сервери банків неймовірно велику кількість запитів. За однією оцінкою, потік даних у декілька разів перевищував трафік, який 2007 року російські хакери скерували на естонські комп'ютери, що призвело до збою в усій системі електронної інфраструктури країни, – це була найбільш нищівна кібератака в історії. Банківські інтернет-провайдери доповіли, що на жоден сайт іще ніколи не спрямовували такий величезний трафік. Жертвами хакерів стали дата-центри («хмари»), що складаються з тисяч серверів. Це наче противник відправив на знищення однієї цілі не кілька кораблів, а цілу армаду.

Аналітики змогли відстежити кілька джерел трафіку й дізнатись

інтернет-адреси. Провайдери блокували ці джерела, але потік запитів просто почав надходити з інших місць. Так само як у випадку атаки на мережі газових компаній, вищі керівники держави занепокоїлися. Проте цього разу влада стикнулася з агресивнішим ворогом. Шпигуни, що проникли в мережі газових компаній, здається, бажали лише отримати інформацію, а не знищувати газові трубопроводи. Натомість хакери, що атакували банки, хотіли перешкодити банківським операціям і викликати паніку серед клієнтів і в банківському секторі загалом. Ця стратегія спрацювала навіть краще, ніж було заплановано. Банківські працівники, що відповідали за безпеку, були в паніці через обсяг трафіку, яким їх атакували, як розповідали колишні держслужбовці, що брали участь у відбитті атаки на банківські сервери. «Протягом перших двох-трьох тижнів доводилося працювати до пізньої ночі», позаяк влада намагалася відстежити джерело атаки й зрозуміти її причини, розповідав Марк Везерфорд, що обіймав тоді посаду помічника заступника міністра внутрішньої безпеки з питань кібербезпеки, тобто був головною людиною у сфері захисту від кіберзагроз.

У цієї атаки була ще одна особливість, яка непокоїла, – вона не припинилася після першого удару. Нападники, які називали себе бригадами Із ад-Дін аль-Кассам (Izz ad-Din al-Qassam), дедалі атакували банки, вишукуючи нові цілі. Вони продовжили свою роботу й наступного року. У 2013 році АНБ ідентифікувало близько двохсот нових атак цієї ж групи на банківські сайти. Нападники проголошували себе групою антиамериканського комітету, яка завдає ударів на знак помсти за випуск любительського онлайн-відео «Невинність мусульман», в якому пророка Магомета зобразили кровожерним педофілом, що викликало хвилю протестів на Близькому Сході. Проте американські розвідники підозрювали, що це лише прикриття, а хакери насправді працюють на уряд Ірану і, вірогідно, мстяться за кібератаки на атомні підприємства в Нетензі.

Протягом останніх років агентства американської розвідки спостерігали за створенням іранської кіберармії. Лідери іранського Корпусу вартових революції, що володіли найбільшою телекомунікаційною компанією в Іраку, не приховували намірів створити кіберармію, яка зможе змагатися з США. Аналітики вважали, що іранська кіберармія збільшується і що до неї входять не лише розвідувальні та військові підрозділи, а й групи патріотичних «хактивістів».

Згідно зі звітами розвідки, влада Ірану з 2011 року витратила понад мільярд доларів на розвиток оборонних і наступальних кіберресурсів у відповідь на атаки «хробаком» Stuxnet, а також двома іншими комп'ютерними вірусами, які заражали комп'ютерні системи Ірану і, на загальне переконання, були справою рук американських та ізраїльських спецслужб.

Лише держава мала достатні фінансові та технічні ресурси, а також досвід і мотив для проведення операції проти банків, виснували американські можновладці. «Масштаб і складність атак не вкладалися в жодні рамці. Цього не міг зробити один парубійко з якогось підвалу», – твердить Везерфорд.

Те, що спочатку здавалося звичайною DDOS-атакой, виявилося потенційною міжнародною кібервійною небачених масштабів. Американські державні діячі вищого рангу ставили запитання: чи можуть Сполучені Штати розпочати кібератаку у відповідь на дії Ірану? Вони обговорювали, чи призведе атака на іранську критично важливу інфраструктуру до припинення хакерської активності та чи буде така контратака законною? На це запитання не існувало однозначної відповіді. Банки належали до критично важливих об'єктів інфраструктури, за визначенням самого уряду. Але хакери атакували сайти банків, а не системи управління міжбанківськими транзакціями й не системи зберігання банківської інформації. Це був не той жахливий сценарій, що його змалював Майк МакКоннелл для президента Буша в 2007 році. Везерфорд розповів, що керівник Міністерства внутрішньої безпеки, який відповідав за невідкладні дії у надзвичайних ситуаціях, не запропонував жодного виходу: «Він сказав: "У нас немає сценарію для таких ситуацій"».

Влада почала непокоїтися, що DDOS-атака такого самого масштабу, націлена на корпоративні комп'ютерні мережі, не лише спричинить тимчасові незручності, а й може призвести до фізичних руйнувань. Американські держслужбовці щодня контактували з банками та їхніми провайдерами. Хакери повідомляли про дату запланованих кібератак на онлайн-форумах. І щоразу банки та влада готувалися до нападу. «Інтернет-провайдери й уряд серйозно непокоїлися, що можуть зазнати поразки, – каже Везерфорд. – І що можуть постраждати інші критично важливі об'єкти інфраструктури й інтернет у цілому».

Після повідомлення групою Із ад-Дін аль-Кассам про наступну заплановану атаку керівник відділу безпеки провайдера поставив запитання Везерфордові, та й уряду загалом. «Що ви робитимете, хлопці? – запитав він. – Атака почнеться у будь-яку мить і матиме наслідки для всієї держави. Як учинить уряд?»

Везерфорд намагався переконати його, що ситуація під контролем, хоча й знав, що жодного контрнаступу не передбачено. Везерфорд вважав, що АНБ надто зволікає з розсекречуванням даних щодо загрози, яки могли б захистити банки. Агентство мусило «відчистити» інформацію, приховати джерела та методи, за допомогою яких здобували дані, до того як передати їх у Міністерство внутрішньої безпеки, яке своєю чергою зробить їх доступними для провайдерів. Везерфорд розповів, що телефонував у АНБ щодня й переконував якнайшвидше обробити розвіддані, щоб встигнути передати їх компаніям до початку нової атаки. «Для обробки інформації потрібно було шість годин. Але й сама атака могла тривати лише шість годин», – каже він.

Група високопоставлених фінансистів тиснула на представників АНБ під час особистих зустрічей. Вони хотіли знати, чому уряд не атакує джерело шкідливого трафіку й не виведе його в офлайн подібно тому, як для знищення ворожого табору запускає ракету. Представники АНБ відповідали, що кіберзброя, насамперед тисячі експлойтів нульового дня, тримають на випадок загрози державі або початок війни. «Щойно ми скористаємось одним із них, ми ніколи не зможемо застосувати його знову, – сказав один посадовець, як розповідає фінансовий керівників, що брав участь у тій нараді. – Ви справді хочете, щоб ми змарнували оцю зброю тому, що ваші сайти не працюють?»

Керівники відступили.

Атаки на банки стали перевіркою намірів держави. АНБ і військові не застосують силу, поки нападники не загрожуватимуть інфраструктурі транзакцій фінансового сектора або не почнуть знищувати дані рахунків, роблячи їх ненадійними. Держава відповість лише на кібератаку, що завдасть руйнівного удару по різних верствах суспільства. Злам сайту, хоч би яким брутальним він був, – не привід для початку війни. Так само як шпигунські дії.

Банки – та й інші компанії, які постраждали внаслідок дій іноземних кібернападників і мародерів, – ставили очевидне запитання: якщо держава не збирається їх рятувати, то хто це зробить?

13
ОБОРОННИЙ БІЗНЕС

За неповних 50 кілометрів од ділового центру Вашинґтона, на околиці міста Ґейтерсберґа (штат Меріленд), уздовж жвавої вулиці поблизу транспортного агентства й крамниці іграшок Toys «R» Us розташувалася присадкувата офісна будівля. Двоє охоронців на прохідній – перша ознака того, що це не якийсь там склад чи звичайний офісний центр. У майже позбавленому вікон крилі будівлі площею 7 тисяч кв. м розташований центр кіберспостереження. Декілька десятків аналітиків і дослідників шкідливого ПЗ моніторять трафік у глобальній розподіленій мережі комп'ютерів і серверів, на яких зберігається частина найсекретнішої інформації Сполучених Штатів, зокрема схеми реактивних винищувачів, систем управління ракетами та супутниками-шпигунами. Проте цей об'єкт, який вельми нагадує надсекретні об'єкти у Форт-Міді або Пентаґоні, ані належить владі, ані підпорядковується їй. Розташована тут компанія NexGen Cyber Innovation & Technology Center (це повна назва) належить компанії Lockheed Martin – найбільшому оборонному підрядникові країни. Тут і в подібних центрах у Денвері, Фарнборо (Велика Британія) і Канберрі (Австралія) компанія, яка зробила своє ім'я на розробці систем озброєння, створює новий бізнес у сфері кіберзахисту.

Проблему кібербезпеки Lockheed вивчила на власній шкірі, коли 2006 року мережі компанії атакували китайські хакери, що викрали креслення Єдиного ударного винищувача. Компанія є найбільшим постачальником товарів і послуг у сфері інформаційних технологій для цивільних і розвідувальних агентств, а також для військових структур і саме тому становить бажану ціль для хакерів. Після кібератаки 2006 року компанія впродовж кількох років досліджувала методи й технології, використовувані хакерами для проникнення в секретні системи та крадіжки державних таємниць. Молодий аналітик Lockheed Ерік Гатчінз дізнався, що деякі військові льотчики використовують термін «убивчий ланцюг» (kill chain), щоб описати

всі поступові кроки до відкриття вогню – від ідентифікації мети до визначення її географічного положення. Гатчінзу спало на гадку, що спритні хакери, які намагаються проникнути в комп'ютерні мережі Lockheed, також слідують певній покроковій моделі: вишукують цілі, готують шкідливе ПЗ, запускають фішинґову атаку і, врешті-решт, крадуть дані. Разом із двома колегами він адаптував військову концепцію та взяв «убивчий кіберланцюг» (cyber kill chain) за основу для оборонної стратегії Lockheed, призначеної для захисту не лише мереж компанії, а й мереж деяких державних замовників, а також банків, фармацевтичних компаній і щонайменше 17 комунальних підприємств, які обмінюються інформацією з компанією та дозволяють їй сканувати власний трафік у пошуках загроз.

Модель «убивчий кіберланцюг» складається з семи різних етапів, більшість яких залишає можливість заблокувати вторгнення або атаку до їхнього початку. Перший етап – це стеження. Компанія Lockheed відстежує ключові слова у пошукових запитах різних пошукових систем, які виводять користувачів на сайт компанії. Для вдалої фішинґової атаки хакери вишукають у прес-релізах і на вебсторінках компанії імена співробітників. Потому вони визначають, якими програмами користуються менеджери, що працюють над конкретними державними замовленнями. Вони слідкують за публічними виступами керівників, щоб створити достовірний електронний лист із посиланням на якийсь запланований захід. Компанія попереджає своїх співробітників, які можуть стати потенційними жертвами атаки, про особливу пильність, з якою треба відкривати вкладення в електронних листах, і про небезпеку натискання на лінки.

На другому етапі, який в Lockheed називають «озброєння», аналітики шукають очевидні кримінальні докази присутності шкідливого ПЗ: наприклад, заражений pdf-документ, прикріплений до електронного листа. У Lockheed ведуть базу даних усіх заражених pdf-файлів, що будь-коли потрапляли на очі аналітикам компанії, і ця інформація використовується у програмі автоматичного сканування всіх електронних листів, отриманих співробітниками компанії, і відправки у карантин листів, які можуть бути заражені шкідливим ПЗ.

«Убивчий ланцюг» містить такі етапи: «доставка» (надсилання шкідливої програми через електронну пошту або інфікований USB-носій); «експлойт», під час якого аналітики приділяють пильну увагу пошукові вразливості нульового дня (Гатчінз каже, що вони виявили

принаймні три експлойти, направлені на вразливості у продуктах компанії Adobe); «установка» на комп'ютер; «управління і контроль» комунікацій із вузловим комп'ютером і, нарешті, «відпрацьовування об'єкта» (викрадання файлів, видалення даних або знищення елементів фізичного устаткування). На останньому етапі хакер представляє максимальну загрозу. Якщо аналітики Lockheed зауважують таку активність, вони миттєво повідомляють керівництво компанії, яку атакують. Хакери, виявлені на ранніх етапах «ланцюга», скажімо, на третьому етапі, несуть менше загрози, бо їм потрібно пройти ще кілька кроків, перш ніж вони зможуть заподіяти шкоду. Якщо аналітики виявили, що хакер намагається заразити комп'ютери за допомогою зовнішніх носіїв, компанія може запрограмувати свої системи так, щоб заборонити виконання комп'ютерних програм з будь-яких USB-носіїв. Що раніше Lockheed або інша компанія, яка використовує модуль «убивчого ланцюга», інсталює захист, то в більшій безпеці опиниться.

За допомогою цієї моделі Lockheed могла завчасно попереджати своїх клієнтів про потенційні вторгнення, за словами віце-президента з питань кібербезпеки, генерала у відставці Чарлі Крума. Компанія не називає замовників, тому це твердження перевірити неможливо. Але концепція здається логічною. Однак чимало експертів з кібербезпеки, серед яких і ті, що працюють на конкурентів Lockheed, говорять, що ця оприлюднена 2011 року концепція почала новий етап в еволюції кіберзахисту. «Убивчий ланцюг» розбивав процес вторгнення на окремі дії та етапи, кожен з яких дозволяв заблокувати противників. А захисники мереж могли ефективніше керувати ресурсами, позаяк їм не доводилося реагувати на кожне попередження як на екстрену ситуацію. Це була концептуальна схема, яка дозволяла збудувати лінії захисту на значній віддалі від об'єкта атаки й заблокувати нападників, поки вони не підійшли впритул.

Ця концепція була важлива ще з однієї причини: її розробила корпорація, а не державне агентство. Гатчінз, який у 34 роки обійняв посаду головного інформаційного аналітика Lockheed, ніколи не працював на державу й ніколи не служив у збройних силах. Фактично він навіть не працював на жодну іншу компанію, крім Lockheed, в яку прийшов 2002 року, щойно отримавши освіту в сфері комп'ютерних наук у Вірґінському університеті. У Lockheed працює багато колишніх держслужбовців і армійських офіцерів – серед них і Крум, який до

2008 року очолював Агентство захисту інформаційних систем. Проте компанія Lockheed розробила модель «убивчого кіберланцюга» задля власного захисту, не сподіваючись на допомогу АНБ або якогось іншого агентства. А згодом компанія перетворила свої знання на бізнес.

Аналітики Lockheed самостійно моніторять трафік у власних мережах, але вони також отримують інформацію майже від 50 оборонних підприємств, також залучених до роботи над засекреченими державними програмами. Lockheed є головним підрядником Центру захисту від кіберзлочинності – найбільшої державної кіберкримінал істичної організації, яка веде антитерористичну й контррозвідувальну діяльність. А ще ця компанія адмініструє «Глобальну інформаційну мережу» (Global Information Grid – GIG), застосовуючи розроблену модель для захисту глобальної інформаційної технологічної мережі Міністерства оборони. Сума контракту становить $4,6 млрд. Лише у власних мережах Lockheed аналізує щодоби близько двох мільярдів транзакцій – кожен надісланий і отриманий лист, кожен відвіданий сайт, кожну дію, зареєстровану в цифрових журналах безпеки або логах. Усі дані зберігаються протягом одного року, натомість інформація про шкідливу діяльність – протягом необмеженого часу. Компанія Lockheed створила ефективну бібліотеку хакерської історії, до якої можна звернутися під час аналізу нових вторгнень. Вивчаючи заархівовані дані, аналітики виявили, що нещодавні вторгнення насправді є частиною масштабних кампаній, які почалися декілька місяців або навіть років тому й були націлені на конкретні фірми й організації. Крум говорить, що на час його звільнення з Міністерства оборони у 2008 році військове відомство спромоглось ідентифікувати й відстежити близько п'ятнадцяти операцій загальнодержавного масштабу. Нині Lockheed відстежує близько сорока хакерських операцій. Міністерство оборони також спостерігає за кількома з них (Крум відмовляється сказати, за якими саме), і компанія ділиться власною інформацією з державою в рамцях програми DIB. За словами Крума, Lockheed виявила шість кампаній, про які не знало Міністерство оборони. Усі подробиці засекречені.

Єдине, чого в рамцях закону Lockheed не може робити, – це зламати чужу комп'ютерну систему для збору інформації. Ця діяльність надалі залишається прерогативою АНБ. Проте компанія не зводить пильного погляду з деяких іноземних противників, за якими стежить і держава. У головному центрі управління NexGen Center на стінах

висять годинники, які показують поточний час у всіх країнах, де Lockheed має станції кіберспостереження, – у Пекіні теж. Упродовж семи років компанія збирала інформацію про операції з категорії «підвищеної загрози», і аналітики мають доступ до всіх цих даних. Величезний монітор на стіні показує операції у цілому світі, які відстежує Lockheed, і здебільшого це спроби вторгнення у власні мережі компанії з трьох мільйонів інтернет-адрес у майже 600 локаціях у 60 країнах світу. Що більша компанія, на яку націлені хакери, то більше інформації можна здобути. Державні контракти надалі залишаються основним бізнесом компанії, позаяк урядові замовлення приносять понад 80 % прибутку, який 2012 року становив $47,2 млрд. Однак у 2011 році Lockheed розширила співпрацю в комерційному секторі, зосередившись на технологічних послугах для перших 200 компаній зі списку Fortune 500, більшість яких є операторами критично важливих об'єктів інфраструктури, розповів Крум. І компанія хоче відкрити ще один кібернетичний центр на Близькому Сході, де попит на інтернет-розвідку та захист мереж зростає.

Навряд чи Lockheed – це єдина компанія, яка узяла кібероборону у власні руки. Після атак на банківські сайти у 2012 році американські фінансові організації створили власні підрозділи кіберстеження. (Деякі з них, поза сумнівом, є клієнтами Lockheed.) Коли неймовірний потік трафіку спричинив масштабний збій, їм довелося поквапитися. Нині найбільші банки Сполучених Штатів наймають фахівців у сфері кібербезпеки, які вміють знаходити вразливості в програмному забезпеченні та мережевих конфігураціях, аналізувати шкідливе ПЗ, досліджувати методи його роботи й призначення, а також відбивати атаки. Серед основних постачальників талановитих фахівців для банків – військові та розвідувальні організації.

Колишній керівник відділу інформаційної безпеки Bank of America починав свою кар'єру як лінгвіст-криптограф у військово-повітряних силах, а згодом очолював технологічний підрозділ в адміністрації директора національної розвідки США. Керівник відділу інформаційної безпеки банку Wells Fargo 20 років служив у військово-морських силах, а пізніше працював у ФБР. Керівник відділу інформаційних ризиків у JPMorgan Chase ніколи не працював на уряд, проте один рік пропрацював у компанії SAIC, яка процвітає здебільшого завдяки контрактам із розвідувальними агентствами, тому її часто називають

«АНБ-захід». Іще рік він пропрацював у компанії Booz Allen Hamilton, яка є одним із провідних підрядників федерального уряду в сфері кібербезпеки і де колишній директор АНБ Майк МакКоннелл почувається наче удома.

«Упродовж кількох найближчих років усі хлопці з кіберпідрозділів, що залишилися в грі, працюватимуть у банках. Вони закриють доступ до своїх мереж і обмінюватимуться інформацією лише один з одним», – розповідає колишній офіцер військової розвідки, учасник кібератаки на Ірак у 2007 року, який згодом працював для великої оборонної компанії.

На думку експертів, банки переманюють співробітників військових і розвідувальних служб, навчених працювати за високими державними стандартами, зваблюючи їх подвоєнням або й потроєнням зарплати після переходу до приватного сектора. Банки почали активніше купувати інформацію про вразливості нульового дня та експлойти від приватних аналітиків, хоча раніше найбільшим їхнім клієнтом було АНБ. Один експерт у сфері безпеки, який має тісні зв'язки з продавцями експлойтів, розповідає, що банки накопичують кіберзброю на той випадок, якщо виникне необхідність відповісти на атаку. Якщо будь-коли вибухне «приватна» кібервійна, вірогідно, її розпочне якийсь банк.

Не лише фінансові компанії розробляють власні оборонні операції. Серед компаній, які наймають військових фахівців з інформаційної безпеки на такі високі посади, як віце-президент або керівник відділу, – Johnson&Johnson, T-Mobile USA, Automated Data Processing, Coca-Cola, Intel, AstraZeneca, eBay, FedEx і сотні інших. Коли компанії не можуть себе захистити, вони шукають допомоги ззовні, тож на ринку з'являється дедалі більше послуг у сфері безпеки. У звіті для акціонерів за 2012 рік компанія Lockheed Martin заявила, що «стикнулася зі зростанням конкуренції, зокрема у сфері інформаційних технологій і кібербезпеки… з боку незвичних конкурентів з-поза меж аерокосмічної й оборонної промисловості». Це завуальований натяк на молоді компанії у сфері безпеки, як-от CrowdStrike, Mandiant і Endgame, які вибудовують власну базу джерел інформації та методів її збору й аналізу.

Компанії опинилися на порозі нової ери приватної кібербезпеки. «У нас уже є кібернетичний еквівалент агентства Пінкертона», – каже Марк Везерфорд. Так само як багатьох інших експертів, Везерфорда

турбує те, що деякі фірми не лише займаються захистом, а й інколи переходять межу, організовуючи атаки у відповідь, щоб зупинити хакерів і шпигунів. Він розмежовує хакерство у відповідь і виставлення кіберперешкод, які ускладнюють викрадання даних із атакованої мережі. Влаштування пасток, ба навіть звиблення хакерів за допомогою заражених шпигунським ПЗ документів, які вони переноситимуть до власних систем, – це сумнівні, однак, захисні методи. «Проте реальне вторгнення в мережі, атака на них – це та межа, яку я не хочу перетинати», – стверджує Везерфорд.

На його думку, вже за кілька років більшість компаній матимуть змогу фільтрувати трафік за дорученням власних клієнтів, взявши на себе роль справжніх кібервартових. Ця модель роботи вдосконалюється завдяки державним програмам передачі провайдерам секретної інформації про кіберзагрози. Наказ президента Обами від 2013 року, покликаний посилити безпеку критично важливих об'єктів інфраструктури, зобов'язує уряд «наставляти» компанії, спонукаючи їх купувати доступні на ринку комерційні продукти та послуги, що відповідають схваленим стандартам безпеки. Це один із прикладів стимулювання державою приватного бізнесу в сфері кібербезпеки, що призведе до неминучого зростання цього сектора економіки, і, ймовірно, кращий вихід, ніж державна монополія на цю сферу діяльності.

«Держава ніколи не зможе реагувати так швидко, як приватний сектор», – стверджує Везерфорд. Приватні підприємства можуть краще захистити себе.

Перебираючи на себе повноваження у сфері національної кібероборони, компанії почали впливати на курс державної політики США. 18 лютого 2013 року фірма Mandiant, що спеціалізується на комп'ютерній безпеці, оприлюднила безпрецедентний звіт, присвячений китайському кібершпигунству, називаючи Народно-визвольну армію Китаю джерелом нестримного й невгамовного шпигунства проти Сполучених Штатів. Це було пряме звинувачення, на яке б не зважилася жодна офіційна особа. Звіт фірми Mandiant був надзвичайно детальним. Він містив адресу локації хакерів і навіть фотографії їхнього офісу – бежевої 12-поверхової будівлі в районі Пудун у Шанхаї. Зважаючи на площу будівлі (понад 12 тисяч кв. м), а також публічні

заяви китайських урядовців, Mandiant виснував, що там працюють сотні, а можливо, і тисячі співробітників.

Компанія Mandiant зосередилася лише на одній з близько двадцяти груп, діяльність яких відстежувала протягом кількох років. Ці хакери працювали для китайського аналога АНБ. Група хакерів, яких Mandiant назвала APT1, працювала в Другому відділі Третього підрозділу Генерального штабу Народно-визвольної армії Китаю, відомої на загал під кодовим позначенням 61398. Генеральний штаб армії нагадує Об'єднаний комітет начальників штабів армії США, а Третій підрозділ займається радіотехнічною розвідкою, комп'ютерними атаками й експлуатацією мереж. Компанія Mandiant назвала APT1 «однією з найнебезпечніших китайських кіберзагроз».

Компанія Mandiant, яка на той час існувала менше 10 років і була заснована колишнім експертом у галузі кіберкриміналістики військово-повітряних сил, фактично заклала бомбу під одну з найчутливіших і складних сфер американської зовнішньої політики. Звіт сприйняли як одкровення. Не лише тому, що в ньому прямо вказали на китайських хакерів – те, чого раніше не хотів робити жоден аналітик, ані приватний, ані державний, – а й тому, що інформація була дуже змістовною. На 74 сторінках звіту висвітлювалася діяльність розлогої шпигунської інфраструктури, що складалася з 937 серверів або «програм для стеження», розміщених на 849 різних інтернет-адресах, більшість яких зареєстрована на організації з Китаю, але понад 100 були розташовані у Сполучених Штатах. Слідчі виявили сайти, створені хакерами так, щоб вони виглядали наче звичайні сайти новин, як-от CNN.com, щоб використовувати їх для атак APT. Компанія Mandiant назвала імена конкретних хакерів, зокрема й людини, яка ховалася під прізвиськом «Потворна горила» (Ugly Gorilla). Кілька років тому цей хакер розкрив себе в онлайн-спілкуванні на тему китайського кібервійська, спілкуючись із видатним фахівцем у сфері комп'ютерних наук, який написав докладну книжку про китайські «інформаційні війни». Mandiant навела неспростовні докази зв'язків між певними хакерами і була впевнена, що деякі з них не лише особисто знайомі, а й, можливо, працюють в одному офісі. У звіті був навіть словник китайського хакерського сленґу: наприклад, заражений комп'ютер називали «курячим м'ясом».

Компанія виснувала, що китайські кіберпідрозділи отримували «безпосередню підтримку від лінгвістів, дослідників відкритих дже-

рел, розробників шкідливого ПЗ і промислових експертів». Імовірно, працювала ціла команда, яка замовляла й обслуговувала комп'ютерне обладнання, а також персонал, який забезпечував фінансовий і організаційний менеджмент, логістику й транспорт. Інакше кажучи, це був організований на вищому рівні бюрократичний апарат, який нагадував американські державні структури.

Подробиці, що їх містив звіт Mandiant, зазвичай характерні для секретних документів державної розвідки. Це ще одна причина того, чому звіт став таким важливим. Він продемонстрував, що приватні дослідники можуть зібрати й проаналізувати інформацію не гірше, а можливо, і краще, ніж державні розвідувальні служби. Почасти це свідчило й про рівень кваліфікації фахівців Mandiant. Але водночас цей звіт виявив і справжню природу кіберпростору. У некерованому середовищі, в якому хакери можуть потрапити будь-куди завдяки спільній мережевій інфраструктурі, насправді не існує жодних секретів. За умови достатньої підготовки і за допомогою відповідних інструментів приватні нишпорки можуть відстежити хакера не гірше, ніж федеральні агенти або військові оперативники. Звіт Mandiant не лише зірвав завісу таємничості з китайського кібершпигунства, а й перевернув догори дриґом уявлення про те, що лише держава готова до битв у кіберпросторі.

Наслідки оприлюднення звіту не забарилися. Представники китайської влади виступили зі своїми звичайними спростуваннями, називаючи необґрунтованими звинувачення у шпигунстві на замовлення влади. Не минуло й місяця, як радник з питань державної безпеки США Том Донілон у своїй промові застеріг Пекін і назвав китайське кібершпигунство «дедалі важчим випробуванням для наших економічних взаємин із Китаєм» і «ключовою проблемою для обговорення з усіма рівнями китайської влади». Між країнами вже тривали переговори за зачиненими дверима: представники американської влади вимагали в Китаю припинення агресивних операцій. Відтепер ці дискусії перейшли у публічну площину. Зауваги Донілона стали першою офіційною заявою представників Білого дому щодо китайського кібершпигунства. Донілон запевнив, що проблема «перемістилася на передній план», і закликав китайську владу звернути увагу на «актуальність і масштаб цієї проблеми й приховану в ній загрозу для міжнародної торгівлі, репутації китайської промисловості та наших відносин загалом».

Уперше американці вимагали від Китаю покласти край кібершпигунству. «Пекін повинен піти на серйозні кроки для розслідування та припинення цієї діяльності, – сказав Донілон, – і розпочати з нами конструктивний прямий діалог для вироблення прийнятних норм поведінки в кіберпросторі».

Адміністрація Обами нарешті кинула виклик. І Mandiant допомогла в цьому. Так само як у випадку з одкровеннями компанії Google щодо китайського шпигунства, оприлюдненими після операції Aurora, американські високопосадовці почали обговорювати проблему, яка впродовж років тихенько їх нервувала. Звіт Mandiant містив детальну і, що найважливіше, надсекретну документацію, на підставі якої можна було висунути конкретні звинувачення. Уряд ніколи б не наважився на оприлюднення такого звіту.

Викривальна заява Mandiant викликала неабиякий суспільний резонанс. Проте публікація звіту була ретельно підготована задля максимального висвітлення пресою й погоджена з владою. Ще в жовтні 2012 року, після декількох років збору інформації про китайських шпигунів, керівники Mandiant збиралися оприлюднити звіт про свої знахідки. «Ми вирішили, що це цікава ідея, тож треба її втілити», – розповідає Ден МакВортер, директор операційного відділу компанії Mandiant, що відповідав за пошук інформації про кіберзагрози. Але спочатку компанія планувала оприлюднити лише стислий звіт, зовсім не те багатосторінкове обвинувачення, що було оприлюднене згодом. Від плану довелося відмовитись у листопаді, після телефонного дзвінка з видання New York Times. Ішлося не про прохання журналіста дати експертний коментар для статті. Йшлося про допомогу. Керівництво видання виявило, що хакери атакували їхні комп'ютери, і хотіло, аби Mandiant провела розслідування.

Аналітики Mandiant виявили, що китайські шпигуни проникли в комп'ютерні мережі газети й шпигували за понад 60 найманими працівниками, зокрема і за журналістом, який працював у Китаї над викриттям політичної корупції на верхніх щаблях влади. Шпигуни намагалися замаскуватися, перенаправляючи трафік через контрольовані ними комп'ютери в американських університетах Північної Кароліни, Нью-Мексико, Арізони і Вісконсина – вдаючись до методів, уже відомих компанії Mandiant завдяки спостереженню за іншими шпигунськими операціями, сліди яких вели до Китаю. Шпигуни отри-

мали доступ до комп'ютера в комп'ютерній мережі Times і викрали паролі від 53 особистих комп'ютерів працівників, більшість яких перебувала за межами офісу. Хакери були частиною групи, яку Mandiant колись уже вистежувала і якій дала кодове ім'я APT1. Очевидно, хакери прагнули отримати детальну інформацію про заплановану до публікації велику статтю, присвячену родичам прем'єра Держради КНР Вень Цзябао, про те, як вони використали свої політичні зв'язки та заробили мільйони доларів у тіньовому бізнесі. Компанія Mandiant знайшла докази, що китайські хакери викрали інформацію у понад 30 журналістів і керівників інших західних порталів новин, зокрема електронні адреси, контакти джерел і файли. Ба більше, шпигуни продовжували полювати на кількох журналістів. Згодом з'ясувалося, що шпигуни створили спеціальну шкідливу програму, щоб зламати обліковий запис Джима Ярдлі – тодішнього директора південноазійського бюро газети Times, який працював у Індії, а раніше очолював бюро у Пекіні. Вони також проникли в комп'ютер Дейвіда Барбози, керівника Шанхайського бюро, який написав статтю, присвячену прем'єр-міністрові Вень Цзябао, яка згодом принесла йому Пулітцерівську премію. Розслідування показало, що китайські кібершпигуни також проникали в мережі газет The Washington Post і The Wall Street Journal.

Керівники Mandiant вирішили, що стислого звіту про китайське шпигунство буде недостатньо. У компанії вважали, що в них є безліч доказів масштабної й тривалої операції проти різних галузей американської економіки, зокрема й оборонної, що почалася ще 2006 року. Спростування офіційного Китаю здавалися «комічними», як висловився МакВортер. У січні 2013 року Times написала про власне зіткнення з хакерством. Офіційна влада Китаю публічно висловила сумнів у достовірності даних Mandiant – саме ця компанія надавала допомогу в розслідуванні, а її експерти готували коментарі для статті в Times, що можна було розцінити як довіру до розслідувань Mandiant. Тоді в компанії вирішили, що настав час назвати речі своїми іменами. Спроби Китаю дискредитувати компанію та її інформацію «вочевидь лише зміцнили наше рішення надати документові широкий розголос», – розповідає МакВортер.

Представники адміністрації Обами були задоволені рішенням Mandiant. Річ не в тім, що президент і команда державної безпеки досі не знали про витівки Китаю; але тепер існував документ із конкрет-

ними доказами, які могли перевірити й обговорити експерти, змінивши характер дискусії щодо китайського шпигунства. Більше жодних неофіційних звинувачень. Жодних евфемізмів штибу «підвищеної постійної загрози», коли йдеться про Китай. І Сполученим Штатам не потрібно розкривати жодних секретних джерел інформації і методів її отримання, щоб відкрито заявити про китайське шпигунство. (Водночас із підготовкою звіту Mandiant Міністерство юстиції таємно готувало судову справу проти членів хакерської групи 61398. У травні 2014 року прокурори висунули офіційне звинувачення п'ятьом військовим чиновникам із Китаю, пов'язаним із групою хакерів. Це був перший зареєстрований випадок кримінального переслідування за хакерство на державному рівні.)

Того самого дня, коли Mandiant оприлюднила звіт, Міністерство внутрішньої безпеки надіслало групі власників і операторів критично важливих об'єктів інфраструктури та іншим фахівцям у сфері безпеки, що мали доступ до державної інформації, офіційне повідомлення. Документ містив деякі інтернет-адреси і сайти, згадані у звіті Mandiant. Варто зауважити, що Міністерство внутрішньої безпеки жодного разу не згадало Китай і не пов'язувало кібершпигунів із конкретними локаціями. Компанія Mandiant також не згадувалася.

Це повідомлення отримала вибрана група «рівноправних і партнерських організацій», і, за порадою міністерства, цей інформаційний бюлетень не поширювали у відкритих джерелах. Звіт Mandiant виявився кориснішим, бо був змістовнішим і доступним кожному. Проте урядовий бюлетень підтверджував висновки Mandiant. Час, обраний для його публікації, також говорив сам за себе. Міністерство внутрішньої безпеки могло випустити свій звіт першим, але зачекало, поки Mandiant зніме завісу таємничості з APT1. Mandiant зробила державі послугу. Джерела, близькі до авторів звіту, розповіли, що уряд поділився з компанією Mandiant деякою інформацією, але більшість висновків у звіті випливала з власних розслідувань компанії, які тривали понад сім років.

Фактично за одну ніч Mandiant перетворилася з порівняно непомітної криміналістично-експертної компанії, відомої здебільшого лише фахівцям зі сфери кібербезпеки та невеликим технологічним стартапам, на шановану організацію у сфері комп'ютерної безпеки. Керівники Mandiant стали для журналістів компетентними джерелами інформації. Тепер вони сиділи за одним столом з колишніми співро-

бітниками розвідслужб і аналітичних центрів і висловлювали власні думки щодо того, як краще захистити кіберпростір від шпигунів і хакерів. Бізнес почав процвітати. У 2013 році компанія заробила понад $100 млн на продажах, більша частина яких припадала на програмне забезпечення, розроблене Mandiant для захисту компаній від хакерських атак APT. З офіційних джерел відомо, що понад третина компаній зі списку Fortune 100 користувалася послугами Mandiant. У січні 2014 року, менш ніж через рік після публікації звіту Mandiant про групу APT1, фірма FireEye, що спеціалізується у сфері безпеки, придбала компанію за $1 млрд. Це було найдорожче надбання на ринку послуг кібербезпеки за останні роки й одна з десяти подібних угод у 2013 році, що удвічі більше, ніж попереднього року.

Компанія FireEye належала до пестунок Кремнієвої долини. Її акції з'явилися на біржі Nasdaq у вересні 2013 року, і вже в січні їхня вартість зросла вдвічі. Перший публічний продаж акцій компанії FireEye став найуспішнішим серед компаній у сфері кібербезпеки у 2013 році.

Об'єднання з Mandiant мало на меті збільшення масштабу операцій у сфері кібербезпеки. Mandiant спеціалізувалася на розслідуванні кібервторгнень, натомість FireEye намагалася їм запобігти, ізолюючи вхідний мережевий трафік у віртуальний карантин і аналізуючи дані у пошуках шкідливого ПЗ. Цей процес нагадує методи Міністерства внутрішньої безпеки для відстеження трафіку в державних мережах – і це ще один доказ того, що держава не має монополії на кіберзахист.

Поширення інформації про масштабне китайське шпигунство, доповнене викриттям глобальних розвідувальних операцій АНБ, допомогло Mandiant і FireEye створити новий бізнес, який виник унаслідок злиття. «Лише погляньте на суперспроможність цих компаній у моніторингу трафіку й запобіганні крадіжкам», – вихваляється Дейвід ДеВолт, виконавчий директор і голова ради директорів FireEye.

Його клієнти вирішили захищатися самостійно. «Ми бачимо ріст усвідомлення, про яке ще рік тому годі було й мріяти».

Якщо деякі компанії ще не переконалися в ефективності приватних фірм у сфері кібербезпеки, додатковий привід зробити це з'явився у червні 2013 року, коли 29-річний Едвард Сноуден, що працював за контрактом для АНБ, оприлюднив неймовірну кількість

викрадених ним секретних документів, у яких йшлося про глобальну систему стеження агентства. Сноуден поділився цією інформацією з журналістами видань Guardian і Washington Post, після чого почалася небачена злива публікацій, безпрецедентна за масштабами й специфікою. Було викрито практично всі аспекти шпигунських підходів агентства. Документи доводили, що АНБ збирало інформацію зі сховищ даних Google, Facebook, Yahoo, а також інших технологічних і телекомунікаційних компаній. Також агентство записувало телефонні розмови сотень мільйонів американців і зберігало їх протягом п'яти років. Представники адміністрації намагалися переконати занепокоєних громадян у тому, що більшість шпигунських операцій спрямовані проти іноземців, що мешкають за кордоном. Представники технологічних компаній збентежилися. Вони пояснювали офіційним особам, громадськості й у приватних розмовах, що чимало їхніх клієнтів мешкають в інших країнах і навряд чи їх заспокоїть те, що АНБ шпигує за ними лише тому, що вони не американці.

Іще до витоку інформації, організованого Сноуденом, АНБ робило спроби здобути підтримку хакерів для державного кіберзахисту. У 2012 році Кіт Александер виступав на хакерській конференції Def Con у Лас-Веґасі, зодягнувшись у сині джинси й чорну футболку, змінивши військову форму на одяг, який, на його думку, був звичнішим для аудиторії. У липні 2013 року, за місяць після викриттів Сноудена, організатори Def Con скасували запрошення Александера. «Сестринська конференція» хакерів Black Hat не відмовила керівникові шпигунів. Але за півгодини після початку виступу аудиторія почала його цькувати.

– Свобода! – вигукнув один із присутніх, приватний консультант зі сфери безпеки.

– Так точно, ми обстоюємо свободу, – не розгубився Александер.

– Дурня! – гукнув консультант, і аудиторія зааплодувала.

Деякі хакери – «білі капелюхи», які дбали про посилення кіберзахисту й співпрацювали з АНБ у технічних питаннях, почали сумніватися в своєму виборі, як розповів колишній співробітник агентства, який боїться, що хакери можуть розвернути свою зброю у бік уряду та намагатимуться розкрити більше секретної інформації, ба навіть атакувати державні агентства й комп'ютерні системи державних підрядників. Сноуден продемонстрував, що одна-єдина людина може

викрити величезну кількість секретів АНБ. Яких тоді збитків може завдати рух сильно вмотивованих хакерів?

Сам Сноуден був досвідченим хакером. Працюючи за контрактом на АНБ, він навчався на поглиблених курсах «етичного хакерства» і аналізу шкідливого ПЗ у приватному навчальному закладі в Індії. За словами людей, які знали про цю подорож, у країні він перебував із секретною державною місією та працював у американському посольстві в Нью-Делі. Справжня мета його роботи засекречена, проте перед приїздом до Індії у вересні 2010 року Сноуден уже вивчив деякі просунуті техніки зламу й був здібним учнем, за словами його інструктора. Його навчили зламувати комп'ютери та викрадати інформацію начебто для того, щоб краще протистояти зловмисним хакерам. Для того щоб украсти велику частину секретних документів АНБ, до яких він мав вільний доступ, цих умінь було не потрібно. Виявилося, що АНБ, яке прагнуло захистити всі комп'ютери, починаючи від Волл-стріт і до водопровідних компаній, не могло завадити 29-річному співробітникові зробити копії секретних документів про свою глобальну систему стеження.

Викриття Сноудена зашкодили АНБ з політичного погляду більше, ніж будь-що за 61-річну історію існування агентства. У липні 2013 року палата представників США практично ухвалила законопроект, який би захистив простих американців од збору агентством записів телефонних розмов, і це було б перше суттєве обмеження державної влади в питаннях стеження після теракту 11 вересня. Республіканці уклали нетиповий для них союз, бажаючи стриножити шпигунське агентство. Президент Обама створив комісію з експертів розвідки та юристів для розробки реформи програм спостереження АНБ. Комісія склала 300-сторінковий звіт і дала 46 рекомендацій, зокрема: припинити практику закупівлі експлойтів нульового дня, відмовитися від упровадження бекдорів у криптографічні продукти, призначати цивільних осіб на керівні посади в агентстві і, нарешті, розмежувати агентство та Кіберкомандування, заборонивши одній і тій самій людині очолювати їх. Фактично ця програма пропонувала заходи для зменшення впливу агентства та поступової відмови від його провідної ролі у кіберзахисті.

Проте потреба у захисті кіберпростору була актуальною як ніколи. У вересні 2013 року старший офіцер ВПС США розповів, що досі

не знає, як сильно їхні мережі вразливі до хакерських атак, позаяк аналіз вразливості був виконаний лише на чверть. А після вторгнення хакерів у систему управління повітряним рухом, що дозволяло зловмисникам впливати на плани польотів літаків і роботу радарних систем, минуло вже понад чотири роки! Генеральний інспектор Міністерства оборони вже за місяць після отримання доступу до систем ВПС звітував, що в Пентаґоні, Міністерстві внутрішньої безпеки й АНБ немає централізованої системи обміну інформацією про кіберзагрози у режимі реального часу. Існувала державна система обміну попередженнями і ще одна система для надсилання інструкцій про те, як на ці загрози реагувати, однак обидві системи не були поєднаними.

Новини із сектора критично важливих об'єктів інфраструктури, які держава прагнула захищати, також не тішили. Трохи раніше цього ж року двоє інженерів виявили низку вразливостей у комунікаційних системах, які використовували підприємства з галузей енергетики та водопостачання в країні. Виявлені вразливості дозволяли зловмисникам викликати масштабні знеструмлення або виводити з ладу системи водопостачання. Представники Міністерства внутрішньої безпеки розіслали попередження, однак лише кілька комунальних підприємств оновили версії вразливих програм. Натомість інтенсивність кібершпигунства проти Сполучених Штатів, здається, не зменшувалася. «У цій країні немає жодної важливої комп'ютерної системи, в яку цієї самої миті не намагаються проникнути, атакуючи її терабайтами інформації», – заявив колишній директор АНБ МакКоннелл у жовтні, під час виступу у Вашинґтоні. І ця заява луною рознеслась у прилюдних і приватних розмовах численних співробітників розвідки, військових і правоохоронних організацій.

Представники влади досі намагались оговтатися після минулорічної атаки, спрямованої на державну нафтову компанію Aramco у Саудівській Аравії, яка, за деякими оцінками, була найдорожчою компанією світу, бо постачала близько 10 % обсягу світового видобутку нафти. Хакери використали потужний вірус для повного знищення інформації з близько 75 % комп'ютерів компанії, тобто приблизно з 30 тисяч пристроїв. За словами представників компанії, хакери хотіли зупинити виробництво нафти і газу, а вірус видаляв листи, електронні таблиці та документи. Хакери не змогли зашкодити виробничим потужностям Aramco, проте атака стала попередженням про те, що компанія може зазнати серйозних збитків, якщо хтось знищить

сховища корпоративної інформації. Деякі американські чиновники підозрювали, що атаку провів Іран, аби помститися за впровадження «хробака» Stuxnet. Якщо так, то це означало ескалацію міжнародної кібервійни й демонструвало США, що не варто розраховувати на те, що американські кіберудари залишатимуться без відповіді.

Кіберзлочинність у США також сягнула критичного рівня. У середині грудня 2013 року торговельний гігант Target виявив, що хакери пробилися в комп'ютерні системи компанії та викрали інформацію про дебетові і кредитні карти клієнтів. Шахраї інсталювали шкідливу програму безпосередньо у касові апарати в магазинах мережі Target і звідти викачували фінансові дані. За першими оцінками компанії, було викрадено фінансову інформацію про 40 млн покупців. Проте за місяць цю кількість скорегували: кількість потерпілих коливалася від 70 до 110 млн. Ці цифри приголомшують і роблять витік інформації з Target однією з найбільших кіберкрадіжок в історії. Слідчі виснували, що хакери, найімовірніше, походили зі Східної Європи або Росії і здійснили свій перший злам комп'ютерної мережі Target за допомогою мережевих сертифікатів, викрадених у пенсільванської компанії, яка обслуговувала холодильні системи у супермаркетах. Компанія Target також виявила, що була викрадена інформація про імена клієнтів, їхні телефонні номери, поштові та електронні адреси. Компанії загрожували величезні штрафи за недотримання промислових стандартів захисту інформації про дебетові і кредитні карти.

Державні агентства не досягли значно більшого успіху, захищаючи власні мережі. У лютому 2014 року комітет сенату повідомив, що цивільні федеральні агентства, за рідкісним винятком, не встановлювали необхідні оновлення програм, зокрема й антивірусних. На відміну від колег із військових і розвідувальних організацій, працівникам цивільних агентств бракує найелементарніших знань у сфері безпеки й усвідомлення її необхідності. Держслужбовці використовували дуже прості паролі. Дослідники виявили, що одним з найпопулярніших паролів було слово «пароль». У звіті йшлося про те, що навіть у Міністерстві внутрішньої безпеки оновлення програмного забезпечення встановлене не на всіх системах, хоча це «основне правило безпеки, якого дотримується майже кожен американець, який має комп'ютер».

Попри викриття Сноудена, Александер продовжував упиратися. Невтішні новини щодо слабкої кібероборони лише посилили його арґументи про те, що АНБ повинно відігравати впливовішу роль у захисті країни. У жовтні 2013 року на конференції з питань кібербезпеки у Вашинґтоні, спонсованій компанією Raytheon, що працює за контрактом на оборонну сферу, Александер просив більше повноважень для захисту фінансового сектора, висуваючи доволі сумнівні технічні арґументи. Він мріяв, що банки надаватимуть АНБ інформацію в режимі реального часу, щоб агентство могло виявити «кіберпакет, ладний знищити Волл-стріт» і перехопити його, наче ракету. Термін «кіберпакет» у цьому контексті не має очевидного пояснення. Імовірно, Александер мав на увазі, що просунутий комп'ютерний «хробак» або вірус може порушити роботу комп'ютерів фінансової установи чи пошкодити інформацію, яка зберігається на цих комп'ютерах. Проте твердження, що один-єдиний пакет даних зможе знищити Волл-стріт, звісно, було абсурдним. Стверджувати таке – це наче заявити, що пейнтбольна кулька може вивести з ладу танк.

Рівень перебільшення Александером кіберзагроз і таке спрощене пояснення дій у відповідь його власного агентства показало його відчайдушну потребу в суспільній підтримці місії, а також переляк, який він відчував. Сноуден допоміг підірвати репутацію агентства, яку Александер вибудовував упродовж багатьох років.

14
НА ЗОРІ

17 січня 2014 року Барак Обама встав за кафедру у Великому залі Міністерства юстиції у Вашинґтоні, щоб оголосити своє рішення про те, які програми АНБ зі стеження та кібербезпеки він збереже, а які скасує. Якщо американські шпигуни боялися того, що президент відсуне їх на другий план, то після перших вимовлених ним слів могли зітхнути з полегшенням.

Обама почав із порівняння співробітників АНБ з Полом Ревіром*, лідером організації «Сини свободи», який створив «секретний розвідувальний комітет» для патрулювання вулиць колоніального Бостона, «щоб доповідати про будь-які ознаки того, що британці готуються до рейдів проти молодих патріотів Америки». Це був найпромовистіший виступ Обами на захист АНБ і радіотехнічної розвідки США. Адже президент щойно порівняв їх з героєм американської революції.

Потому Обама згадав, як під час Громадянської війни шпигуни на повітряних кулях визначали розміри армії конфедератів, як розшифровувалися повідомлення, що розкривали військові плани Японії під час Другої світової війни, і як «перехоплення повідомлень зберігало життя солдатів, коли загони генерала Паттона просувались Європою». І далі в такому самому стилі про те, як президент Гаррі Трумен створив на початку холодної війни Агентство національної безпеки, «щоб ми могли поглянути зсередини на Радянський блок і надати нашим лідерам потрібну їм інформацію для протистояння агресії та уникнення катастрофи».

Виступові Обами передував брифінґ Білого дому, під час якого журналістам були подані президентські пропозиції змін у розвідувальній діяльності АНБ.

---

* Пол Ревір (1735–1818) – один із найвідоміших героїв Американської революції. Як головний вісник Бостонського комітету безпеки, оповіщав повстанців про наближення британських військ.

Реформи були мінімальними. Обама збирався внести кілька поправок у контраверсійну програму каталогізації записів телефонних розмов американців, а саме пропонував зберігати ці записи не в базах АНБ, а десь в іншому місці. Він залишив Конгресу та міністрові юстиції складне завдання – визначити, де саме зберігатиметься ця інформація. Зрештою, президентська адміністрація та законодавці погодилися, що записи зберігатимуть телефонні компанії, які надаватимуть АНБ доступ до інформації в рамцях розслідувань. Обама також погодився на деякі незначні вдосконалення в питаннях захисту приватного життя іноземців, якими зацікавилося АНБ. Але загалом повноваження АНБ залишилися недоторканими.

Обама відклав реалізацію або й відмовився від усіх пропозицій із приборкання АНБ, отриманих їм від радників. Колись він уже відхиляв пропозицію розділити керівництво АНБ і Кіберкомандування. А зараз знехтував закликом ревізійної комісії позбавити агентство повноважень у сфері інформаційного забезпечення й усунути його від роботи із захисту комп'ютерних систем від кібератак і проникнень. Якби Обама погодився на ці зміни, місія АНБ могла б кардинально змінитись і сама організація змінилася б до невпізнання.

Обама відкинув пропозицію комісії не залучати керівництво АНБ до проведення або супроводу операцій на території Сполучених Штатів. Заклики зробити директором АНБ цивільну особу й затверджувати його кандидатуру в сенаті президент також не почув. Директор АНБ Кіт Александер міг заспокоїтися: більша частина збудованої ним імперії залишилася недоторканною, попри всі випади преси в його бік після викривальних заяв Сноудена. Генерал планував звільнитися в березні. Президент Обама запропонував посаду віце-адміралові Майклові Роджерсу, який мав відповідний досвід для посади директора АНБ і кіберкомандувача. Роджерс керував тоді службою радіотехнічної розвідки ВМС США та кібервоєнними операціями. Як і Александерові, йому вже доводилося сидіти на двох стільцях.

У своїй промові Обама не згадав пропозиції комісії щодо припинення збору експлойтів нульового дня та дискредитації стандартів шифрування. Одна високопоставлена офіційна особа розповідала, що президент попросив проглянути рекомендації та поділитися висновками. Врешті-решт адміністрація зупинилася на ухильному рішенні, дозволяючи розкривати інформацію про вразливості, але залишаючи в таємниці будь-які дані, що можуть мати важливе значення для

безпеки держави. Це була велика поступка АНБ, яке могло засекретити всю інформацію про вразливості нульового дня, оголошуючи їх важливими для забезпечення безпеки, і працювати як зазвичай. Нова політика не поклала край дискусії. Обама просто відклав її, і здавалося малоймовірним, що він або його радники запропонують якісь значні зміни.

Практично в усіх питаннях, починаючи від методів ведення операцій і закінчуючи персоналом, Обама вирішив зберегти статус-кво. Авжеж, його апеляція до історичної важливості розвідки під час бойових дій свідчила про бажання захистити АНБ і зберегти його повноваження.

Обама вибрав вдалий час для виступу. 17 січня 1961 року, 33 роки тому, президент Дуайт Ейзенгауер у своїй прощальній промові до нації виступив із застереженням щодо «військово-промислового комплексу», чий «глобальний вплив – економічний, політичний і навіть духовний – відчувається в кожному місті, у кожній урядовій будівлі, у кожному офісі федерального уряду». Ейзенгауер говорив про те, що армія вже майже не нагадує ту, в якій він служив під час Другої світової війни, або ту, якою командували його попередники в Білому домі. «До останнього нашого світового конфлікту в Сполучених Штатах не було оборонної промисловості», – говорив Ейзенгауер, переконуючи громадян «стати на варті проти невиправданого альянсу влади й промисловості, умисного чи неумисного», вважаючи його необхідним бастіоном для захисту від комуністичної тиранії, однак розумів «згубні наслідки» такого союзу, якщо не контролювати «потенціал катастрофічного зростання недоречної сили». «Це злиття величезного військового потенціалу та величезної військової промисловості – новий для Америки досвід», – заявив Ейзенгауер.

Те саме стосується злиття військових організацій із величезною індустрією інтернет-технологій. Іще нещодавно в Сполучених Штатах не було кібервійськової індустрії. Збройні сили не вважали інтернет полем битви. Корпорації не купували захист від шпигунів і хакерів. Зростання потужності та стрімке утворення альянсу між великим військовим комплексом і великим бізнесом відбувалося на очах Барака Обами. Проте, на відміну від Дуайта Ейзенгауера, він не бачив підстав для страху й поганих передчуттів.

Ейзенгауер помер через вісім років після свого пророчого виступу. Він передбачив появу військово-промислового комплексу, але не міг уявити, що одного чудового дня ринкова вартість провідних оборонних підприємств перевищить ВВП багатьох країн світу, а створення зброї, транспортування солдатів і навіть їхнє харчування в зоні бойових дій збройні сили Сполучених Штатів доручать підрядникам. Військово-мережевий комплекс також разюче змінить характер воєнних дій і навіть самого кіберпростору. Що принесе наступне десятиріччя?

Насамперед державна влада не буде домінувати в цій сфері, принаймні не постійно. І це фундаментальне порушення балансу сил від часів Ейзенгауера і свідчення того, що його попередженням знехтували. Уряди держав ухвалюватимуть стратегії та закони, а також контролюватимуть стандарти безпеки, яких банки, комунальні підприємства та інші критично важливі об'єкти інфраструктури повинні дотримуватися (можливо, з порушеннями).

І ці організації створюватимуть кіберармії й учитимуть їх воювати в мережах, які, врешті-решт, інтегруються до військового арсеналу держави. Якщо Китай, Іран або інші ворожі країни будь-коли розпочнуть масштабну атаку на американську електростанцію чи банк, військові дадуть відсіч як у віртуальному, так і в реальному світі. Атаку, яка призведе до поширення паніки, порушення життєдіяльності держави або людських жертв, зустрінуть аналогічною контратакою.

Проте щоденний захист критично важливих об'єктів ляже на плечі корпорацій, які впораються з цим завданням не згірше від держави. Компанія Lockheed Martin і подібні до неї фірми розвинуть бізнес із моніторингу, аналізу трафіку та створення застосунків для виявлення шкідливих програм і хакерської активності, вдаючись до методів, які ґрунтуватимуться на інформації, зібраній у режимі реального часу у власних глобальних інформаційних мережах, а також у мережах клієнтів. Щось штибу краудсорсингу*. Такі компанії, як CrowdStrike і та, що повстала після об'єднання Mandiant і FireEye, будуть не лише розслідувати вторгнення, що відбулися, а й пропонувати клієнтам по-

* Краудсорсинг – передача певних функцій невизначеному колу осіб на підставі публічної оферти (пропозиції укласти договір), коли клієнт стає рівноправним партнером бізнесу.

слуги із захисту мереж від потенційних загроз – так само як охоронні фірми пропонують захищати будинки й офіси від грабіжників.

Військово-мережевий комплекс нагадує свого промислового попередника в тому, що стосується делегування деяких питань національної безпеки. Збройні сили не розробляють озброєння та методи оборони, вони платять за це приватним компаніям, і так було повсякчас від заснування Республіки. Проте саме держава завжди володіла монополією на застосування сили. І ось тут військово-мережевий комплекс круто звертає зі шляху історії. Можливості корпорацій зі збору інформації не поступаються можливостям держави. Компанії розробляють методи виявлення загроз, розшукують уразливості нульового дня, а відтак використовують їх у власних інтересах. Передбачаючи зростання загрозливої влади військово-промислового комплексу, Ейзенгауер не міг припустити, що корпорації колись конкуруватимуть з державою навіть на полі битви.

Ринок дозрів для складних і надійних технологій кібербезпеки. Щоразу, коли стає відомо про масштабний витік даних, як-от викрадення даних дебетових і кредитних карт у компанії Target у 2013 році, яке торкнулося майже третини населення США і заполонило перші шпальти всіх головних ЗМІ країни на декілька тижнів, дедалі більше компаній відчайдушно потребують захисту від потенційних утрат. У 2013 році федеральна влада повідомила понад триста компаній про проникнення в їхні мережі – це величезна кількість, але, вірогідно, аж ніяк не повна. Адже йшлося лише про вторгнення, виявлені державою або компаніями, що займаються комп'ютерною безпекою. Власники критично важливих об'єктів інфраструктури опинились у надзвичайно загрозливій ситуації. У грудні 2013 року міністр енергетики Ернест Моніз заявив, що більшість минулорічних кібератак у Сполучених Штатах була скерована проти енергетичної інфраструктури, до якої входять компанії, що володіють і управляють електромережами, а також видобутком нафти й природного газу. Дотепер хакери намагалися лише проникнути в мережі управління цими об'єктами або ж у комп'ютери, розташовані в офісах корпорацій, яким ці об'єкти належать. Проте, за словами Моніза, «немає жодних сумнівів», що Сполучені Штати зазнають масштабніших атак, які загрожують частковим знеструмленням. «Абсолютно зрозуміло, що, коли йдеться про кібератаки, слова "якщо" вже не існує. Я не хочу, щоб дійшло до виходу

з ладу енергомережі. Але це перегони, і ми намагаємось якнайшвидше посилити захист… На нас чекає багато роботи».

Очевидно, держава також бере участь у цих перегонах і вона може дещо зробити для компаній: давати більше конкретної та корисної інформації про те, з якого боку очікувати небезпеки; чинити тиск на провайдерів, аби ті блокували доступ до відомих ворожих джерел; урешті-решт, іти у наступ для відбиття атаки, наближення якої можна спрогнозувати. Не всі із запропонованих рішень вимагають змін у законодавстві. Адміністрація має на це повноваження виконавчої влади. Проте енергетичні компанії, так само як менш важливі для економіки підприємства, і досі покладаються лише на власні сили, стримуючи нападників, які щодня наближаються до брами, загрожуючи пробити стіну захисту. Збільшується кількість мереж, розкиданих географічно, і держава просто не в змозі їх захистити, навіть у тому разі, якби втілила план Александера, інсталюючи сенсори у кожній банківській мережі.

Вороги не вгамовуються. Лише з вересня 2013-го до березня 2014 року банки зазнали понад триста DDOS-атак, подібних до приписуваної Ірану операції з виведення в офлайн сайтів, що викликала сильну паніку в фінансовому секторі. Владі чудово відомо про ці атаки – їхня кількість зазначена у звіті АНБ. Якщо компанії прагнуть захистити себе, їм доведеться ділитися з владою деякою інформацією про те, що відбувається в їхніх мережах. Хоча в них є сильний мотив подбати про власну безпеку й захищатися власноруч.

Урешті-решт, потужні заходи з безпеки стануть популярним товаром, особливістю, яку банки, провайдери інтернету та інші компанії, що мають доступ до персональних даних, використовуватимуть для залучення клієнтів – точнісінько так, як автовиробники рекламують товар, згадуючи про подушки безпеки і ABS. Це вже відбувається. Компанія American Express, яка тривалий час позиціонувала себе не як постачальника кредитних карт, а як закритий клуб із річним внеском за членство, яке дає особливі привілеї (певний статус, вищий кредитний ліміт), 2013 року запустила на телебаченні та в інтернеті серію рекламних роликів, у яких наголошує на системі «інформаційної безпеки», що надсилає повідомлення на мобільний телефон клієнта, щойно з'явиться підозра про шахрайське списання коштів. У одному з роликів охайний, добре одягнений міський мешканець під спостереженням відеокамер минає охоронців на вході до елегантного

багатоквартирного будинку, повз який мчать поліцейські машини. Лунає голос за кадром: «А хто захистить вас у мережі, де ми витрачаємо понад два мільярди доларів щороку?» Відповідь: «American Express – завдяки алгоритму, що вивчає характер ваших витрат і виявляє аномалії». (Випадково чи ні, закадровий текст озвучила акторка Клер Дейнс, яка зіграла в серіалі Homeland роль оперативної співробітниці ЦРУ, що намагалася запобігти терористичній атаці на США.)

Звичайно, фінансові організації багато років поспіль використовували системи виявлення шахрайських операцій, однак лише нещодавно почали рекламувати їх як престижний сервіс, реагуючи на ріст усвідомлення клієнтами того, що вони та їхні гроші вразливі у кіберпросторі. Наш стильний власник кредитки отримує попередження на айфон і, стоячи посеред жвавої вулиці, повідомляє American Express, що ні, дев'ять секунд тому він не авторизовував операції купівлі в інтернет-магазині електроніки на суму $1245. Він спокійно насолоджується обідом у кафе й упевнено кладе на стіл кредитку Amex, знаючи, що він «громадянин безпечнішого світу». Повідомлення прозоре. Ви можете себе захистити. (Ви повинні *хотіти* себе захистити.) Але це коштуватиме вам грошей.

У лютому 2014 року адміністрація Обами підготувала низку інструкцій у сфері кібербезпеки та прикладів «кращих практик», заохочуючи компанії переймати їх. Проте не примушувала до цього. «Урешті-решт, саме ринок визначає, як треба чинити компаніям» і чи дотримуватися цих інструкцій, пояснював один із керівників адміністрації президента.

Саме комерційні компанії відповідальні за більшість інновацій у сфері кібербезпеки – за появу нових засобів і методів безпечного зберігання даних і проведення кібератак на противників. Компанії, що спеціалізуються у сфері кібербезпеки, спроможні залучати найдосвідченіших і найкваліфікованіших працівників, оскільки платять значно більше, ніж державні агентства та військові організації. Держава ніколи не зможе запропонувати конкурентну зарплату кваліфікованим технічним фахівцям. Аби звабити талановитих працівників, державні та військові структури обіцятимуть повну пригод роботу – шпигунство, військові операції – і апелюватимуть до почуття обов'язку й честі, які завжди супроводжують працю заради суспільства. Проте

цього виявиться не досить, щоб вирішити проблеми безпеки, з якими стикнеться держава, особливо у цивільних агентствах, де рівень безпеки досі незадовільний. Найімовірніше, вам спадає на гадку Міністерство у справах ветеранів, яке регулярно втрачає інформацію про пацієнтів, зокрема номери соціального страхування та інші важливі дані, але не ЦРУ з його надійним захистом. На жаль, державні організації, які володіють особистою інформацією громадян, доволі вразливі та зазвичай найгірше захищені.

Агентства, які не можуть найняти захисників, звертатимуться до корпорацій, у лавах яких працюють досвідчені колишні військові або державні службовці і керівники яких колись відповідали за низку державних програм і операцій з кіберзахисту. Державну службу вже нині вважають лише сходинкою на шляху до особистого збагачення. Державні агентства та військові вже знають, що більшість співробітників затримаються на стільки часу, скільки потрібно для здобуття знань і навичок, високого рівня доступу до секретної інформації (необхідна вимога для роботи у сфері кібербезпеки) і накопичення професійних контактів, а потім перейдуть у приватний бізнес. Це наче обертові двері між державним і приватним сектором, що рухатимуться дедалі швидше.

Уряд США продовжуватиме ділитися секретною інформацією про загрози з провайдерами, які використовуватимуть отримані дані для сканування трафіку своїх клієнтів, а отже, ваших електронних листів, пошукових запитів, переглянутих вами сайтів. Конгресові доведеться внести законодавчі зміни, щоб спонукати уряд частіше ділитися інформацією. Постачальники послуг, так само як і компанії, що працюють із персональними даними, вимагають гарантій відсутності відповідальності за порушення таємниці приватного життя у разі передачі даних владі. Деякі з цих компаній також хочуть отримати імунітет на той випадок, якщо не зможуть відбити кібератаку і це призведе до фізичних збитків або втрат інформації. Якщо провайдерам гарантуватимуть захист від відповідальності, держава чекатиме від них посилення заходів із захисту кіберпростору. Уся інфраструктура кіберпростору фактично належить близько 5 тисячам провайдерів і операторів зв'язку, тому очікується, що вони припинять продавати доменні імена кіберзлочицям, не обслуговуватимуть відомих або підозрюваних зловмисників і почнуть перенаправляти або блокувати трафік під час масштабних кібератак.

Деякі спостерігачі порівнюють сучасних кіберзлочинців з європейськими піратами XVII століття. Це дуже влучне й доречне порівняння. Англійські пірати колись панували у морі, атакуючи торговельні кораблі та завдаючи прикрощів потужнішому королівському флотові, здебільшого іспанському. Китайські кібершпигуни, так само як ті пірати, діють на замовлення уряду, але на віддалі й потай, щоб влада могла заявити про безпорадність перед ними. Однак за цей фасад проникнули. Американські офіційні особи публічно й у приватних розмовах закликають китайський уряд припинити кіберпіратство, яке, як відомо обом сторонам, він підтримує. Водночас, так само як пірати, щоб протистояти можливим загрозам, держави можуть залучати кіберприватників. Сучасний аналог дозвільної системи або традиційна система заохочень дає змогу приватним кібернайманцям атакувати злочинців і шпигунів або принаймні вдаватися до «активної оборони», яка є прерогативою АНБ. Звісно, влада звернеться до цих брудних методів лише у тому разі, якщо стан кібербезпеки значно погіршиться. Проте компанії, що володіють потрібним досвідом і навичками, вже працюють. Здається неймовірним, але не виключено, що держава колись надасть конкретним фірмам повноваження, які дозволять їм проводити контратаки проти небезпечних цілей, зокрема під час масштабних атак, що загрожують критично важливим об'єктам інфраструктури.

Уряди досі забороняють розпочинати приватні кібервійни, до яких належать проникнення в мережі противника як відплата за крадіжку інформації з мережі або атаки на неї. Проте правила, які визначають право на самооборону, ще потрібно скласти. Чи будуть вони сформульовані у формі законів? Можливо, в далекій перспективі. Але в найближчому майбутньому вони матимуть форму загальноприйнятих норм поведінки, які досить складно регламентувати. Щойно одна компанія зламає комп'ютер противника з метою самозахисту, інша вирішить учинити так само, попри законну заборону. Приватні кібервійни, ймовірно, неминучі. Одного дня якась компанія вирішить звабити хакерів документами, зараженими вірусами, що знищать ворожу мережу, щойно вони їх відкриють. Провокація перетвориться на дуель. Потому владі доведеться втрутитися, щоб зупинити конфлікт, або – у найгіршому сценарії – застосувати силу.

Щоб захистити людей від щоденних кіберзагроз, які не несуть значної небезпеки для життя чи гаманця, компанії створюватимуть

безпечні зони інтернету. Банки вже намагалися позбутися доменної назви .com і перейти на .bank чи власну назву банку. Вони сподівалися, це стане сигналом для клієнтів, що вони мають справу зі справжнім банком, а не з шахрайським сайтом. Компанії створюватимуть цілі кібернетичні інфраструктури, фундаментом яких буде безпека, а трафік аналізуватиметься активніше й ретельніше, ніж у глобальній мережі інтернеті. Це буде онлайн-аналог територій під пильною охороною. Власники такої інфраструктури, так само як і власники приватного бізнесу, зможуть обмежувати користування нею, укладати власні правила й вимагати їхнього виконання, а також пропонувати особливі переваги, насамперед безпеку. Пригадайте всі сервіси, якими ви користуєтеся на щодень – банк, електронна пошта, улюблені інтернет-крамнички, – усі вони працюють в одній або в декількох приватних мережах. Власники цих мереж ретельно аналізують трафік, відстежуючи шкідливі програми, попереджають вас про потенційну небезпеку викрадення ваших особистих даних, контролюють тих, хто намагається увійти до мережі, і не пускають до неї підозрілих відвідувачів. По суті, це аналог надсекретних мереж, якими користуються військові. Однак такі мережі не зупинять ворогів, так само як не здатні на це військові – і це довела операція «Американська картеч». Проте вони зможуть надати вищий рівень безпеки, ніж той, який ми маємо нині на неконтрольованій території глобального інтернету.

Хто зможе забезпечити таке співтовариство? Можливо, Amazon. Дійсно, компанія вже створила версію такої інфраструктури – для ЦРУ. Веб-сервер служби Amazon, який слугує за сховище для зберігання й обробки даних інших компаній, отримав за контрактом $600 млн за створення закритої системи, або «хмари», для шпигунського агентства. На відміну від інших «хмар», доступ до яких здійснюється через глобальну мережу, ця «хмара» буде управлятись апаратним і мережевим обладнанням, розробленим Amazon. Раніше компанія не надавала послуг зі створення приватних мереж, і ЦРУ може стати першим клієнтом на цьому новому ринку.

У найближчому майбутньому ви проводитимете більше часу всередині таких захищених співтовариств. І платитимете за вхід утратою анонімності. Компанія потребуватиме інформації про те, хто ви, ба більше, де ви і ваш комп'ютер або мобільний пристрій розташовані. Операторові безпечної зони потрібно знати ваше розташування, щоб

визначити, друг ви чи ворог. І це дозволить йому викинути вас із цієї зони за порушення правил. Анонімність сприйматимуть як загрозу. Адже вона означатиме, що вам є що приховувати, так само як зловмисному хакерові, який ховає свою локацію за допомогою зламаного сервера, розташованого в іншій країні. У вас буде посвідчення, схоже на ID-картку з фото, яке підтверджуватиме вашу належність до зони безпеки й згоду з її правилами в обмін на захист. Безпека в кіберпросторі не буде вашим правом. Вона стане привілеєм. І ви за нього заплатите.

Фундаментальні питання щодо нашого майбутнього в кіберпросторі полягають не в тому, чи слід нам ухвалити закони й правила, що регулюватимуть поведінку в ньому. Некеровані простори розпадаються. Вони нездорові. Вони дають прихисток злочинцям і терористам. Жодна людина серйозно не розглядає майбутнє без законів і правил. Дилема полягає в тому, яку вагу ми надамо безпеці в кіберпросторі і хто за неї відповідатиме. Які транзакції, і яку їхню кількість, потрібно ретельно аналізувати? Усі електронні листи? Усі пошукові запити? Усі покупки? І хто це робитиме? Чи дозволяти людям відмовитися від безпечнішого кіберпростору на користь того, в якому можлива анонімність? Ми ніколи не визнавали право на анонімність. Проте кіберпростір дарує нам таку можливість. Для багатьох саме це є запорукою свободи самовираження, яку інтернет покликаний підтримувати. Уряд США схвалив цю концепцію, допомагаючи створювати анонімну мережу Tor.

А як щодо нашої приватності? Наш словниковий запас для опису цієї ідеї неужитковий завдяки усюдисущому оку держави. Більша частина інформації, зібраної розвідкою США про американських громадян, складається з логів і цифрових записів, так званих метаданих, не захищених від пошуку й вилучення четвертою поправкою. Коли люди говорять про право на недоторканність приватного життя в мережі, чи йдеться їм про право на анонімність? На право бути невпізнанними для влади? З погляду держави, анонімність викликає підозру. Анонімність – це потенційна загроза. Саме тому АНБ присвятило стільки часу, щоб підірвати роботу мережі Tor. Анонімність і колективна безпека в кіберпросторі – несумісні поняття. Немає жодного сумніву, що конфлікт між ними проіснує багато років.

Ми повинні скептично ставитися до того, що влада шукатиме баланс між цими інтересами, що суперечать один одному. Нелегальні розвідувальні операції – не дуже доречна діяльність, якщо йдеться про створення прозорої та чесної відкритої політики. АНБ вело масове нелегальне стеження за американцями впродовж чотирьох років і реалізовувало секретну програму, деякі частини якої були абсолютно незаконними, але саме агентство заклало підвалини військово-мережевого комплексу. Ми й гадки не мали про його народження, аж поки він не націлився на нас.

Власними діями, санкціонованими двома президентами, АНБ зробило інтернет менш безпечним у багатьох сенсах. Інсталюючи шкідливі програми в десятки тисяч комп'ютерів і серверів у всьому світі, агентство цілком могло зробити вразливими комп'ютери невинних людей і піддати їх підвищеному ризику стати об'єктом атаки або шпигунства, зокрема й державного. Агентство ускладнило американським компаніям ведення бізнесу в глобальній економіці. Компанії IBM, Hewlett-Packard, Cisco і Microsoft звітували про зменшення обсягів продажу в Китаї та на інших важливих ринках після оприлюднення викривальних матеріалів щодо шпигунства АНБ. Іноземні держави вбачають в американських технологіях, які колись були золотим стандартом якості та інновацій, інструменти американського шпигунства. Звісно, компанії також завинили й почасти відповідають за таке ставлення, адже брали участь у державних програмах стеження або заплющували очі на те, що АНБ інсталює бекдори в їхніх системах. До намірів корпорацій урівноважити конкурентні питання цивільних свобод і безпеки у кіберпросторі слід поставитися критично. Але саме компанії найбільше вплинуть на майбутнє інтернету, і вони вже роблять перші кроки на цьому шляху – переважно задля протидії шпигунству АНБ, – працюючи над вдосконаленням захисту власних продуктів і послуг. Наприклад, компанія Google посилила шифрування електронних листів, що суттєво ускладнило шпигунам розшифрування перехопленої приватної кореспонденції. Це перемога для користувачів, які переймаються недоторканністю приватного життя. Запит на безпечніші та потенційно більш анонімні технології допоможе розвинутися новому високотехнологічному секторові економіки: захисту від стеження в кіберпросторі.

Проте АНБ – не ворог. Це домівка експертів, які знають, як захистити комп'ютери та їхніх користувачів од недоброзичливців, хоч

би ким ті були: злочинцями, шпигунами чи солдатами. АНБ і Кіберкомандування повинні розвивати власні можливості задля державного захисту. Проте шпигунське агентство надто тісно пов'язане з еволюцією Кіберкомандування. Кібервійна – це справа військових, тому військові відомства під контролем цивільних, а не солдатів чи шпигунів повинні відігравати в ній провідну роль. Кібернетичні військові операції стануть частиною військової доктрини – безсумнівно, так учинять усі армії світу. Можливо, майбутній президент вирішить розділити керівництво АНБ і Кіберкомандування, що в перспективі лише посприяє підвищенню компетентності та відповідальності кіберармії.

Але кіберпростір дуже розлогий і надто всеосяжний, щоб дозволити якійсь одній силі управляти їм або диктувати правила поведінки. Немає точного визначення кіберпростору. Це не громадське місце, але й не приватна територія. Ми дійшли до того, що почали залежати від нього, як від електрики чи водопостачання. Проте кіберпростір і надалі залишається колекцією приватних пристроїв. На щастя, ми опинилися на зорі нової епохи, не у її сутінках і ще маємо трохи часу, щоб замислитися про бойові барабани, бій яких супроводжує будь-яку дискусію про природу кіберпростору, до якого ми так прив'язалися.

Проте час спливає швидко. Держави та корпорації змінюють правила в процесі гри, і їхні дії мають серйозніші наслідки, ніж більшість із нас припускає. Вони стосуються кожного, хто стикається з кіберпростором (який, поза сумнівом, таки є громадським місцем), а отже, може побачити те, що Ейзенгауер називав «важливою угодою з актуальних питань цього видатного моменту, мудрий аналіз якого дозволить краще усвідомити й сформувати майбутнє нації». Хоч як непокоїла Ейзенгауера поява потужних і потенційно руйнівних нових технологій, найбільше його хвилювала «науково-технічна еліта», яка заявляла, що краще за всіх знає, як ухвалювати рішення, які вільні люди можуть приймати самостійно. А найбільше Ейзенгауер боявся появи військово-промислового комплексу. І його заклик залишатися пильними, коли йдеться про «зростання недоречної сили», нині знаходить такий самий відгук, як і тоді. «Ми не повинні нікому сліпо вірити. Лише пильне та інформоване суспільство може підкорити громіздку військово-оборонну машину нашим мирним цілям задля процвітання безпеки й свободи».

ПОДЯКИ

Написання книжки вимагає самотності. Проте вихід її у світ – це колективна праця. Я хотів би згадати деяких людей, чиї настанови, підтримка та час виявилися дуже цінними у ході роботи над книжкою.

Мені вже давно бракує захоплених епітетів, щоб описати мою агентку Тіну Бенетт, і це, повірте мені, проблема всіх її клієнтів. Це одна з найчуйніших і найдбайливіших осіб, яких я знаю, і невтомна захисниця письменників та їхніх творів. Це наша друга спільна книжка. Так само як під час роботи над першою, Тіна допомагала мені викарбувати та вдосконалити власні ідеї, а також збагнути, що саме я хочу сказати. Не існує кращого за неї компаньйона для письменника.

Мені страшенно пощастило мати їх обох. Своєму редакторові, Імону Долану, я б довірив власного первістка, хоча, гадаю, я так і вчинив. Це наша друга книжка, і, здається, не потрібно нагадувати про його обдарованість і шляхетність, однак я знову про це згадав. Імон не лише покращив цю книжку своєю майстерною редактурою та неймовірною увагою до деталей. Він допоміг створити структуру моєї історії. Не буде перебільшенням сказати, що без Імона це була б інша книжка – і аж ніяк не краща.

Подяка належить також колегам Тіни та Імона. Свєтлана Кац не пропустила жодної дрібнички, відповідала на всі мої запитання, а якось урятувала мій бекон. А Бен Гімен допомагав мені дотримуватися термінів, з якими доводиться мати справу до і після написання книжки. Я вдячний Марґарет Вімберґер, яка дбайливо відредагувала мій рукопис, виявивши безліч образних «гайок», які слід було «підтягнути», і «складок», які потрібно було випрасувати. Дякую також Ларрі Куперу за супровід видавничої підготовки рукопису аж до публікації.

Саймон Тревін із WME став першим захисником мене й моєї книжки у Лондоні. Він надіслав мою пропозицію Саймонові Торогуду з видавництва Headline Publishing Group, яке з непідробним ентузі-

азмом поставилося до цього проекту. Я дуже вдячний, що ця книжка дякуючи їм знайшла домівку і що завдяки їхнім зусиллям більше людей зможуть її прочитати.

Я вдячний моїм новим друзям і колегам з фонду «Нова Америка» за підтримку цієї книжки та моїх досліджень і за те інтелектуальне товариство, яке вони створили. Я страшенно щасливий бути його частиною, насамперед тому, що багато років захоплювався роботою вчених «Нової Америки». Особлива вдячність Андресу Мартінесу та Бекі Шафер, які так вміло виправляли й скеровували нашу групу. Бекі та Кірстен Берґи допомагали провести дослідження для деяких важливих розділів цієї книжки, і я дуже вдячний за допомогу. Дякую Пітерові Берґену за його доброту й підтримку моїх досліджень. Тім Маурер організував низку неймовірних обговорень питань кібербезпеки, які поглибили мої переконання. Я вдячний університету Арізони та його ректорові Майклу Кроу за допомогу в дослідженні війни майбутнього. І дякую Енн-Мері Слотер, президентці та генеральній директорці «Нової Америки», за її наставництво, підтримку й ентузіазм.

Я найщасливіший письменник у місті, тому що протягом трьох років моїм редактором у журналі Washingtonian була Деніз Віллс, а ще щасливішим мене робить наша з нею дружба. Вона – редакторка мрії, водночас наставниця й співавторка. Те саме можу сказати про Ноя Шахтмана, який повернув мене у відділ новин Foreign Policy. Ми страшенно веселилися кілька місяців, поки працювали разом, і так вийшло, що наша робота збіглася з найбільшою новиною 2013 року. Прекрасні були часи, Папі.

Дякую своїм колегам з Foreign Policy за щастя щодня приходити на роботу, особливо Йоші Дризену і нашій команді новин. Також дякую Бену Паукеру, Пітерові Скобліку, Мінді Кей Брікер і Девіду Роткопфу за все, що вони зробили, керуючи цим стрімким «кораблем», екіпаж якого невпинно збільшується.

Я завинив особливу вдячність плідним і проникливим репортажам деяких колег-журналістів, чия робота стала джерелом інформації для моїх досліджень, зокрема Сіобану Ґорману і Денні Яадрон з Wall Street Journal; Девіду Сенґеру, Ніколь Перлрот і Джону Маркоффу з New York Times; Еллен Накашіма з Washington Post; Тоні Ромму з Politico; Спенсеру Акерману з Guardian, який раніше вів блог Danger Room на сайті Wired; Кім Зеттер також з Wired, авторці блогу Threat Level;

Джозефу Менну з Reuters і Майклові Райлі з Bloomberg Businessweek. Кожен із них зробив переворот у цій сфері.

Дякую моєму другу й улюбленому обідньому компаньйонові Бенові Віттсу, чий блог Lawfare дає важливу поживу для серйозних роздумів на тему національної безпеки. Бен був моїм відданим радником і консультантом упродовж років і щедро ділився ідеями та часом.

Керол Джойнт була джерелом веселощів і сміху, допомоги і мудрості. Вона справжня подруга й класна журналістка, яка навчала та надихала мене. Також дякую Спенсерові Джойнту за те, що дозволяв мені затримуватися допізна, і за його дружбу.

Дейв Сінґлтон залишається для мене найкращим другом, якого лише можна уявити. Важко знайти когось, хто б зміг миритися, а частенько навіть терпіти деякі риси мого характеру. Ми познайомилися близько 15 років тому і тоді не знали, що наша дружба така рідкісна. Тепер знаємо.

Крістофер Кернс змушував мене заходитися від сміху й водночас замислюватися. Його готовність говорити те, що він думає, і думати те, що говорить, зробила мене кращим мислителем і сильнішим журналістом. Я дуже ціную наші розмови – і ті, за келихом, і ті, під час тривалих поїздок автомобілем.

Особлива вдячність моїм друзям Джейсону Келло і Джейсону Вілсону, чиї вдумливі роздуми про кібербезпеку – її сучасний стан і майбутнє – дали матеріал для багатьох частин цієї книжки. Їхній ентузіазм заразливий. А їхнє вміння перекладати складні технічні речі на просту, зрозумілу мову – дивовижне.

Моя давня наставниця та подруга Енн Лорен посідає особливе місце у серці того, про що я пишу. Понад десять років тому вона запропонувала мені писати про перехресні стежки технологій і безпеки. Поза сумнівом, якби не вона, я б цього не написав.

Дякую своїй сім'ї, особливо матері та батьку, Керол і Еду Гаррісам, за те, що вони були моїми вчителями й партнерами саме тоді, коли я цього потребував. Дякую Трою, Сюзан і Меделін Гаррісам, які щодня нагадують мені про родинну відданість. Моїй бабусі, Беттіанн Кінні, яка навчила мене розповідати історії і продовжує бути для мене завжди несподіваним джерелом натхнення. Дякую моїй свекрусі Мері де Фео та новим (тепер уже законним) членам моєї сім'ї, дякую за те, що принесли так багато сміху й щастя в моє життя, і за те, що пустили мене в своє.

Нарешті, дякую моєму чоловікові Джо де Фео, що я можу сказати такого, чого ти ще не знаєш? Якимось чином ти щодня робиш мене щасливішим, ніж я був дотепер. Ті місяці, які я провів за написанням цієї книжки, сидячи в одній кімнаті з двома маленькими монстрами, а ти працював у іншій, були найщасливішими з тих, що ми провели разом. Дякую за все, що ти зробив для мене і для нас. Дякую за те, що направляв мене. І дякую, що чекаєш на мене, коли я повертаюся додому. Це мій улюблений час дня.

ДЖЕРЕЛА ТА ПРИМІТКИ

Вступ

Це був колишній військовий офіцер: На підставі інтерв'ю з кількома відставними співробітниками Міністерства оборони, а також повідомлень у новинах.

Близько 7,5 млн рядків програмного коду: «Joint Strike Fighter: Strong Risk Management Essential as Program Enters Most Challenging Phase», US Government Accountability Office, GAO-09-711T, 20 травня 2009 року, http://www.gao.gov/products/GAO-09-711T.

У 2006 році вона уклала контрактів на $33,5 млрд: «Top 200 Contractors», Government Executive, 15 серпня 2007 року, http://www.govexec.com/magazine/2007/08/top-200-contractors/25086/.

Шпигуни викрали кілька терабайтів інформації, яка стосувалася конструкції винищувача: «Computer Spies Breach Fighter-Jet Project», Wall Street Journal, 21 квітня 2009 року, http://online.wsj.com/news/articles/SB124027491029837401.

Шпигуни проникли у мережі субпідрядників: «Security Experts Admit China Stole Secret Fighter Jet Plans», Australian, 12 березня 2012 року, http://www.theaustralian.com.au/news/world/security-experts-admit-china-stole-secret-fighter-jet-plans/story-fnb64oi6-1226296400154#mm-premium.

Він був дуже схожим на F-35: Andrea Shalal-Esa, «Pentagon Sees Risks, Progress on Lockheed's F-35 Jet», Reuters, 24 квітня 2013 року, http://www.reuters.com/article/2013/04/25/us-lockheed-fighter-dUSBRE93O00E20130425.

Керівники компаній докладно не знали, навіщо їх викликали до Пентаґону: Автор спілкувався з учасниками цієї зустрічі та людьми, які були присутні на брифінґах влади, а також із високопосадовцями з Міністерства оборони, що працювали над програмою DIB. Серед опитаних були Роберт Ленц, помічник міністра оборони, який наглядав за впровадженням програми; Джеймс Льюїс, експерт із кібербезпеки з Центру стратегічних і міжнародних досліджень, а також Стів Гокінз, який у 2009 році був віце-президентом компанії Raytheon з інформаційної безпеки. У 2013 року автор інтерв'ював також генерала Майкла Басла.

«Чимало людей, які увійшли до цієї кімнати темноволосими, вийшли з неї сивими»: З розмови автора з Джеймсом Льюїсом, квітень 2009 року.

Після тієї зустрічі Міністерство оборони почало надавати компаніям інформацію про кібершпигунів і небезпечних хакерів: Автор спілкувався з колишніми і нинішніми працівниками Міністерства оборони та Міністерства внутрішньої безпеки, а також чільниками корпорацій у 2009-му і 2013 році.

«Сполучені Штати стоять на межі "електронного Перл-Гарбору"»: З виступу Панетти в Музеї моря, повітря та космосу «Інтрепід» у Нью-Йорку 12 жовтня 2012 року, http://www.defensenews.com/article/20121012/DEFREG02/310120001/Text-Speech-by-Defense-U-S-Secretary-Leon-Panetta.

За п'ять місяців до того президент Барак Обама написав у газетній передовиці: Barack Obama, «Taking the Cyberattack Threat Seriously», Wall Street Journal, 19 липня 2012 року, http://online.wsj.com/news/articles/SB10000872396390444330904577535492693044650.

Директор ФБР Джеймс Комі: Комі давав свідчення Комітету сенату з внутрішньої безпеки і справ державного управління 14 листопада 2013 року, http://www.fbi.gov/news/testimony/homeland-threats-and-the-fbis-response.

У 2014 році уряд витратив понад $13 млрд на програми кібербезпеки: Chris Strohm, Todd Shields, «Obama Boosts Pentagon Cyber Budget Amid Rising Attacks», Bloomberg.com, 11 квітня 2013 року, http://www.bloomberg.com/news/2013-04-10/lockheed-to-general-dynamics-target-shift-to-cyber-spend.html.

...того ж року витрати на боротьбу зі зміною клімату, яку президент Обама назвав «сучасною глобальною загрозою», становили $11,6 млрд: Federal Climate Change Expenditures Report to Congress, серпень 2013 року, http://www.whitehouse.gov/sites/default/files/omb/assets/legislative_reports/fcce-report-to-congress.pdf.

1. Перша кібервійна

Боб Стасіо ніколи не планував ставати кіберсолдатом: Інтерв'ю автора, жовтень 2013 року.

У травні 2007 року, коли лейтенант Стасіо опинився у небезпечній ситуації: Інформація про нараду отримана завдяки двом великим інтерв'ю з Майком МакКоннеллом, на той час директором національної розвідки, а також з інтерв'ю з Френ Таунсенд, тогочасної радниці Буша з питань протидії тероризму, і з Дейлом Меєрроузом, відставним

генералом ВПС, який був у той час високопоставленим співробітником у штабі директора Національної розвідки. Оперативні подробиці кібероперацій АНБ і армії в Іраку отримані на умовах анонімності у трьох колишніх офіцерів військової розвідки, які брали в них участь. Деякі представники влади, зокрема й колишній командувач американських військ в Іраку Дейвід Петреус, відкрито розповідали про кібероперації в Іраку та внесок американських військових у перемогу.

Президент уже схвалив інший секретний проект: Крім інтерв'ю автора з нинішніми і колишніми американськими чиновниками й експертами з безпеки, джерелом інформації про операцію Stuxnet стали численні дослідницькі та новинні статті, серед яких найбільше інформації містять: Ralph Langner, «Stuxnet's Secret Twin», Foreign Policy, 21 листопада 2013 року, http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack#sthash.nq7VuMAC.8FWcquMx.dpbs; David Sanger, «Obama Order Sped Up Wave of Cyberattacks Against Iran», New York Times, 1 червня 2012 року, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all; James Bamford, «The Secret War», Wired, 12 червня 2013 року, http://www.wired.com/threatlevel/2013/06/general-keith-alexander-cyberwar/all/; Jim Finkle, «Researchers Say Stuxnet Was Deployed Against Iran in 2007», Reuters, 26 лютого 2013 року, http://www.reuters.com/article/2013/02/26/us-cyberwar-stuxnet-idUSBRE91P0PP20130226.

Минулий рік став для коаліції одним із найкривавіших: Джерело статистичних даних: iCasualties.org, http://icasualties.org/Iraq/index.aspx.

Кількість загиблих іракських цивільних: Там само, http://www.iraqbodycount.org/database/.

До вересня 2004 року, лише через 18 місяців після початку американської окупації, АНБ розробило секретну методику: Dana Priest, «NSA Growth Fueled by Need to Target Terrorists», Washington Post, 21 липня 2013 року, http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html.

Ця тенденція дає силам союзників безпрецедентні можливості: David E. Peterson, «Surveillance Slips into Cyberspace», Signal, лютий 2005 року, http://www.afcea.org/content/?q=node/629.

Оперативний центр розташовувався в залізобетонному ангарі на військово-повітряній базі в Баладі: Опис походить із декількох джерел, зокрема з інтерв'ю з колишнім старшим армійським офіцером, армійськими офіцерами й офіцерами розвідки, що служили в Іраку, а також із

публікацій, зокрема: Priest, «NSA Growth»; Joby Warrick, Robin Wright, «US Teams Weaken Insurgency in Iraq», Washington Post, 6 вересня 2008 року, http://articles.washingtonpost.com/2008-09-06/world/36869600_1_salim-abdallah-ashur-abu-uthman-iraqi-insurgents. Див. також: David H. Petraeus, «How We Won in Iraq», Foreign Policy, 29 жовтня 2013 року, http://www.foreignpolicy.com/articles/2013/10/29/david_petraeus_how_we_won_the_surge_in_iraq?page=0,3; Stanley A. McChrystal «It Takes a Network», Foreign Policy, 22 лютого 2011 року, http://www.foreignpolicy.com/articles/2011/02/22/it_takes_a_network.

У вересні 2007 року внаслідок американського рейду в селі Сінджар: Див.: Eric Schmitt, Thom Shanker, Counterstrike: The Untold Story of America's Secret Campaign Against Al Qaeda (New York: Times Books, 2011).

Фахівці АНБ розробили операцію під назвою «Полярний бриз»: Scott Shane, «No Morsel Too Minuscule for All-Consuming NSA», New York Times, 2 листопада 2013 року, http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?_r=2&pagewanted=all&&pagewanted=print.

Місцеві християни, які жили в Дорі протягом десятиліть: Ned Parker, "Christians Chased Out of District," Los Angeles Times, June 27, 2007, http://articles.latimes.com/2007/iun/27/world/fg-christians27.

*В операції, яка розпочалась у червні 2007 року, брали участь близько 10 тисяч солдатів: «*US Launches Major Iraq Offensive», BBC News, 19 червня 2007 року, http://news.bbc.co.uk/2/hi/middle_east/6766217.stm; «Start of 'Arrowhead Ripper' Highlights Iraq Operations», American Forces Press Service, 19 червня 2007 року, http://www.defense.gov/News/NewsArticle.aspx?ID=46459.

Хакерство у телекомунікаційних мережах, якими користувалися лідери «Аль-Каїди» в Іраку, допомогло ТАО звільнити передмістя Баґдада від терористичної влади, а американським військам – захопити або знищити принаймні десятьох чільників «Аль-Каїди» на полі бою: Warrick, Wright, «US Teams Weaken Insurgency».

За перші шість місяців 2008 року «Аль-Каїда» влаштувала лише 28 вибухів: Там само.

Петреус вважав, що ця нова кіберзброя «була головною причиною значного прогресу американського війська»: Звіт АНБ про програму стеження, 9 серпня 2013 року, http://cryptome.org/2013/08/nsa-13-0809.pdf. Також див.: Petraeus, «How We Won in Iraq».

2. RTRG

Штаб-квартира АНБ переїхала до цього містечка: 60 Years of Defending Our Nation, офіційна історія АНБ, опублікована 2012 року до ювілею агентства, http://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf.

Агентство створило підрозділ для цілодобового стеження: Опис так званої президентської програми із ведення стеження та програми Stellar Wind походить із численних інтерв'ю з колишніми урядовцями, а також зі звіту головного ревізора АНБ ST-09-002 (робочий проект) від 24 березня 2009 року, оприлюдненого Едвардом Сноуденом. Копія цього документа доступна за посиланням: http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection. Див. також книжку автора: The Watchers: The Rise of America's Surveillance State (New York: Penguin Press, 2010).

У літанії кодових назв АНБ: Невідомо, як саме в АНБ підбирають кодові назви. У 1960-х роках за підбір кодових назв у АНБ відповідав лише один співробітник, який, очевидно, вибирав назви навмання, вважаючи, що вони не повинні бути пов'язаними з діяльністю агентства. Див.: Tom Bowman, «Why Does the NSA Keep an EGOTISTICALGIRAFFE? It's Top Secret», NPR News, 10 листопада 2013 року, http://www.npr.org/2013/11/10/244240199/why-does-the-nsa-keep-an-egotisticalgiraffe-its-top-secret.

«Він належав до тих хлопців, про яких ніколи не чує нація...»: Matt Schudel, «Pedro Luis Rustan, 65, Aerospace and Surveillance Innovator», Obituaries, Washington Post, 7 липня 2012 року, http://articles.washingtonpost.com/2012-07-07/local/35486174_1_nro-spy-satellites-national-reconnaissance-office.

В інтерв'ю галузевому виданню 2010 року Рустан говорив: «Change Agent», C4ISR Journal, 8 жовтня 2010 року, http://www.defensenews.com/article/20101008/C4ISR01/10080311/.

«Чітке розуміння іракцями того, що іранські елементи підтримували членів найекстремальніших шиїтських угруповань...»: David H. Petraeus, «How We Won in Iraq», Foreign Policy, 29 жовтня 2013 року, http://www.foreignpolicy.com/articles/2013/10/29/david_petraeus_how_we_won_the_surge_in_iraq?page=0,3.

Елітний підрозділ хакерів агентства – відділ операцій з особливим доступом (Tailored Access Operations – TAO) – віддалено встановив шпигунське програмне забезпечення на мобільні телефони агентів «Аль-Каїди»: Craig Whitlock and Barton Gellman, «To Hunt Osama bin Laden, Satellites Watched over Abbottabad, Pakistan, and Navy SEALs»,

Washington Post, 29 серпня 2013 року, http://articles.washingtonpost.com/2013-08-29/world/41712137_1_laden-s-osama-bin-laden.

3. Створення кіберармії

Армія теж підтримала ініціативу і почала шукати способи «вирубати світло Тегеранові»: З інтерв'ю автора з колишнім офіцером військової розвідки.

Його колишній шеф Дік Чейні сказав: Автор провів низку інтерв'ю з МакКоннеллом у його офісі в 2009 році.

А місяць потому АНБ поповнило нову систему збору інформації: Список компаній, що брали участь у програмі спостереження Prism, походить із презентації АНБ, оприлюдненої колишнім співробітником агентства Едвардом Сноуденом і опублікованої спочатку газетами Washington Post і Guardian, а потім передрукованої іншими ЗМІ. Подробиці щодо програми Prism були отримані також під час інтерв'ю автора з нинішніми і колишніми держслужбовцями.

Після перемоги сенатора Барака Обами на президентських виборах: Інтерв'ю з МакКоннеллом.

Згодом, під час особистої зустрічі з Бушем: Див.: David Sanger, «Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power» (New York: Crown, 2012).

Щоб з'ясувати це, 7 травня 2010 року: Інформація про «Воєнну гру Шрайвера» та її результати отримані з трьох джерел: авторського інтерв'ю з генерал-лейтенантом Майклом Басла, керівником підрозділу інформаційного домінування та головним фахівцем із питань інформації військово-повітряних сил; з журналу High Frontier: The Journal for Space and Cyberspace Professionals 7, № 1, який був цілком присвячений описові й аналізу минулої гри, http://www.afspc.af.mil/shared/media/document/AFD-101116-028.pdf; зі статті Robert S. Dudney «Hard Lessons at the Schriever Wargame», Air Force Magazine 94, № 2, лютий 2011 року, http://www.airforcemag.com/MagazineArchive/Pages/2011/February%202011/0211wargame.aspx.

Однак під час приватних розмов деякі розвідники розповідали: З авторських інтерв'ю з урядовцями, експертами та керівниками компаній. Інтерв'ю про кіберможливості китайців дали екс-президент Союзу індустрії кібербезпеки Тім Беннетт; Стівен Спунамор, колишній генеральний директор компанії Cybrinth, яка надавала послуги у сфері кібербезпеки державним і корпоративним клієнтам; і Джоель Бреннер, голова контррозвідки, що підпорядковується директорові національної розвідки. Див. також: Shane Harris, «China's Cyber-Militia», National

Journal, 31 травня 2008 року, http://www.nationaljournal.com/magazine/china-s-cyber-militia-20080531.

«Можливо, керівництво доручило хакеру викрасти схему систем…»: Інтерв'ю автора.

Це сталося шість років потому, як у комп'ютерах законодавців виявили шпигунське програмне забезпечення: З авторських інтерв'ю зі співробітниками Конгресу та людьми, що здійснювали розслідування, а також із матеріалів закритої наради, проведеної експертами у сфері безпеки в палаті представників, отриманих автором. Див.: Shane Harris, «Hacking the Hill», National Journal, 20 грудня 2008 року, http://www.nationaljournal.com/magazine/hacking-the-hill-20081220.

Торговельна палата США: Представники Торговельної палати США неодноразово коментували це. Див.: http://www.pcworld.com/article/260267/senate_delays_maybe_kills_cybersecurity_bill.html.

Ще одна директива, відома під назвою PDD-20: Список директив президента Обами можна знайти на сайті Федерації американських учених: http://www.fas.org/irp/offdocs/ppd/. Директиву PDD-20, що стосується кібернетичних армійських операцій, оприлюднив колишній співробітник АНБ Едвард Сноуден. Текст директиви був опублікований у червні 2013 року.

Підрозділ АНБ, відомий як Відділ порушень: Scott Shane, «No Morsel Too Minuscule for All-Consuming N. S. A.», New York Times, 2 листопада 2013 року, http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html.

Найсуттєвіша зміна від початків кібервійни: Див. Chairman of the Joint Chiefs of Staff, Joint Targeting, Joint Publication 3-60, 31 січня 2013 року, http://cfr.org/content/publications/attachments/Joint_Chiefs_of_Staff-Joint_Targeting_31_January_2013.pdf.

За допомогою електромагнітних хвиль хакери атакують бортові системи спостереження: Генерал-лейтенант Герберт Карлайл, тоді заступник командувача операціями ВПС, розповів про тактику китайців на конференції з питань оборони у Вашинґтоні в 2012 році. Див.: David Fulghum, «China, US Chase Air-to-Air Cyberweapon», Aviation Week, 9 березня 2012 року.

«З їхнього боку була залучена величезна кількість людських ресурсів»: Dune Lawrence, Michael Riley, «A Chinese Hacker's Identity Unmasked», Bloomberg Businessweek, 14 лютого 2013 року, http://www.businessweek.com/articles/2013-02-14/a-chinese-hackers-identity-unmasked.

«Бракує фахівців із критично важливими навичками»: Генерал-майор Джон Дейвіс, виступ на Міжнародному кібернетичному симпозіумі

Військової асоціації зв'язку та електроніки (AFCEA), конференц-зал Балтімора, 25 червня 2013 року, http://www.dvidshub.net/video/294716/mg-davis-afcea#.UpSILmQ6Ve6#ixzz2lkc87oRy.

«Університети не хочуть цього навчати»: Jason Koebler, «NSA Built Stuxnet, but Real Trick Is Building Crew of Hackers», US News & World Report, 8 червня 2012 року, http://www.usnews.com/news/articles/2012/06/08/nsa-built-stuxnet-but-real-trick-is-building-crew-of-hackers.

4. Поле битви – інтернет

Найобдарованіші та найдосвідченіші хакери агентства: Щоб отримати додаткову інформацію про TAO, див. статті журналіста й історика розвідки Метью Ейда, який багато писав про цей відділ, зокрема: «The NSA's New Code Breakers», Foreign Policy, 16 жовтня 2013 року, http://www.foreignpolicy.com/articles/2013/10/15/the_nsa_s_new_codebreakers?page=0%2C1#sthash.jyc1d12P.dpbs.

Едвард Сноуден розповів китайським журналістам: Lana Lam, «NSA Targeted China's Tsinghua University in Extensive Hacking Attacks, Says Snowden», South China Morning Post, 22 червня 2013 року, http://www.scmp.com/news/china/article/1266892/exclusive-nsa-targeted-chinas-tsinghua-university-extensive-hacking?page=all.

Згідно з міжнародним дослідженням, Цінхуа є провідним університетом континентального Китаю: QS World University Rankings, 2013 рік, http://www.topuniversities.com/university-rankings/university-subject-rankings/2013/computer-science-and-information-systems.

Саме цього року хакери отримали нагороди: Matthew Aid, Secret Sentry: The Untold History of the National Security Agency (New York: Bloomsbury Press, 2009 рік), http://www.amazon.com/The-Secret-Sentry-National-Security/dp/B003L1ZX4S.

Метью Ейд пише, що «TAO стало бажаним місцем роботи»: Matthew Aid, «Inside the NSA's Ultra-Secret China Hacking Group», Foreign Policy, 15 жовтня 2013 року, http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group.

У другій половині 2009 року невеличка команда Гавайського центру націлилася на високопріоритетні об'єкти з «Аль-Каїди»: Інформацію надав колишній співробітник Гавайського центру, який брав участь у розробці операції.

У надсекретному звіті, що стосувався операції під назвою Flatliquid: Уперше про операцію Flatliquid написала газета Der Spiegel. Публікація повстала на основі документів, наданих колишнім співробітником АНБ Едвардом Сноуденом. Див.: Jens Glüsing et al., «Fresh Leak on US Spying:

NSA Accessed Mexican President's Email», Spiegel Online, International edition, 20 жовтня 2013 року, http://www.spiegel.de/international/world/nsa-hacked-e-mail-account-of-mexican-president-a-928817.html.

Кілька десятків секретних співробітників ЦРУ: Matthew Aid, «The CIA's New Black Bag Is Digital», Foreign Policy, 18 серпня 2013 року, http://www.foreignpolicy.com/articles/2013/07/16/the_cias_new_black_bag_is_digital_nsa_cooperation#sthash.XUr4mt5h.dpbs.

ЦРУ також створило власний хакерський відділ: Barton Gellman, Ellen Nakashima, «US Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show», Washington Post, 30 серпня 2013 року, http://articles.washingtonpost.com/2013-08-30/world/41620705_1_computer-worm-former-u-s-officials-obama-administration.

Проте в систему аналізу завантажувалася й інша інформація: Див.: Siobhan Gorman, Adam Entous, Andrew Dowell, «Technology Emboldened the NSA», Wall Street Journal, 9 червня 2013 року. http://online.wsj.com/news/articles/SB10001424127887323495604578535290627442964; а також: Noah Shachtman, «Inside DARPA's Secret Afghan Spy Machine», Danger Room, Wired, 21 липня 2011 року, http://www.wired.com/dangerroom/2011/07/darpas-secret-spy-machine/.

Старшого рядового авіації, лінгвіста за освітою, стурбувала інформація про «телефонну нараду» лідерів «Аль-Каїди»: John Reed, «An Enlisted Airman Deciphered al-Qaeda's 'Conference Call' of Doom», Foreign Policy, 18 вересня 2013 року.

Нарада керівників «Аль-Каїди» відбувалася не в телефонному режимі: Eli Lake, Josh Rogin, «US Intercepted al-Qaeda's 'Legion of Doom' Conference Call», Daily Beast, 7 серпня 2013 року, http://www.thedailybeast.com/articles/2013/08/07/al-qaeda-conference-call-intercepted-by-u-s-officials-sparked-alerts.html; а також Eli Lake, «Courier Led US to al-Qaeda Internet Conference», Daily Beast, 20 серпня 2013 року, http://www.thedailybeast.com/articles/2013/08/20/exclusive-courier-led-u-s-to-al-qaeda-internet-conference.html.

…після повернення з Іраку: Інтерв'ю автора з Бобом Стасіо, 14 жовтня 2013 року.

5. Ворог серед нас

…Александер попередив свою команду про наближення «війни в мережі»: Siobhan Gorman, «Costly NSA Initiative Has a Shaky Takeoff», Baltimore Sun, 11 лютого 2007 року, http://articles.baltimoresun.com/2007-02-11/news/0702110034_1_turbulence-cyberspace-nsa.

Тому не дивно, що 2006 року АНБ почало робити спроби підірвати анонімні можливості технології Tor: Детальніше про операції АНБ проти мережі Tor див.: Shane Harris, John Hudson, «Not Even the NSA Can Crack the State Department's Favorite Anonymous Network», Foreign Policy, 7 жовтня 2013 року, http://thecable.foreignpolicy.com/posts/2013/10/04/not_even_the_nsa_can_crack_the_state_departments_online_anonymity_tool#sthash.1H45fNxT.dpbs; Barton Gellman, Craig Timberg, Steven Rich, «Secret NSA Documents Show Campaign Against Tor Encrypted Network», Washington Post, 4 жовтня 2013 року, http://articles.washingtonpost.com/2013-10-04/world/42704326_1_nsa-officials-national-security-agency-edward-snowden; James Ball, Bruce Schneir, Glenn Greenwald, «NSA and GCHQ Target Tor Network That Protects Anonymity of Web Users», Guardian, 4 жовтня 2013 року, http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

…хакери розглядали можливість організації збою у мережі Tor: Презентацію можна знайти за посиланням: http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document.

У рамцях секретної програми SIGINT Enabling Project: З авторських інтерв'ю зі співробітниками технологічної компанії та експертами. Також див. секретні бюджетні документи, що містять детальну інформацію про проект, опубліковані в New York Times: http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us.

Завдяки тісній співпраці з ФБР АНБ дізналося: Glenn Greenwald et al., «Microsoft Handed the NSA Access to Encrypted Messages», Guardian, 11 липня 2013 року, http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

Проте за лаштунками цього здебільшого відкритого процесу: Див. Nicole Perlroth, Jeff Larson, Scott Shane, «NSA Able to Foil Basic Safeguards of Privacy on the Web», New York Times, 5 вересня 2013 року, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all.

Відомий експерт із комп'ютерної безпеки Брюс Шнаєр: Bruce Schneier, «Did NSA Put a Secret Backdoor in New Encryption Standard?» Wired, 15 листопада 2007 року, http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115.

Згодом АНБ посилалося на раннє впровадження алгоритму: Joseph Menn, «Secret Contract Tied NSA and Security Industry Pioneer», Reuters, http://mobile.reuters.com/article/idUSBRE9BJ1C220131220?irpc=932.

Нойберґер назвала NIST «надзвичайно шанованим, близьким партнером у багатьох питаннях»: Повний аудіозапис інтерв'ю Нойберґер доступний за посиланням: http://www.lawfareblog.com/2013/12/lawfare-podcast-episode-55-inside-nsa-part-iv-we-speak-with-anne-neuberger-the-woman-on-front-lines-of-nsas-relations-with-industry/.

«NIST відкрито запропонував [стандарт] у серпні 1991 року…»: Відомості, отримані Інформаційним центром захисту електронних персональних даних (EPIC), доступні за посиланням: http://epic.org/crypto/dss/new_nist_nsa_revelations.html.

У 1997 році, згідно з нещодавно розсекреченим інформаційним бюлетенем АНБ: Journal of Technical Health 23, № 1 (весна 1997 року). http://cryptome.org/2013/03/nsa-cyber-think.pdf.

Цей ринок не зовсім легальний: Інформація про тіньовий ринок уразливостей нульового дня отримана під час інтерв'ю з нинішніми та колишніми держслужбовцями США, а також із технічними експертами, зокрема з Крісом Саґояном – головним технологом і старшим аналітиком програми захисту свободи слова, конфіденційності і технологій Американського союзу захисту цивільних свобод (ACLU). Додатковим джерелом інформації стали документи та статті у вільному доступі.

Наприклад, 2005 року аспірант Каліфорнійського університету в Лос-Анджелесі виявив: Tadayoshi Kohno, Andre Broido та k. c. claffy, «Remote Physical Device Fingerprinting», https://www.caida.org/publications/papers/2005/fingerprinting/KohnoBroidoClaffy05-devicefingerprinting.pdf.

Через рік після публікації статті: Steven J. Murdoch, «Hot or Not: Revealing Hidden Services by Their Clock Skew», http://www.cl.cam.ac.uk/~sjm217/papers/ccs06hotornot.pdf. Див. також Quinn Norton, «Computer Warming a Privacy Risk», Wired, 29 грудня 2006 року, http://www.wired.com/science/discoveries/news/2006/12/72375.

«Ми не продаємо зброю, ми продаємо інформацію»: Joseph Menn, «US Cyberwar Strategy Stokes Fear of Blowback», Reuters, 10 травня 2013 року, http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510.

У 2013 році бюджет АНБ на придбання експлойтів нульового дня: Barton Gellman, Ellen Nakashima, «US Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show», Washington Post, 30 серпня 2013 року, http://articles.washingtonpost.com/2013-08-30/world/41620705_1_computer-worm-former-u-s-officials-obama-administration.

«Випускники цієї програми стають [для агентства] безцінними працівниками…»: «About the Program», Systems and Network Interdisciplinary Program, http://www.nsa.gov/careers/_files/SNIP.pdf.

Компанія неодноразово опинялася під прицілом: John Markoff, «Cyber Attack on Google Said to Hit Password System», New York Times, 19 квітня 2010 року.

6. Найманці

«"Хірургічна пила" – це інструмент для створення схеми…»: Aram Roston, «Nathaniel Fick, Former CNAS Chief, to Head Cyber Targeting Firm», C4ISR Journal, січень–лютий 2013 року, http://www.defensenews.com/article/20130115/C4ISR01/301150007/Nathaniel-Fick-Former-CNAS-Chief-Heads-Cyber-Targeting-Firm.

Внутрішня документація показує: Michael Riley and Ashlee Vance, "Cyber Weapons: The New Arms Race," Bloomberg Businessweek, July 20, 2011, http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html#p4.

«Врешті-решт, нам необхідно дозволити корпораціям…»: Andy Greenberg, «Founder of Stealthy Security Firm Endgame to Lawmakers: Let US Companies 'Hack Back'», Forbes, 20 вересня 2013 року, http://www.forbes.com/sites/andygreenberg/2013/09/20/founder-of-stealthy-security-firm-endgame-to-lawmakers-let-u-s-companies-hack-back/.

«Якщо ви прогнозуєте, що війни майбутнього відбуватимуться у кіберпросторі, хіба не варто мати власну кіберармію?»: Joseph Menn, «US Cyberwar Strategy Stokes Fear of Blowback», Reuters, 10 травня 2013 року, http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510.

…Один із провідних гравців у цьому бізнесі: Інформація про методи роботи компанії CrowdStrike отримана під час розмов автора зі Стівеном Чабінські, головним юридичним радником компанії, що в минулому обіймав керівну посаду в ФБР, у липні та серпні 2013 року. Додаткова інформація походить із сайту компанії.

Проте співзасновник CrowdStrike Дмітрій Альперович в інтерв'ю 2013 року розповів: John Seabrook, «Network Insecurity: Are We Losing the Battle Against Cyber Crime?» New Yorker, 20 травня 2013 року.

Маркетинґові документи фірми Gamma: Jennifer Valentino-Devries, «Surveillance Company Says It Sent Fake iTunes, Flash Updates», Wall Street Journal, 21 листопада 2011 року, http://blogs.wsj.com/digits/2011/11/21/surveillance-company-says-it-sent-fake-itunes-flash-updates-documents-show/.

Дослідники в сфері безпеки стверджують: Vernon Silver, «Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma», Bloomberg.com, 25 липня 2012 року, http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html.

Мансур мимохіть завантажив шпигунську програму: Vernon Silver, «Spyware Leaves Trail to Beaten Activist Through Microsoft Flaw», Bloomberg.com, 12 жовтня 2012 року, http://www.bloomberg.com/news/2012-10-10/spyware-leaves-trail-to-beaten-activist-through-microsoft-flaw.html.

Немає жодних доказів того, що Hacking Team знала або була якимсь чином причетна до нападів на Мансура: Adrianne Jeffries, «Meet Hacking Team, the Company That Helps the Police Hack You», The Verge, 13 вересня 2013 року, http://www.theverge.com/2013/9/13/4723610/meet-hacking-team-the-company-that-helps-police-hack-into-computers.

Восени 2010 року: Shane Harris, «Killer App: Have a Bunch of Silicon Valley Geeks at Palantir Technologies Figured Out How to Stop Terrorists?» Washingtonian, 31 січня 2012 року, http://www.washingtonian.com/articles/people/killer-app/.

Компанія заявила, що влада найняла Tiversa: Sindhu Sundar, «LabMD Says Gov't Funded the Data Breach at Probe's Center», Law360, http://www.law360.com/articles/488953/labmd-says-gov-t-funded-the-data-breach-at-probe-s-center.

Згідно з документами судової справи, компанія Triversa виявила інформацію про пацієнтів LabMD у піринґовій мережі: Судові документи можна переглянути за посиланням: https://www.courtlistener.com/ca11/5cG6/labmd-inc-v-tiversa-inc/?q=%22computer+fraud+and+abuse+act%22&refine=new&sort=dateFiled+desc.

«Це протизаконно»: Авторське інтерв'ю.

У червні 2013 року корпорація Microsoft об'єдналася з кількома найбільшими фінансовими організаціями: Jim Finkle, «Microsoft, FBI Take Aim at Global Cyber Crime Ring», Reuters, 5 червня 2013 року, http://www.reuters.com/article/2013/06/05/net-us-citadel-botnet-idUSBRE9541KO20130605.

Юристи компанії знайшли нові правові підстави для судових позовів: Jennifer Warnick, «Digital Detectives: Inside Microsoft's Headquarters for the Fight Against Cybercrime» Microsoft/Stories, http://www.microsoft.com/en-us/news/stories/cybercrime/index.html.

Опитування 181 респондента, проведене 2012 року: nCirle, Black Hat Survey, BusinessWire, липень 2012 року, http://www.businesswire.com/news/home/20120726006045/en/Black-Hat-Survey-36-Information-Security-Professionals#.UtMp8WRDtYo.

Рік Говард, до того як стати приватним кібершпигуном: Авторське інтерв'ю, серпень 2013 року.

7. Поліцейські стають шпигунами

Це відділ технологій перехоплення інформації (Data Intercept Technology Unit): Інформація про відділ походить з інтерв'ю автора з нинішніми та колишніми співробітниками правоохоронних органів, представниками технологічної галузі та експертами з питань права у листопаді 2013 року, а також із сайтів ФБР. Для отримання додаткової інформації про програму «Чарівний ліхтар» див.: Bob Sullivan, «FBI Software Cracks Encryption Wall», MSNBC, 20 листопада 2001 року, http://www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall/#.UsWEOmRDtYo; див. також: Ted Bridis, «FBI Develops Eavesdropping Tools», Associated Press, 21 листопада 2001 року, http://globalresearch.ca/articles/BRI111A.html.

«Бюро зосереджується передусім на зборі інформації і передачі її АНБ»: Інтерв'ю автора, жовтень 2013.

Від 2001-го до 2009 року кількість агентів у відділі протидії тероризму збільшилася вдвічі: G. W. Shulz, «FBI Agents Dedicated to Terror Doubled in Eight Years», Center for Investigative Reporting, 26 квітня 2010, http://cironline.org/blog/post/fbi-agents-dedicated-terror-doubled-eight-years-671.

«…Ми просто збираємо розвіддані»: Авторське інтерв'ю, листопад 2013 року.

Згідно зі звітом Фрідмана, наступного ранку він зустрівся з агентом ФБР: Звіт Фрідмана можна прочитати за посиланням: http://www.stratfor.com/weekly/hack-stratfor.

Згодом один хакер звинуватив компанію в «шпигунстві за цілим світом»: Vivien Lesnik Weisman, «A Conversation with Jeremy Hammond, American Political Prisoner Sentenced to 10 Years», Huffington Post, 19 листопада 2013 року, http://www.huffingtonpost.com/vivien-lesnik-weisman/jeremy-hammond-q-and-a_b_4298969.html.

Проте Stratfor не була однією з них: Nicole Perlroth, «Inside the Stratfor Attack», Bits, New York Times, 12 березня 2012 року, http://bits.blogs.nytimes.com/2012/03/12/inside-the-stratfor-attack/?_r=0.

Ба більше, хакери надіслали до WikiLeaks 5 млн електронних листів: Там само.

Компанії довелося задовольнити груповий судовий позов: Basil Katz, «Stratfor to Settle Class Action Suit Over Hack», Reuters, 27 червня

2012 року, http://www.reuters.com/article/2012/06/28/us-stratfor-hack-lawsuit-idUSBRE85R03720120628.

У 2013 році Міністерство юстиції вимагало від судді відкласти винесення вироку: Matthew J. Schwartz, «Anonymous Hacker Claims FBI Directed LulzSec Hacks», Dark Reading, InformationWeek, 27 серпня 2013 року, http://www.informationweek.com/security/risk-management/anonymous-hacker-claims-fbi-directed-lulzsec-hacks/d/d-id/1111306?.

«Багатьом невідомо, що Сабу використовував своїх маріонеток…»: Заяву Гаммонда можна прочитати за посиланням: http://freejeremy.net/yours-in-struggle/statement-by-jeremy-hammond-on-sabus-entencing/.

8. Ще один «мангеттенський проект»

– Ще щось?: Інформація про зустріч отримана під час двох великих інтерв'ю з Майком МакКоннеллом, який обіймав тоді посаду директора національної розвідки. Частина інформації отримана з інтерв'ю з Френ Таунсенд, радницею Буша з питань протидії тероризму, і з інтерв'ю з відставним генералом ВМС Дейлом Меєрроузом, який у 2009–2010 роках був старшим офіцером штабу директора національної розвідки.

Окрім креслень і секретних розробок систем озброєння, які хакери викрали або збиралися викрасти: Перелік озброєнь і технологій можна знайти в звіті Наукової ради з оборонної політики Resilient Military Systems and the Advanced Cyber Threat за січень 2013 року, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf. Список не був оприлюднений, але він є в газеті Washington Post і його можна переглянути за посиланням: http://www.washingtonpost.com/world/national-security/a-list-of-the-us-weapons-designs-and-technologies-compromised-by-hackers/2013/05/27/a95b2b12-c483-11e2-9fe2-6ee52d0eb7c1_story.html.

Це був надзвичайний захід: Див. David Petraeus, «How We Won in Iraq», Foreign Policy, 29 жовтня 2013 року, http://www.foreignpolicy.com/articles/2013/10/29/david_petraeus_how_we_won_the_surge_in_iraq?page=0,3.

…«почасти наглядову, почасти сторожову і почасти снайперську»: William J. Lynn III, «Defending a New Domain: The Pentagon's Cyberstrategy», Foreign Affairs, вересень–жовтень 2010 року, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

9. «Американська картеч»

П'ятниця 24 жовтня 2008 року стала несподівано метушливим днем: Подробиці операції «Американська картеч» отримані під час інтерв'ю

автора з нинішніми й колишніми офіцерами армії та розвідки, зокрема з розмов із генералом Майклом Басла у червні 2013 року й з аналітиком Міністерства оборони, який брав участь у програмі (розмова відбулася в листопаді 2013 року). Додаткові джерела інформації: Ellen Nakashima, «Cyber-Intruder Sparks Massive Cyber Response – and Debate Over Dealing with Threats», Washington Post, 8 грудня 2011 року, http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html; Jason Healey, ed., A Fierce Domain: Conflict in Cyberspace 1986 to 2012 (Vienna, VA: Cyber Conflict Studies Association, 2013); William J. Lynn III, «Defending a New Domain: The Pentagon's Cyberstrategy», Foreign Affairs, вересень – жовтень 2010 року, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

«*Так багато слів*»: Інтерв'ю автора, червень 2013 року.

«Наші очі розплющилися»: Там сам.

За словами колишнього інформаційного аналітика з Міністерства оборони: Інтерв'ю автора, листопад 2013 року.

Деякі офіційні особи, що працювали над операцією «Американська картеч»: Noah Shachtman, «Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack», Danger Room, Wired, 25 серпня 2010 року, http://www.wired.com/dangerroom/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/.

«Александер, наче чарівник із країни Оз, створив ауру неймовірних можливостей…»: З інтерв'ю з колишнім співробітником адміністрації, який співпрацював із Александером і Білим домом у питаннях кібербезпеки, серпень 2013 року.

«Якщо ви дістанете USB-накопичувач і вставите його в мій комп'ютер…»: Інтерв'ю автора, березень 2012 року.

10. «Секретний складник»

Під час передвиборної кампанії китайські шпигуни зламали електронні поштові скриньки членів виборчого штабу Обами: Michael Isikoff, «Chinese Hacked Obama, McCain Campaigns, Took Internal Documents, Officials Say», NBC News, 6 червня 2013 року. http://investigations.nbcnews.com/_news/2013/06/06/18807056-chinese-hacked-obama-mccain-campaigns-took-internal-documents-officials-say.

Тепер, коли 44-й президент США: «Securing Cyberspace for the 44th Presidency", Center for Strategic and International Studies, грудень 2008 року, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

Серед іншого там були описи зламування електронної пошти: Інтерв'ю автора з американськими чиновниками, нинішніми і колишніми, а також технічним експертом, який проаналізував китайське шпигунське ПЗ, травень 2008 року.

Ці та інші проникнення в мережу: Інтерв'ю автора, 2013 рік.

Хакери розіграли надзвичайно майстерний сценарій: Інформація про фішинґову атаку міститься в телеграмі Державного департаменту США, оприлюдненій сайтом WikiLeaks. Див. також авторську статтю «Chinese Spies May Have Tried to Impersonate Journalist Bruce Stokes», Washingtonian, 2 лютого 2011 року, http://www.washingtonian.com/blogs/capitalcomment/washingtonian/chinese-spies-may-have-tried-to-impersonate-journalist-bruce-stokes.php.

У 2009 році один із підлеглих Гілларі Клінтон: Авторські інтерв'ю з держслужбовцем і колишнім співробітником Держдепартаменту, проведені у 2012–2013 роках.

Чарлі Крум, відставний генерал ВПС: Інтерв'ю автора, січень 2014 року.

Обама не сказав, де саме це сталося, проте розвідники та військові виснували: Про зв'язок між хакерським атаками та знеструмленнями в Бразилії першими повідомили журналісти програми 60 Minutes на каналі CBS News 6 листопада 2009 року, http://www.cbsnews.com/news/cyber-war-sabotaging-the-system-06-11-2009/. У січні 2008 року Том Донаг'ю, старший офіцер ЦРУ з питань кібербезпеки, публічно заявив, що хакери зламали комп'ютерні системи комунальних компаній за межами США і вимагали викуп. Донаг'ю виступив на конференції з питань безпеки в Новому Орлеані. «Це наслідки вторгнення через інтернет», – сказав він, проте не назвав ані країни, ані міста, де відбулася атака.

Власники й оператори електромереж спростовували чутки про спричинені хакерами знеструмлення: Див.: Shane Harris, «China's Cyber-Militia», National Journal, 31 травня 2008 року, http://www.nationaljournal.com/magazine/china-s-cyber-militia-20080531.

Він привіз із собою згорнутий аркуш паперу: Інтерв'ю автора з колишнім американським держслужбовцем, 2013 рік.

У АНБ цей план назвали «Транш 2»: Інтерв'ю автора з колишніми співробітниками розвідки й адміністрації президента, 2011–2013 роки.

Александер розповів їм, що закон, який зобов'яже компанії передавати дані, не схвалює адміністрація президента: Авторські інтерв'ю з двома конгресменами, які були присутні на нараді з Александером, а також із колишнім представником адміністрації, який співпрацю-

вав із Александером і Білим домом у питаннях кібербезпеки, серпень 2013 року.

«Люди з центру незадоволені мною»: Інтерв'ю автора з колишнім співробітником апарату Конгресу, присутнім під час розмови, жовтень 2013 року.

Іще до початку роботи у міністерстві у перші дні *2009 року*: Інформація про роботу Лют в Міністерстві внутрішньої безпеки отримана від колишніх міністерських працівників, од високопосадовця з правоохоронних органів, який співпрацював із багатьма агентствами та їхніми керівниками у питаннях кібербезпеки, і співробітників апарату Конгресу, які працювали в комітетах, що опікувалися діяльністю Міністерства внутрішньої безпеки.

Центр нагляду за надзвичайними мережевими ситуаціями Міністерства внутрішньої безпеки: Richard L. Skinner, «Einstein Presents Big Challenge to U. S.-CERT», GovInfo Security, 22 червня 2010 року, http://www.govinfosecurity.com/einstein-presents-big-challenge-to-us-cert-a-2677/op-1.

Род Бекстром звільнився у березні: Заяву про звільнення Бекстрома надрукувала газета *Wall Street Journal*, http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf.

Фактично вона була технофобкою: Авторське інтерв'ю, 28 вересня 2012 року.

«Уявіть, що телефонний довідник Мангеттена – це всесвіт шкідливого ПЗ»: Інтерв'ю автора з двома колишніми співробітниками адміністрації, вересень–жовтень 2013 року.

«Є припущення, що коли інформація засекречена, то вона правдива»: Інтерв'ю автора з високопосадовцем із правоохоронних органів, вересень 2013 року.

«Його позиція виглядала так: "Якби ви лише знали…»: Інтерв'ю автора з колишнім високопосадовцем, що займався питаннями безпеки, жовтень 2013 року.

«…Я перебував тоді по інший бік таємничої завіси»: Інтерв'ю автора з колишнім представником адміністрації, який співпрацював з Александером і Білим домом у питаннях кібербезпеки, серпень 2013 року.

«У мене немає повноважень для припинення атак на Волл-стріт…»: З виступу Кіта Александера на симпозіумі AFCEA Defending America Cyberspace 9 лютого 2011 року. Див.: http://www.soteradefense.com/media/events/afcea-defending-america-cyberspace-symposium-2011/. Високопосадовець із правоохоронних органів також розповідав про словесний двобій між Александером і Лют.

14 лютого, за три дні до запланованого виступу: Jane Holl Lute, Bruce McConnell, «A Civil Perspective on Cybersecurity», Threat Level, Wired, 14 лютого 2011 року, http://www.wired.com/threatlevel/2011/02/dhs-op-ed/.

Він виступив із запланованою промовою: Declan McCullagh, «NSA Chief Wants to Protect 'Critical' Private Networks», CNET, 17 лютого 2011 року, http://news.cnet.com/8301-31921_3-20033126-281.html.

«Багато народу говорить, що їм до вподоби технічні можливості АНБ»: З виступу Кіта Александера на конференції AFCEA Homeland Security у Вашинґтоні 22 лютого 2011 року. «CyberCom Commander Calls for Government Protection of Critical Infrastructure», Homeland Security News Wire, 23 лютого 2011 року, http://www.homelandsecuritynewswire.com/cybercom-commander-calls-government-protection-critical-infrastructure. Повний запис виступу Александера можна подивитися за посиланням: http://www.youtube.com/watch?v=Z_lLSP_1Ng0.

З 52 випадків шкідливої активності: Ellen Nakashima, «Cyber Defense Effort Is Mixed, Study Finds», Washington Post, 12 січня 2012 року, http://www.washingtonpost.com/world/national-security/cyber-defense-effort-is-mixed-study-finds/2012/01/11/gIQAAu0YtP_story.html.

«Вони вирішили, що він несповна розуму»: Інтерв'ю автора, серпень 2013 року.

«Десь посередині зустрічі ми запитали»: Інтерв'ю автора зі Стівом Чабінські, липень 2013 року.

«Росіяни попередять хакерів, що ми за ними стежимо»: Інтерв'ю автора з високопосадовцем із правоохоронних органів, жовтень 2013 року.

У 2013 році в АНБ працювало: Кіт Александер розповів про кількість співробітників, коментуючи захід, присвячений кібербезпеці, організований компанією Politico у Вашинґтоні 8 жовтня 2013 року, http://www.politico.com/events/cyber-7-the-seven-key-questions/.

11. Корпоративна контратака

Під час цієї операції, яку Google згодом назве «хитромудрою і цілеспрямованою атакою…: David Drummond, «A New Approach to China», Google blog, 12 січня 2010 року, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

…розробники вважали «коштовним каменем у короні»: John Markoff, «Cyberattack on Google Said to Hit Password System», New York Times, 19 квітня 2010 року, http://www.nytimes.com/2010/04/20/technology/20google.html?_r=0.

«Google зламала цей сервер»: З розмови автора з колишнім керівником розвідслужби, лютий 2013 року.

Компанія Google розкрила подробиці: Для отримання детальнішої інформації про розслідування Google див.: David E. Sanger, John Markoff, «After Google's Stand on China, US Treads Lightly», New York Times, 14 січня 2010 року, http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?_r=0.

Заступник держсекретаря Джеймс Штейнберґ: Інтерв'ю автора з консультантом розвідувального агентства США, який знає про цю розмову (лютий 2010 року). У іншому інтерв'ю в жовтні 2013 року Штейнберґ сказав, що не може пригадати, чи почув ці новини під час вечірки, але підтвердив, що Google звернулася в Держдепартамент за день до публікації і повідомила про свої наміри.

«Це була слушна нагода...»: Авторське інтерв'ю.

«...проект "Угоди про спільне дослідження та розвиток"»: Siobhan Gorman, Jessica E. Vascarellaro, «Google Working with NSA to Investigate Cyber Attack», Wall Street Journal, 4 лютого 2010 року, http://online.wsj.com/news/articles/SB10001424052748704041504575044920905689954?mod=WSJ_latestheadlines. Новину про угоду між АНБ і Google першою оприлюднила газета Washington Post в статті Ellen Nakashima «Google to Enlist NSA to Help It Ward Off Cyberattacks», 4 лютого 2010 року, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html.

Влада може наказати компанії надати цю інформацію: Див.: NSA's Prism overview presentation, http://s3.documentcloud.org/documents/807036/prism-entier.pdf.

Незабаром після викриття китайського втручання: Michael Riley, «US Agencies Said to Swap Data with Thousands of Firms», Bloomberg.com, 15 червня 2013 року, http://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html.

А невдовзі одна компанія зі сфери інформаційної безпеки вирахувала: Kim Zetter, «Google Hackers Targeted Source Code of More Than 30 Companies», Threat Level, Wired, 13 січня 2010 року, http://www.wired.com/threatlevel/2010/01/google-hack-attack/.

«Масштаб цієї діяльності значно більший, ніж хтось будь-коли уявляв»,: Kim Zetter, «Report Details Hacks Targeting Google, Others», Threat Level, Wired, 3 лютого 2010 року, http://www.wired.com/threatlevel/2010/02/apt-hacks/.

«Вони пускають когось на один день і показують безліч розвідданих, пов'язаних із небезпеками»: Авторське інтерв'ю, серпень 2013 року.

«Ми лякаємо їх до бісиків»: Tom Gjelten, «Cyber Briefings 'Scare the Bejeezus' Out of CEOs», NPR, 9 травня 2012 року, http://www.npr.org/2012/05/09/152296621/cyber-briefings-scare-the-bejeezus-out-of-ceos.

Деякі секретні програми дозволяють компаніям ділитись інформацією про власні розробки: Інтерв'ю автора з нинішніми та колишніми співробітниками розвідки, а також експертами у сфері безпеки. Див. також: Riley, «US Agencies Said to Swap Data».

За словами представників компанії й американських можновладців, Microsoft передавала АНБ звіти: Там само. Див. також: Glenn Greenwald et al., «Microsoft Handed the NSA Access to Encrypted Messages», Guardian, 11 липня 2013 року, http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

Компанія Cisco, один із провідних світових виробників мережевого обладнання: Авторське інтерв'ю.

Компанія McAfee, що працює у сфері інтернет-безпеки: Див.: Riley, «US Agencies Said to Swap».

У 2010 році аналітик компанії IBM: Andy Greenberg, «Cisco's Backdoor for Hackers», Forbes, 3 лютого 2010 року, http://www.forbes.com/2010/02/03/hackers-networking-equipment-technology-security-cisco.html?partner=relatedstoriesbox.

Міністерство внутрішньої безпеки також проводить зустрічі з представниками компаній: Зі списком зустрічей і їхньою тематикою можна ознайомитися за посиланням: http://www.dhs.gov/cross-sector-working-groups.

Ще до терористичної атаки 11 вересня представники АНБ виходили на керівників Qwest: Див. судові документи у справі «США проти Nacchio», зокрема «Exhibit 1 to Mr. Nacchio's Reply to SEC. 5 Submission», яке містить покази Джеймса Пейна, колишнього керівника компанії Qwest. Див. також: Shane Harris, «The Watchers: The Rise of America's Surveillance State» (New York: Penguin Press, 2010), с. 16, де описані подробиці співпраці Qwest і АНБ.

Щоб отримати цю інформацію, компанія повинна відповідати державному визначенню критично важливого об'єкта інфраструктури: Див. список критично важливих секторів інфраструктури, складений Міністерством внутрішньої безпеки: http://www.dhs.gov/critical-infrastructure-sectors.

...генерал-майор Джон Дейвіс заявив у своїй промові: Виступ на Міжнародному кібернетичному симпозіумі Військової асоціації зв'язку й електроніки (AFCEA), конференц-зал Балтімора, 25 черв-

ня 2013 року, http://www.dvidshub.net/video/294716/mg-davis-afcea#.UpSILmQ6Ve6#ixzz2lkc87oRy.

12. Весняне пробудження

У березні того самого року: Інтерв'ю автора з нинішніми та колишніми американськими держслужбовцями, зокрема й з представником Міністерства внутрішньої безпеки (травень 2012 року). Наступні інтерв'ю відбулись у жовтні 2013 року. Інформація про атаки на газові компанії вперше з'явилася в статті: Mark Clayton, «Alert: Major Cyber Attack Aimed at Natural Gas Pipeline Companies», Christian Science Monitor, 5 травня 2012 року, http://www.csmonitor.com/USA/2012/0505/Alert-Major-cyber-attack-aimed-at-natural-gas-pipeline-companies.

Проте подейкують, що під час холодної війни: Див.: Thomas Reed, «At the Abyss: An Insider's History of the Cold War» (New York: Presidio Press, 2004).

Попередження від компаній щодо виявлення шпигунів «нескінченні»: Інтерв'ю автора, жовтень 2013 року.

Вони поділилися з персоналом, що опікується корпоративною безпекою, «стратегіями зменшення заподіяної шкоди»: Інтерв'ю автора зі співробітником Міністерства внутрішньої безпеки, травень 2012 року.

Того літа Міністерство внутрішньої безпеки: «Information Sharing Environment 2013 Annual Report to the Congress», http://www.ise.gov/annual-report/section1.html#section-4.

Міністерство внутрішньої безпеки, ФБР, Міністерство енергетики та Агентство безпеки транспорту почали так звану активну кампанію: «Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team, Monthly Monitor (ICS – MM201310), July – September 2013», 31 жовтня 2013 року, http://ics-cert.us-cert.gov/sites/default/files/Monitors/NCCIC_ICS-CERT_Monitor_Jul-Sep2013.pdf.

Shell, Schlumberger та інші великі компанії: Zain Shauk, «Phishing Still Hooks Energy Workers», FuelFix, 22 грудня 2013 року, http://fuelfix.com/blog/2013/12/22/phishing-still-hooks-energy-workers/.

У травні 2013 року, під час одного з небагатьох своїх публічних виступів: Берлін виступав на конференції з питань кібербезпеки в Музеї журналістики і новин Newsuem у Вашинґтоні 22 травня 2013 року.

За кілька місяців після виявлення втручання в мережі газових підприємств: Brian Krebs, "Chinese Hackers Blamed for Intrusion at Energy industry Giant Telvent," *KrebsonSecurity*, September 26, 2012, http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/.

Країна відчуває нагальну потребу: World Bank, «GDP Growth», http://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG.

Китай – це друга країна світу за обсягами споживання вугілля: US Energy Information Administration, http://www.eia.gov/countries/country-data.cfm?fips=CH.

Принаймні одна американська енергетична компанія: Michael Riley, Dune Lawrence, «Hackers Linked to China's Army Seen from E. U. to D. C.», Bloomberg.com, 26 липня 2012 року, http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html.

Тому Китай шукає законні стежки до отримання інформації про пошуки джерел енергії: Ryan Dezember, James T. Areddy, «China Foothold in US Energy», Wall Street Journal, 6 березня 2012 року, http://online.wsj.com/news/articles/SB10001424052970204883304577223083067806776.

За однією оцінкою, потік даних у декілька разів перевищував трафік, який 2007 року російські хакери скерували на естонські комп'ютери: Nicole Perlroth, Quentin Hardy, «Bank Hacking Was the Work of Iranians, Officials Say», New York Times, 8 січня 2013 року, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?pagewanted=all&_r=3&.

Банківські інтернет-провайдери доповіли: Авторське інтерв'ю з Марком Везерфордом, серпень 2013 року.

«Протягом перших двох-трьох тижнів доводилося працювати до пізньої ночі»: Там само.

Згідно зі звітами розвідки, влада Ірану з 2011 року витратила понад мільярд доларів: Yaakov Katz, «Iran Embarks on $1b. Cyber-Warfare Program», Jerusalem Post, 18 грудня 2011 року, http://www.jpost.com/Defense/Iran-embarks-on-1b-cyber-warfare-program.

Група високопоставлених фінансистів тиснула на представників АНБ: Інтерв'ю автора з керівником фінансової компанії, який був присутній на зустрічі, листопад 2013 року.

13. Оборонний бізнес

Гатчінзу спало на гадку: Інтерв'ю автора з Еріком Гатчінзом, січень 2014 року.

За допомогою цієї моделі Lockheed могла завчасно попереджати своїх клієнтів: Інтерв'ю з Чарлі Крумом, січень 2014 року.

«Упродовж кількох найближчих років усі хлопці з кіберпідрозділів, що залишилися в грі, працюватимуть у банках»: Інтерв'ю автора з колишнім офіцером військової розвідки, липень 2013 року.

Один експерт у сфері безпеки, який має тісні зв'язки з продавцями експлойтів: Інтерв'ю автора з експертом у питаннях кібербезпеки, грудень 2013 року.

«У нас уже є кібернетичний еквівалент агентства Пінкертона»: Інтерв'ю автора з Марком Везерфордом, серпень 2013 року.

18 лютого 2013 року фірма Mandiant: «Mandiant, APT1: Exposing One of China's Cyber Espionage Units», http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Не минуло й місяця, як радник з питань державної безпеки США Том Донілон: Повний виступ Донілона перед Азійським співтовариством 11 березня 2013 року можна переглянути за посиланням: http://asiasociety.org/video/policy/national-security-advisor-thomas-donilon-complete.

«Ми вирішили, що це цікава ідея»: Інтерв'ю автора з Деном МакВортером, лютий 2013 року.

Аналітики Mandiant виявили: Nicole Perlroth, «Hackers in China Attacked the Times for Last 4 Months», New York Times, 30 січня 2013 року, http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0.

…понад третина компаній зі списку Fortune 100 користувалася послугами Mandiant: Hannah Kuchler and Richard Waters, "Cyber Security Deal Highlights Threats from Spying," *Financial Times,* January 3, 2014, http://www.ft.com/intl/cms/s/0/e69ebfdc-73do-11e3-beeb-00144feabdco.html?siteedition=intl#axzz2pM7S3G9e.

«Лише погляньте на суперспроможність цих компаній…»: Там само.

…він [Сноуден] навчався на поглиблених курсах «етичного хакерства»: Інтерв'ю автора з представниками школи та приватними особами, які знали про поїздку Сноудена, січень 2014 року.

Комісія склала 300-сторінковий звіт: President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

У вересні 2013 року старший офіцер ВПС США розповів: John Reed, "The Air Force Still Has No Idea How Vulnerable It Is to Cyber Attack," *Foreign Policy,* 20 вересня 2013 року, http://killerapps.foreignpolicy.com/posts/2013/09/20/the_air_force_still_has_no_idea_how_vulnerable_it_is_to_cyber_attack.

…минуло вже понад чотири роки: Siobhan Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *Wall*

Street Journal, 21 квітня 2009 року, http://online.wsj.com/article/SB124027491029837401.html.

Генеральний інспектор Міністерства оборони вже за місяць після отримання доступу до систем ВПС звітував: Aliya Sternstein, "IG: Government Has No Digital Cyber Warning System," Nextgov, 5 листопада 2013 року, http://www.nextgov.com/cybersecurity/2013/11/ig-government-has-no-digital-cyber-warning-system/73199/.

Трохи раніше цього ж року двоє інженерів виявили низку вразливостей: Nicole Perlroth, "Electrical Grid Is Called Vulnerable to Power Shutdown," Bits, New York Times, 18 жовтня 2013 року, http://bits.blogs.nytimes.com/2013/10/18/electrical-grid-called-vulnerable-to-power-shutdown/.

«У цій країні немає жодної важливої комп'ютерної системи, в яку цієї самої миті не намагаються проникнути»: Виступ МакКоннела на конференції з питань кібербезпеки, організованій корпорацією Bloomberg у Вашинґтоні 13 жовтня 2013 року.

Слідчі виснували, що хакери, найімовірніше, походили зі Східної Європи або Росії: Brian Krebs, "Target Hackers Broke in Via HVAC Company," *KrebsonSecurity*, 5 лютого 2014 року, http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

У лютому 2014 року комітет сенату повідомив: Craig Timberg and Lisa Rein, "Senate Cybersecurity Report Finds Agencies Often Fail to Take Basic Preventative Measures," Washington Post, 4 лютого 2013 року, http://www.washingtonpost.com/business/technology/senate-cybersecurity-report-finds-agencies-often-fail-to-take-basic-preventive-measures/2014/02/03/493390c2-8ab6-11e3-833c-33098f9e5267_story.html.

У жовтні 2013 року на конференції з питань кібербезпеки у Вашинґтоні: Виступ Александера в Newsuem у Вашинґтоні 8 жовтня 2013 року, http://www.youtube.com/watch?v=7huYYic_Yis.

14. На зорі

Одна високопоставлена офіційна особа розповідала: Інтерв'ю автора з представником адміністрації, січень 2014 року.

Обама вибрав вдалий час для виступу: Olivier Knox, "Obama NSA Speech on Anniversary of Eisenhower Warning," Yahoo News, 16 січня 2014 року, http://news.yahoo.com/obama-nsa-speech-on-anniversary-of-eisenhower-warning-025532326.html. Радник Білого дому сказав Ноксу, що президент обрав вдалий час для виступу.

У грудні 2013 року міністр енергетики Ернест Моніз заявив: "Moniz Cyber Warning," *EnergyBiz*, 5 січня 2014 року, http://www.energybiz.com/article/14/01/moniz-cyber-warning.

Владі чудово відомо про ці атаки: Генерал Кіт Александер назвав кількість атак під час виступу в Джорджтаунському університеті 4 березня 2014 року.

«Урешті-решт, саме ринок визначає, як треба чинити компаніям…»: Прес-реліз, оприлюднений адміністрацією президента, 12 лютого 2014 року.

Якщо провайдерам гарантуватимуть захист від відповідальності: Для ретельного вивчення того, як залучити постачальників інтернет-послуг до посилення захисту кіберпростору, див.: Noah Shachtman, "Pirates of the ISPs: Tactics for Turning Online Crooks into International Pariahs," Brookings Institution, липень 2011 року, http://www.brookings.edu/~/media/research/files/papers/2011/7/25%20cybersecurity%20shachtman/0725_cybersecurity_shachtman.pdf.

Деякі спостерігачі порівнюють сучасних кіберзлочинців: Там само. Див. також: Jordan Chandler Hirsch and Sam Adelsberg, "An Elizabethan Cyberwar," *New York Times*, 31 травня 2013 року, http://www.nytimes.com/2013/06/01/opinion/an-elizabethan-cyberwar.html.

На відміну від інших «хмар»: Brandon Butler, "Amazon Hints at Details on Its CIA Franken-cloud," Network World, 14 листопада 2013 року, http://www.networkworld.com/news/2013/111413-amazon-franken-cloud-275960.html.

ПРО АВТОРА

Шейн Гарріс – американський журналіст і автор книжок. Провідний кореспондент видання Daily Beast, яке спеціалізується на питаннях державної безпеки та кіберзахисту. Він також член фонду «Нова Америка», для якого досліджує війни майбутнього. Його статті друкували видання New York Times, Wall Street Journal, Foreign Policy та багато інших. Перша книжка автора «Спостерігачі: розвиток державної американської розвідки» (The Watchers: The Rise of America's Surveillance State) увійшла до переліку найкращих книжок 2010 року, за версією видання Economist, та здобула багато престижних нагород.

ПРЕДМЕТНО-ІМЕННИЙ ПОКАЖЧИК

НАУКОВО-ПОПУЛЯРНЕ ВИДАННЯ

Гарріс Шейн

ВІЙН@
битви в кіберпросторі

Переклад *О. Замойської*

Редактор *О. Попова*
Коректор *М. Бродська*
Обкладинка *Д. Шевчука*
Оригінал-макет *О. Гашенко*

Підписано до друку 31.10.2019. Формат 60x84/16. Папір офсетний.
Друк офсетний. Умовн. друк. арк. 17,21. Зам. № 286.

Видавці:

Видавництво «Ніка-Центр»
03142, Київ, вул. Кржижановського, 4.
т./ф. (044) 39-011-39; e-mail:psyhea9@gmail.com; www.nika-centre.kiev.ua
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів
видавничої продукції ДК №5368 від 27.06.2017

ТОВ «Видавництво Анетти Антоненко»
www.anetta-publishers.com
Для листування: anetta@anetta-publishers.com
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів
видавничої продукції ДК №4873 від 26.03.2015

Віддруковано у ТОВ «ДІА». 03022, Київ, вул. Васильківська, 45.
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів
видавничої продукції ДК №1149 від 12.12.2002