ЗМІСТ

ВІЙН@. Битви в кіберпросторі

Про книгу

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!


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

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.

Кінець безкоштовного уривку.
Щоби читати далі, придбайте,
будь ласка, повну версію
книги.