

Шейн Гарріс

ВІЙН@
битви в кіберпросторі

Переклад з англійської
Олени Замойської

Київ
Ніка-Центр
Львів
Видавництво Анетти Антоненко
2019

ЗМІСТ

<i>Війни нового покоління (С.П.Попович)</i>	7
Зауваги щодо джерел	11
Вступ	13

ЧАСТИНА I

1 Перша кібернетична війна	29
2 RTRG.....	51
3 Створення кіберармії	65
4 Поле битви – інтернет	95
5 Ворог серед нас.....	109
6 Найманці	130
7 Поліцейські стають шпигунами	151

ЧАСТИНА II

8 Ще один «мангеттенський проект».....	167
9 «Американська картеч»	174
10 «Секретний складник».....	181
11 Корпоративна контратака.....	199
12 Весняне пробудження.....	215
13 Оборонний бізнес	225
14 На зорі	243
Подяки	256
Джерела та примітки.....	260
Про автора.....	286
Предметно-іменний покажчик.....	287

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'єданого 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 брифінгах, що Павелл доручив йому проводити щоденні брифінги 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 Пентагону.

Під керівництвом МакКоннелла розвиток кіберзброї трохи пригальмував. 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 Вашингтона, 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 Гейтс, колишній директор ЦРУ і давній товариш МакКоннелла, який нині обіймав посаду міністра оборони.

МакКоннелл відповів Чейні, що йому потрібно поміркувати і він відповідь після Різдва. Він поклав слухавку, а потім зателефонував Гейтсу, 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 Гейтс 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, інсталиючи 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 Чикаго, 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 Обама 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 нищпорити 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 Обама 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 минуше 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 uszkodження переконали Пентагон 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 Гейтсом, який погодився залишитися на посту міністра оборони після приходу нової адміністрації. Гейтс підтримав ідею щодо необхідності кіберкомандування. Проте цього не сталося, поки МакКоннелл залишався на посаді директора АНБ. Офіційний Вашингтон був зайнятий передачею президентської влади: представники адміністрації Буша «передавали ключі» новій команді та детально пояснювали все, над чим працювали. Але Гейтс 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 Пентагоні. 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 Гейтс 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-Вегаса 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, чиім 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 Вашингтон 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 згуртуватися 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, охолонуту 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 спантелених 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 кіберудару першою, і звачити на можливі масштаби руйнувань для обох сторін.

Натомість гра лише зміцнила природну схильність військових до війни. І переконала вищих офіцерів і керівників Пентагону: 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 розважають спроби зламування наших електричних мереж, а в інших країнах кібератаки занурюють у пільму 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 Мічиган, 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, посиляючись 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 Вашингтоні.

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 кіберввторгнення 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 розголошення 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 поїзди, 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 Обама давала військовим «зелене світло» на підготовку до кібервійни.

Постанова Обама 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 оперативного-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 Пентагоні.

Отже, сили кібероборони створили «мисливські загони», які спільно з кібершпигунами з АНБ і Розвідувального управління працюють над пошуком потенційних погроз для військових мереж. У рамках цієї співпраці військові мають доступ до бази даних, що містить досьє на кожного відомого хакера в Китаї, – розповів один посадовець із Пентагону, 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, ймовірно, 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 оперативного 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 радары, 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, вторгтися 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.

Пентагон «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 Вашингтоном 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 військовій 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 захисникові 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 клапти 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 безпроводний 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 – АРТ). Саме вона, на думку американської влади, відповідальна за глобальне поширення шкідливого програмного забезпечення, яке заразило або намагалося заразити кожен 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 АРТ, 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-