РОЗДІЛ І

# ПЕРВОРОДНІ ГРІХИ

Це нагадує серпень 1945-го. Хтось застосував нову зброю, і назад її вже не заховають.

*Генерал Майкл Гейден,*
*колишній директор Агентства національної безпеки*
*та Центрального розвідувального управління*

На початку весни 2012 року я подався до Центрального розвідувального управління; проїхавши по дорозі, що звивалася поміж дерев, я зупинився перед будівлею, якій управління дало химерну назву «Старий штаб»[34].

Я знав, що моя запланована зустріч із заступником директора Майклом Мореллом має бути нелегка. Кілька тижнів тому Білий дім попросив мене зустрітися з Мореллом і обговорити вельми делікатну статтю, яку готувався опублікувати часопис «Таймз». Ми з ним тоді мали коротку зустріч у Західному крилі — в підвальному офісі Бенджаміна Дж. Родса, на той час заступника радника з національної безпеки в царині стратегічних комунікацій, — і я розповів там те, що довідався сам: як обидва президенти з геть різними темпераментами, Джордж В. Буш і Барак Обама, вирішили кожен у свій час використати наймодернішу кіберзброю проти Ірану, вважаючи таке рішення останнім шансом запобігти новій війні на Близькому Сході.





Ані Родс, ані Морелл, схоже, не здивувалися, що я склав докупи ці історії; код тієї кіберзброї, так званий Stuxnet[35], випадково поширився світом ще два роки тому. Тож було очевидно, що хтось використовував шкідливі програми, намагаючись знешкодити іранські ядерні установки. Stuxnet містив виразні цифрові «відбитки пальців» та інші знаки того, де й коли його створили. Хтось колись повинен був вирушити по слідах і виявити задум, з якого виросло написання цього коду. Операція, як я дізнався через декілька місяців журналістського розслідування, мала кодову назву «Олімпійські ігри»[36]. Вона була надто масштабною, а кількість її учасників — надто великою, щоб назавжди залишитися таємницею. Навіть іранці уже давно заявили, що за атакою стояли США та Ізраїль, хоча їм усе ж бракувало доказів. Проте жоден з двох урядів цього не визнав, немов засвідчуючи, що всі кібероперації оповиті щільною завісою секретності.

Лише президент може дозволити використати ядерну або кіберзброю з руйнівною метою. Проте ще жодного американського президента не вдалося доказово звинуватити, що він такий дозвіл надав, оскільки майже всі наступальні кібероперації таємні й неодмінно плануються так, щоб усе можна було спростувати. У статті «Таймз» йшлося про нараду в Ситуаційній кімнаті, на якій обговорювали застосування кіберзброї для такого удару, який раніше можна було здійснити лише завдяки бомбардувальникам чи диверсантам.

Я прямував по знаменитому атріумі будівлі ЦРУ, стіни якого прикрашали бронзові зірки — кожна на честь певного офіцера управління, який загинув, захищаючи країну; і коли здіймався ліфтом до офісу

Морелла, то й не здогадувався, як легко моя розповідь може зруйнувати ті стіни секретності, які США десятиліттями вибудовували довкола своїх заходів зі створення кіберзброї. Так само я не міг передбачити, що започаткую одне з найбільших федеральних розслідувань сучасності, яке стосуватиметься витоку інформації, і не здогадувався, що через це несправедливо переслідуватимуть офіцера, якого високо цінував Б. Обама і який належав до тих, хто вводив Збройні сили США в сучасну еру кібервоєн.

Виявилося, що уряд США ще не готовий обговорювати наслідки свого рішення застосувати кіберзброю проти інших країн у мирний час. Також він не хотів визначати, наскільки такі дії спровокували подальші перегони кіберозброєнь, до яких долучилися Іран, Росія, Північна Корея та Китай.

Поза тим вестибюлем, який часто можна бачити на світлинах, обтоптані робочі кабінети ЦРУ нагадували офіси підупалих комп'ютерних фірм, як-от Burroughs і Digital Equipment Corporation, яких уже нема і про які мені доводилося писати кілька десятиліть тому ще в статусі молодого кореспондента, що спеціалізується в царині технологій. Особливо виразним ретростиль був на сьомому поверсі, в кімнаті, яку Аллен Даллес, директор ЦРУ за часів президентства Ейзенгауера та Кеннеді, облаштував так, щоб керувати хитромудрими спробами викрасти таємниці й здолати ворогів у Холодній війні, сидячи ледь не впритул до свого заступника. Тож своїм виглядом найвідоміше у світі шпигунське агентство справляло загалом дещо оманливе враження. Як засвідчила історія з «Олімпійськими іграми», воно вже давно увійшло у цифрову епоху, проте було геть незацікавлене надмірно демонструвати власні здобутки.





Я прибув у Старий штаб, аби дізнатися, які саме деталі готової от-от з'явитися на світ статті настільки стурбували Морелла та його колег, що вони ладні були просити «Таймз» відкликати публікацію. Мабуть, вона могла б ненароком викрити ті секретні операції, що саме розгорталися. Такі розмови складні вже за своєю суттю. Інформаційні агенції повинні дослухатися до урядових застережень, але й наполягати, що на підставі Першої поправки до Конституції рішення публікувати чи ні явно за ними, а не за урядом. Завжди люб'язний і пильний Морелл уже зазначив, що, на його думку, жодну частину статті про «Олімпійські ігри» оприлюднювати не варто. Проте він був реалістом і знав, що випадкове розповсюдження і викриття мережевого хробака Stuxnet означає, що проблема нікуди не зникне. Тож для ЦРУ наша зустріч була нагодою з'ясувати, що саме було мені вже відомо, і спробувати мінімізувати збитки.

Операцію «Олімпійські ігри» здійснювали переважно АНБ та ізраїльський Підрозділ 8200[37], що спеціалізується на воєнних кіберопераціях цієї країни. Проте, як я згодом довідався, ЦРУ відіграло ключову роль, скориставшись дозволом президента, який у Вашингтоні називали «розпорядженням», провести таємну операцію з метою загальмувати розгортання іранської ядерної програми. Оскільки «розпорядження» таємні, а їхнє існування заперечуватиметься, я не сподівався, що службовці, з якими того дня я мав зустрітися, визнають свою причетність до застосування

кіберзброї, не кажучи вже про подальше виведення з ладу близько тисячі центрифуг, котрі оберталися в надрах іранської пустелі. І вони таки не визнали.

Але щось у цій історії було не так, і напруга через майбутню публікацію лише зростала. Кіберзброя була одним з перших різновидів стратегічної зброї, яку створили розвідувальні служби, а не військові, тож її оповило значно більше таємниць, аніж ядерну й біологічну зброю або нові покоління винищувачів «Стелс» і безпілотників. В уряді вважали, що будь-які публікації про кіберзброю перешкоджатимуть ефективно її застосовувати в майбутньому. Уряд щиро обурювався кібератаками проти Сполучених Штатів і навіть надавав докази проникнення інших держав в американські банківські та електричні мережі, однак обговорювати власні можливості, наміри та доктрини навіть на базовому рівні вважав за неприпустиме. Такий рівень секретності вважали смішним навіть деякі урядовці. Хіба ж можна дискутувати про міжнародні правила застосування зброї, якщо не визнавати володіння нею, а тим паче її використання?

Ясно, що в адміністрації Обами не було консенсусу щодо того, як застосовувати кіберзброю. Навіть даючи дозвіл на нові удари по іранських ядерних установках, Обама сумнівався. Як ішлося в нашому репортажі[38], на засіданнях у Ситуаційній кімнаті в перший рік президентства Обама не раз перепитував, чи ж не створюють США, використовуючи кіберзброю для виведення з ладу ядерної установки, такого прецеденту, про який одного дня самі ж і пожалкують. Він та ще дехто побоювалися, що колись таку високоточну зброю інші країни спрямують проти нас. «Питання





його було слушне, — погоджувався один з високопосадовців, який прийшов в уряд уже після атаки Stuxnet. — Проте ніхто не сподівався, що цей день настане так швидко».

Цікаво, що Обама вже показав готовність публічно обговорити ці питання. Ішлося про безпілотники. Коли Обама прибув до Білого дому, вся інформація про ведення бойових дій за допомогою безпілотників вважалася цілком таємною. Та з часом він оприлюднив деякі деталі програми, був готовий пояснити правові підстави й мотиви рішення застосувати дистанційно керовані машини для вбивства. Так він поступово підняв завісу таємниць, і світова спільнота могла переконатися, чи з безпілотників справді переслідували терористів, а чи то щось ішло не так, коли з них убивали дітей або гостей на весіллі.

З кіберзброєю все було інакше. Уряд не хотів визнавати навіть володіння нею, а тим паче обговорювати правила, коли і як її застосовувати. Але проблема була така сама. Журналістські розслідування про помилкові атаки безпілотників і їхні жертви спричинили дискусію про безпілотну зброю. Отож і ми з редакторами вважали своїм журналістським обов'язком пояснити читачам, як уряд застосовує кіберзброю, яка, зрештою, може бути використана проти нашої батьківщини. Операція «Олімпійські ігри» відхилила двері в новий вимір війни, який ще ніхто до пуття не розумів.

Безперечно було лише те, що вороття вже немає. Майкл Гейден, ключова фігура перших американських експериментів з кіберзброєю, сказав, що застосування Stuxnet «нагадує серпень 1945-го», тобто натякнув на бомбардування Хіросіми та Нагасакі, чим недвознач-

но заявив, що настав світанок нової ери. Оскільки Гейден мав доступ до державної таємниці, він не міг визнати причетність США до Stuxnet, однак не залишив жодних сумнівів, що подія це масштабна й значуща.

«Я в цьому переконаний, — підсумував Гейден. — Щойно ми зробимо якийсь крок, як увесь світ сприйме його як новий стандарт, як щось таке, на що й вони мають право».

Саме так і сталося[39].

Гейден добре навчився говорити про Stuxnet так, наче він сторонній спостерігач, такий собі зоолог, який щойно спостеріг незвичну поведінку тварини й оголосив про відкриття нового виду. Насправді ж він, певно-таки, добре знав, з чим має справу. На момент початку «Олімпійських ігор» Гейден очолював ЦРУ. Він уже давно був у перших лавах тих, що ще в середині 1990-х зрозуміли: кіберзброя — це не лише нове знаряддя. Згідно з військовою термінологією, це був новий вимір, у якому розгортатимуться майбутні великі й малі міждержавні конфлікти.

У 1970-х, коли Гейден здіймався по кар'єрних щаблях у Військово-повітряних силах, всі погоджувалися з тим, що війни обмежені чотирма фізичними вимірами: люди тисячоліттями воювали на землі та в морі, а після Першої світової війни — ще й у повітрі. У 1950-х і 1960-х додався космос — услід за супутниками з'явилася протисупутникова зброя, а за міжконтинентальними балістичними ракетами — антибалістичні ракетні системи. А як щодо кіберпростору? Якось в Академії Військово-повітряних сил у Колорадо-Спрінґз генерал, який давно вийшов у відставку, зі щирим здивуванням





запитав мене: «Хіба можна воювати у місці, якого не бачиш?».

Гейденове розуміння революційної природи кіберконфлікту почало формуватися ще понад двадцять років тому, коли його відрядили в Сан-Антоніо, що у штаті Техас, очолити управління розвідки Військово-повітряних сил (ВПС). У цьому підрозділі він і познайомився з потугою нового покоління радіоелектронної зброї. Він пригадував, як зачаровано спостерігав за колегами, які виводили з ладу віддалені робочі станції й застосовували методи радіоелектронної боротьби, щоб ошукати радар, який намагався відстежити винищувач. Гейдена, який саме повернувся з охоплених війнами Балкан, найбільше вразив факт, що американська воєнна машина зазнає безнастанних атак у мирний час.

1998 року, через рік після того, як Гейден потрапив у Техас, ФБР взялося розслідувати дивні з першого погляду вторгнення[40], що траплялися в різних місцях, пов'язаних з воєнними та розвідувальними мережами: від Лос-Аламоса[41] і Національних лабораторій «Сандія»[42], де розробляють ядерну зброю, до університетів, як-от Гірничої школи Колорадо[43], яка підтримує тісний зв'язок з Військово-морськими силами (ВМС)[44]. Найбільше втручань виявили в мережах авіабази Райт-Патерсон в Огайо, розташованої на місці, де брати Райти колись випробовували свої перші літаки.

Першим втручання зауважив один з комп'ютерних операторів Гірничої школи, побачивши нічну нічим непоясниму активність комп'ютерів. Виявилося, що це була дуже масштабна й тривала атака, ведена, ймовірно, з Росії. Упродовж двох років хакери користувалися