НІКОЛЬ ПЕРЛРОС

ОСЬ ТАКИМ, ЯК МЕНІ КАЖУТЬ, БУДЕ КІНЕЦЬ СВІТУ: ПЕРЕГОНИ КІБЕРОЗБРОЄНЬ

ХАРКІВ
«ФОЛІО»
2022

ПЕРЕДМОВА ДО УКРАЇНСЬКОГО ВИДАННЯ

Книжка, яку ви тримаєте у руках, — це результат багаторічної кропіткої роботи авторки в бажанні розкрити правду щодо діяльності спецслужб найрозвиненіших і найактивніших у сфері кібероперацій держав, топових хакерів та хакерських угруповань. Зокрема, це й співпраця між ними в пошуку, виявленні, купівлі та продажу так званих уразливостей нульового дня та експлойтів, тобто інструментів і засобів використання цих уразливостей у кібератаках й інших кіберопераціях. Діяльності неоднозначної, яка часто народжує ще більше запитань, ніж дає відповідей.

Українською мовою цей бестселер New York Times мав вийти з друку до Книжкового Арсеналу 2022, першого після двох років пандемії, який традиційно очікувався в травні. Ще в січні на прохання видавництва я обговорював із Ніколь Перлрос деталі її візиту до Києва, участі в презентації книги й інших публічних заходах, спрямованих на просування найкращого розуміння викликів глобальної кібервійни, яка, як і гібридна війна та збройна агресія російської федерації проти України, почалася задовго до 24 лютого 2022-го і навіть задовго до 20 лютого 2014 року…

Сьогодні немає завдання, важливішого за перемогу України в усіх трьох традиційних просторах війни. Проте разом із перемогою над ворогом на землі, на морі й у повітрі, звільненням українських міст і сіл від окупанта, поверненням на всій нашій землі мирного життя й розвитку навряд чи колись в найближчому майбутньому настане мир у ще одному просторі — просторі комп'ютерних мереж, систем і даних або, як тепер його заведено спрощено називати, у кіберпросторі.

Україна сьогодні не лише успішно захищається від кібератак, а й атакує ворога у відповідь. І хоча це — новий вид війни не лише для України, а й для всього світу, ми вже маємо з чим порівнювати і свої успіхи, і свої невдачі.

За даними Microsoft, у 2020–2021 роках майже 20% цільових кібератак було спрямовано проти нашої країни, проти США — більше як 45%, Великої Британії — майже 10%, а, наприклад, проти таких країн, як Ізраїль — усього 2%. У досить далекому за мірками темпів цифрової трансформації 2017 році відбулася вже хрестоматійна атака NotPetya, яка почалася з України й мала Україну як головну ціль, але завдала також мільярдних збитків компаніям і урядам по всьому світі. Після цієї та низки інших атак (наприклад, ще одна хрестоматійна кібератака Triton на нафтопереробний завод на Близькому Сході, коли хакери втрутилися в роботу систем функціональної безпеки виробництва, низка кібератак на українські енергетичні компанії, внаслідок яких без світла опинилися тисячі містян, багатьох інших відомих і не дуже атак) світ із жахом усвідомив: крадіжка цінних даних чи блокування роботи інформаційних ресурсів — далеко не найгірше, до чого може призвести витончена кібероперація. І будь-яка країна, уряд, галузь, компанія, організація чи просто людина незалежно від розміру доходів, сфери роботи, місця розташування, географії діяльності, політичного позиціювання чи його відсутності є уразливою.

Тому зовсім не дивно, що таку престижну нагороду, як бізнес-книга року від Financial Times та McKinsey (Business Book of the Year Award), у 2021 році отримала саме Ніколь Перлрос і саме за цю книгу. Адже, незважаючи на постійне зростання загрози, кібербезпека й досі часто лишається поза належною увагою керівників компаній і членів рад директорів.

Очевидно, що успіх цієї книги базується не тільки на актуальності теми. Ніколь Перлрос є однією з найдосвідченіших експерток із питань кібербезпеки та цифрового шпигунства в американській медіаспільноті. За більш ніж 15 років роботи в провідних американських бізнес-виданнях (спочатку п'ять років у Forbes, а потім понад десять — у New York Times) Ніколь по праву здобула славу непересічної розслідувачки й аналітикині.

Вона публікувала розлогі аналітичні матеріали щодо ключових кіберзлочинів останнього десятиріччя — атак російських хакерів на атомні станції, аеропорти й нафтохімічні заводи; розслідувала резонансну кібератаку представників КНДР на Sony Pictures, аналізувала кіберзлочини Ірану до низки американських нафтових компаній і банків, а також об'єктів критичної інфраструктури США. Саме Ніколь Перлрос ініціювала масштабне дослідження діяльності китайських хакерів проти американських медіа, зокрема кібератака на New York Times. Її відзначено низкою престижних журналістських премій, зокрема, її було номіновано як найкращу репортерку у сфері технологій. Вона також отримала відзнаку Best in Business Award американської спілки бізнес-редакторів і письменників (Society of Business Editors and Writers) за матеріал про роботу кіберпідрозділів армії Китаю.

Разом із тим є кілька застережень, які сама авторка робить щодо цієї, безперечно, вчасної й важливої книги. Вона розрахована насамперед на широке коло читачів й однозначно буде цікавою читачам, які хочуть розібратися в карколомному розвитку кіберзброї за останні 30 років — від побутового та промислового шпигунства до масштабних кібероперацій. Ця книга буде корисною і всім тим, хто просто хоче краще розуміти сучасний світ. Щось нове й цікаве в ній для себе знайдуть і фахівці з кібербезпеки, але її мета — не відкриття чогось раніше невідомого з технічного погляду. Це радше спроба допомогти бізнес-лідерам, державним діячам і політикам «розплющити очі» й побачити проблему:

«Кажуть, що перший крок до усунення проблеми — це її визнання. Ця книга — моя спроба зробити це, — пише Ніколь і веде далі: — Це історія нашої величезної цифрової уразливості, того, як і чому вона існує. Це історія про уряди, які її експлуатували й, власне, зробили можливою. І це також історія про підвищення ставок для всіх нас. І хоча для когось ця інформація вже не є новою, я все ж підозрюю, що таких людей небагато. А ще менше тих, хто по-справжньому розуміє суть питання. Але саме наше невігластво у подібних питаннях стало нашою найбільшою уразливістю».

Через таке позиціювання книги деякі думки та висновки авторки професіоналам можуть здатися занадто спрощеними й узагальненими. Але від цього мета книги не стає менш шляхетною. Врешті, кому як не українським фахівцям із кібербезпеки (насамперед тим, які вже понад вісім років перебувають на передовій глобальної кібервійни й щодня протистоять постійному зростанню кіберзагроз, відбиваючи регулярні хвилі потужних кібератак, розслідуючи інциденти, шукаючи та усуваючи уразливості, відновлюючи пошкоджені чи уражені системи, підвищуючи кіберстійкість в умовах вкрай обмежених ресурсів і загалом ще досить нерозвиненої загальної культури кібербезпеки) не вітати вихід цієї книги українською та її важливу місію спонукати «до активізації усвідомлення, необхідного для розв'язання, цілком можливо, найскладнішого завдання нашої цифрової ери», яким є кібербезпека.

Тому завершити цю передмову мені б також хотілося привертанням уваги українських бізнесменів, чиновників і політиків до деяких глобальних та специфічних для нашої країни кібербезпекових викликів, які разом із загрозами створюють і можливості.

Крім безпосередньої кібервійни, сторонами якої є диктаторські країни (росія, Північна Корея, Іран й інші) — з одного боку і країни демократії, свобод і прав людини — з іншого, рівень кіберзагроз загалом у світі зріс до небачених раніше масштабів. Згідно з дослідженням Global Cybersecurity Outlook Всесвітнього економічного форуму, кількість кібератак за 2021 рік збільшилась на 125%. Динаміка 2022 року свідчить, що активність кіберзловмисників наростає.

Кібератаки з кожним днем стають усе складнішими й витонченішими. З метою отримання викупу чи цінних даних кіберзлочинці все частіше послуговуються кіберарсеналом, який раніше застосовували тільки хакера, що працюють в інтересах держав.

Усе частіше спостерігається підривання довіри між клієнтами та постачальниками послуг унаслідок усе поширеніших атак на ланцюги постачань. Якщо в компаній падає довіра до розробників програмного забезпечення, то це ставить під загрозу подальшу диджиталізацію бізнесу та можливість клієнтів отримувати корисні продукти та зручні сервіси.

Зростає кадровий голод. Рівень загроз збільшується так швидко, що у світі просто немає достатньої кількості талантів і спроможностей для ефективної протидії. Безпрецедентні виклики вимагають координації зусиль бізнесу, держави та суспільства як на національному й регіональному, так і на міжнародному рівнях.

Через загальну увагу світу до поточних подій в Україні весь світ побачив: критична інфраструктура України успішно протидіє кібератакам, незважаючи на обмежені ресурси й величезну кількість атак, яка і до початку повномасштабного вторгнення була високою.

Але критична інфраструктура — це не тільки те, що вказано в офіційних документах. Це не тільки про енергетику, телекомунікації, банки, безпекові та правоохоронні структури та сектор державного керування. В умовах війни практично кожна галузь стає критичною. Окрім руйнування нормальних процесів у країні йдеться також про підігрівання ефекту паніки, що і є кінцевою метою ворога — зробити державні, громадські, підприємницькі та цивільні процеси некерованими.

Україна захищається в кіберпросторі насамперед завдяки кваліфікованим професіоналам, які здатні протидіяти найсерйознішим кіберзагрозам. Однак цього недостатньо на майбутнє.

Кібербезпека — це не тільки функція, це також індустрія, яка має великий експортний потенціал, для реалізації якого потрібні дві речі. По-перше, розвиток внутрішнього ринку, і зокрема його публічного сектору. А по-друге, просування іміджу України як передової країни у сфері кібербезпеки. Ми маємо компанії з кібербезпеки світового рівня й повинні зробити все, щоб світ дізнався про це більше.

Кібербезпека — це безперервний процес упровадження та здійснення багатьох ефективних захисних рішень, кожен елемент якої є важливим, а всі складові доповнюють одна одну. Це не соло одного інструмента, а злагоджений оркестр процесів, технологій і людей. Чарівної пігулки від кіберхвороб і загроз здоров'ю та коректній роботі машин і систем не існує. Кібербезпека має бути вбудованою у дизайн кожного

бізнесу й починатися з першого дня стартапу чи цифрової трансформації чинного бізнесу або державної структури.

Хоча кібератаки не відіграли ключову роль у тактичному просуванні жодної зі сторін поточної війни, їх активно застосовують як засоби знищення, підриву та вилучення цінних даних.

Кібератаки є також важливим елементом інформаційної війни. Ними активно послуговуються спецслужби ворога та спонсоровані ними злочинні угруповання для поширення дезінформації й контролю над потоками інформації.

Воєнна агресія проти України — як на полі бою, так і в кіберпросторі — вже змусила провідні країни світу переглянути свої стратегії протидії кіберзагрозам. Україна не повинна відставати й разом із перетвореннями, що відбуваються в наших збройних силах, які поступово стають одними з найкращих у світі, ми маємо також створити ефективні сили кібероперацій. Проте, створюючи їх, не забувати про захист і ще раз не забувати, що кібербезпека — це також галузь і один з критично важливих чинників конкурентоздатності в сучасному світі.

Пів року збройної боротьби проти російських загарбників засвідчили, що Україна за останні роки зробила значний крок уперед щодо стійкості до кібератак, ніж це було на початку війни росії проти України у 2014 році.

Це відбулося завдяки чотирьом чинникам:

— активній комерційній діяльності тих продуктових і сервісних компаній у сфері кібербезпеки й IT, українських і міжнародних, які працювали саме на українському ринку й для українського клієнта;

— чималій увазі до питань кібербезпеки з боку самих українських підприємств і організацій після масштабних атак 2015–2017 років;

— більш системній і цілеспрямованій роботі суб'єктів забезпечення кібербезпеки держави;

— програмам міжнародної технічної допомоги.

Цей успіх потрібно розвинути. Україна має потенціал, щоб стати лідером не лише серед сервісних, а й продуктових компаній у сфері кібербезпеки та достойно конкурувати на світових ринках.

Олег Дерев'янко,
голова ради директорів
ISSP — Information Systems Security Partners

ВИЗНАННЯ КНИГИ Н. ПЕРЛРОС «ОСЬ ТАКИМ, ЯК МЕНІ КАЖУТЬ, БУДЕ КІНЕЦЬ СВІТУ: ПЕРЕГОНИ КІБЕРОЗБРОЄНЬ»

«Цілком можливо — найважливіша книга року… Чітка, зрозуміла та переконлива презентація Ніколь Перлрос приголомшливих викриттів прихованих перегонів озброєнь» — Booklist (відмічений відгук)

«Рішуча та енергійна книга Ніколь вражає кожною сторінкою; робота нагадує найкращий вид репортажу — той, який репортер викладе вам тільки тоді, коли ви сядете з ним у барі з бокалом якогось напою. Перлрос написала ошелешливу та викривальну історію про найпотаємніші завулки Інтернету, — де хакери й уряди підпільно торгують інструментами війни майбутнього, яка водночас є і активною, і різнобарвною. „Ось таким, як мені кажуть, буде кінець світу: перегони кіберозброєнь» — це і докладна й емоційна від першої й до останньої сторінки подорож, і наполегливий заклик до дії, доки наш високотехнологічний світ ще не вийшов з-під контролю. Попри те, що кіберіндустрія вже фактично десять років входить до кола моїх інтересів, думка про те, як майстерно Перлрос вдалося дійти до суті проблеми, раз по раз виникала в моїй голові після кожного наступного прочитаного абзацу», — Гаррет М. Графф, автор бестселлера New York Times „The Only Plane in the Sky".

«Перша чернетка історії. Наріжною ниткою у роботі Перлрос пролягає питання етики: що таке насправді правильний вчинок? Надто багато людей, про яких вона пише, навіть не замислювалися про це: їхні цілі були або короткостроковими, або егоїстичними, або і перше, і друге. Гучна історія про хакерів, продавців багів і шпигунів, у якій також порушуються філософські питання», — Стівен М. Белловін.

«Туманний світ продажів нульового дня був у тіні протягом десятиліть, і мало хто був готовий говорити на цю серйозну тему. Ніколь Перлрос провела грандіозну роботу, дослідивши джерела, переконавши спеціалістів-практиків поділитися їхніми захопливими історіями і, зрештою, пояснивши, чому все це так важливо», — Кім Зеттер, авторка Countdown to Zero Day.

«Ніколь Перлрос робить те, на що в кіберсфері здатні далеко не всі автори: вона розповідає суто технічну, хоч і захопливу історію так, ніби ви сидите за келихом пива в улюбленому дайв-барі. Мастрід», — Ніна Янковіч, авторка How to Lose the Information War.

«Приголомшлива історія діджераті[1] від одного з літераторів: Ніколь Перлрос викриває приховані, спонсоровані урядом еліти, які використовують одиниці та нулі, щоб захистити нас. Або щоб нашкодити. Або щоб збагатитися», — Гленн Крамон, у минулому — старший редактор New York Times.

«Читається як трилер. Зразковий погляд зсередини на високорентабельну індустрію, що була покликана убезпечити нас, однак підвела всіх до порогу наступної світової війни», — Джон Маркофф, в минулому — кореспондент New York Times із питань кібербезпеки.

«Проливає світло на складні реалії дезінформування, хакінгу[2] та уразливостей програмного забезпечення, що є ахіллесовою п'ятою сучасної демократії. Я працюю у цій сфері як учений і технолог, і ця книга налякала мене до смерті. Прочитайте її», — Гері Макгроу, PhD, засновник Берривілльського інституту машинного навчання й автор роботи *Software Security*.

«Вихрове світове турне, що знайомить нас із дивакуватими особистостями й аналогічно шаленими історіями, які формують бекґраунд спроб установити контроль над Інтернетом. У це неможливо було б повірити, якби все це не було правдою», — Алекс Стеймос, директор Стенфордської інтернет-обсерваторії й колишній очільник служби безпеки Facebook та Yahoo.

---

[1] *Діджераті* — вищий ешелон, еліта комп'ютерної індустрії, до якої входять як учені, так й інші спеціалісти зі сфери цифрових технологій *(прим. перекладача)*.

[2] *Хакінг* — привнесення у програмне забезпечення змін із метою досягнення цілей, що відрізняються від прописаних фактичними авторами цифрового продукту *(прим. перекладача)*.

ВІД АВТОРА

Ця книга — результат більш ніж семи років інтерв'ю з понад трьома сотнями людей, які або брали участь в організації кіберударів, або вистежували їх організаторів, або просто відчули на собі вплив таємної індустрії кіберозброєнь. Мова про інтерв'ю з хакерами, активістами, дисидентами, вченими, програмістами, американськими й іноземними урядовими чиновниками, криміналістами та найманцями.

Багато хто з них люб'язно виділяли години, — а іноді навіть і дні, — реконструюючи деталі різних подій та розмов, які й було зафіксовано на цих сторінках. До джерел зверталися з проханням за можливості презентувати фактичну документацію: у формі контрактів, електронних листів, повідомлень та інших цифрових деталей, що класифікувалися або як засекречені, або — у більшості випадків — з особливим доступом відповідно до договорів про нерозголошення. Де можливо, як підтвердження власних думок і спогадів людей про окремі події було використано аудіозаписи, календарі та замітки.

З огляду на специфіку порушеного мною питання більшість із тих, з ким вдалося поспілкуватися, погодилися на розмову тільки за однієї умови: їх імена та прізвища не буде оприлюднено. Ще двоє людей погодилися дати інтерв'ю за умови, що їхні імена буде змінено. Де було можливо, інформація зіставлялася зі словами інших. (А взагалі багато хто погодився приєднатися просто для фактчекінгу слів інших людей.)

Читачеві не варто обманюватися, думаючи, що кожна особа, згадана на сторінках цієї книги, сама виступала джерелом подій та опи-

саних діалогів. Звісно, у низці ситуацій інформація надходила безпосередньо, однак в інших випадках дані збиралися від свідків, третіх сторін, і, де була можливість, із письмової документації.

І потім — як я вже зрозуміла, коли йдеться про торгівлю кіберзброєю, хакери, покупці, продавці й уряди намагатимуться зробити все можливе, щоб уникнути будь-якої письмової документації. Чимало розповідей і кумедних ситуацій було написано в стіл тільки тому, що не було способів підкріпити почуте фактами. Сподіваюсь, читач пробачить мені за такі упущення.

Я намагалася зробити все можливе, однак питання торгівлі кіберзброєю і нині є туманним. Було б просто нерозумно заявляти, що моя робота є надзвичайно вичерпною. Будь-які помилки, безумовно, лежать на мені. Утім, сподіваюсь, що моя робота допоможе пролити хоча б краплину світла на позбавлену уваги надсекретну індустрію кіберозброєнь, щоб ми, суспільство, що стоїть на порозі цього цифрового цунамі, названого Інтернетом речей, могли, доки ще не пізно, запустити бодай трохи необхідних ініціатив.

Ніколь Перлрос, листопад 2020 року

ПРОЛОГ
Київ

На момент, коли мій літак приземлявся у Києві, — це був екватор зими 2019 року, — ніхто не міг точно відповісти: чи завершилася атака, чи всі стали свідками прологу до чогось більш масштабного.

Глухі панічно-параноїдальні ноти почали оповивати наш борт, щойно ми ввійшли до повітряного простору України. Турбулентність підкинула нас так рвучко, що я, сидячи у хвості літака, відчула напад нудоти. Українка модельної зовнішності поряд зі мною схопила мою руку, заплющила очі й почала молитися.

Сотнею метрів нижче Україна дійшла до рівня помаранчевої тривоги[1]. Сильна буря зривала дахи багатоповерхівок, кидаючи їх фрагменти на проїзну частину. Села в передмісті столиці й на Заході України знеструмлювалися — знову. Коли ми зупинилися на злітно-посадковій смузі й почали пробиратися через аеропорт «Бориспіль», здавалося, що навіть молоді довготелесі українські прикордонники нервово перешіптувалися: аномальна буря? чи нова російська кібератака? У нинішню епоху ніхто вже не може сказати точно.

За день до того я попрощалася зі своєю дитиною. До Києва вирушила в рамках такого собі чорного паломництва — я поїхала дослідити «руїни» в епіцентрі найбільш нищівної кібератаки, яку знав світ. Світова громадськість усе ще оговтувалась від наслідків російської кібератаки, код якої замалим двома роками раніше спочатку зупинив роботу державних установ, залізниць, банкоматів, заправок,

[1] Помаранчевий рівень тривоги — відповідно до визначеної категорії — один із рівнів небезпеки метеохарактеру *(прим. перекладача).*

поштової служби та навіть радіаційних моніторів на ЧАЕС, а потім прорвався за кордони України й безсистемно обігнув і земну кулю теж. Вирвавшись, вірус паралізував заводи у віддаленій Тасманії, знищив вакцини в одній із найбільших фармацевтичних компаній світу, просочився в комп'ютери FedEx і занурив у колапс світового лідера з морських вантажних перевезень.

У 2017 році Кремль «присвятив» атаку Дню Конституції України, щоб послати українському народові зловісне нагадування: можна скільки завгодно святкувати свою незалежність, проте Росія-матінка завжди буде поруч.

Та атака стала кульмінацією серії віроломних кіберударів, кількість яких усе збільшувалася, — помсти за Євромайдан 2014 року, за те, що сотні тисяч українців вийшли на Майдан Незалежності, щоб виступити проти прокремлівського тіньового уряду в Україні та проти Віктора Януковича як маріонетки Володимира Путіна.

Протягом кількох наступних днів після падіння президенства Януковича Путін надав йому прихисток у Москві й відправив війська для привласнення Кримського півострова — чорноморського раю, діаманта на південному узбережжі України. Вінстон Черчилль якось назвав Крим *«Рів'єрою Аїда»*. Тепер півострів — інфернальний епіцентр конфронтації між Володимиром Путіним та українським народом — тимчасово окупований Російською Федерацією.

Відтоді цифрова армія Росії й сфокусувалася на Україні. Відтоді російські хакери й зайнялися кривавим спортом — хакінгом, спрямованим на будь-що в Україні, що має цифровий пульс. Протягом п'яти довгих років вони «обстрілювали» українців тисячами кібератак на день, безперервно скануючи мережі України на слабкі місця — ненадійні паролі, некоректні нулі, піратське й незапатчене програмне забезпечення, наспіх увімкнений брандмауер[1]. Одне слово, усього, що можна було б використати для запуску цифрового хаосу. Усього, що можна було б використати у розгортанні розбрату й підриві прозахідного уряду України.

[1] Брандмауер — фактично фільтр між Мережею та комп'ютером *(прим. перекладача)*.

Володимир Путін сформулював для своїх хакерів тільки два правила: по-перше, жодного хакінгу в межах Росії; по-друге, коли Кремль просить про послугу, ти робиш все, що потрібно. У всьому іншому хакери отримали повну автономію. І так, Путін їх одразу полюбив.

У червні 2017 року, буквально за три тижні до того як російські хакери спустошили українські системи, Володимир Путін у розмові з журналістами заявив, що вони (хакери — *прим. перекладача*), «як художники, які прокидаються вранці з хорошим настроєм і починають творити… І якщо вони відчувають у собі патріотичний поклик, то можуть спробувати зробити свій вклад у боротьбу з тими, хто некоректно відгукується про Росію».

Україна стала їхньою цифровою тестовою кухнею, жаристим пеклом, де вони могли випробовувати всі хакерські хитрощі й інструменти з цифрового арсеналу Росії без страху помсти. Тільки в перший рік, у 2014-му, російські державні ЗМІ та «тролі»[1] похитнули президентські вибори в Україні кампанією дезінформації, попереминно звинувачуючи в державному перевороті то прозахідні масові повстання, то так звану хунту, то «глибинні держави» у США та Європі. Хакери рилися в електронних поштових скриньках передвиборчої кампанії, проривалися до даних по виборцях, хакнули Центральну виборчу комісію України, видалили файли й інтегрували шкідливе ПЗ[2] в електронну базу виборчих даних, що могло призвести до помилкового оголошення переможцем президентської гонитви ультраправого кандидата (атаку було розкрито незадовго до оприлюднення результатів українськими ЗМІ). Експерти з питань організації безпеки виборів назвали все це найзухвалішою спробою підірвати національні вибори в історії.

Зазирнувши у минуле, здається, що все це мало б викликати у Сполучених Штатах Америки як мінімум тривогу. Однак 2014 року увага американців була прикута до іншого: протести у Фергюсоні, штат Міссурі; жахіття ІДІЛ з її появою буквально з нізвідки; зрештою, на мій погляд, кібератака КНДР на Sony Pictures, коли в грудні того року

[1] *Інтернет-троль* — особа, яка навмисно розпалює конфлікт одіозними, грубими й агресивними висловлюваннями в Мережі (*прим. перекладача*).

[2] ПЗ — програмне забезпечення (*прим. перекладача*).

хакери Кім Чен Ина помстилися кінокомпанії за комедію Сета Рогена та Джеймса Франко, у якій показано вбивство їхнього священного лідера. У ході атаки, що стала для Путіна ідеальним плейбуком[1] під події 2016-го, північнокорейські кіберсолдати спочатку знищили сервери Sony Pictures шкідливим кодом, а потім почали вибірково зливати[2] електронні листування, щоб принизити керівників кінокомпанії.

В очах левової частки американців Україна була світом десь там. Ми фіксували фрагменти з українцями, що протестували на Майдані, фіксували фрагменти з українцями, які святкували зміну маріонетки Путіна на прозахідний уряд. Хтось стежив за боями на Сході України. Багато хто може згадати катастрофу малайського Boeing 777, який збили незаконні збройні формування, підтримувані Росією.

Та, незважаючи на зазначене вище, якби усі ми все ж були тоді уважнішими, ми б розпізнали пекучі червоні попереджувальні сигнали, хакнуті сервери в Сінгапурі та Нідерландах, блекаути, вивантаження шкідливого коду у всіх напрямах.

Ми б зрозуміли, що кінцевою ціллю всього є не Україна. Нею були ми.

Втручання Росії у президентські вибори-2014 в Україні стало першим пострілом до того, що відбулося згодом, — мова про кампанію кіберагресії та руйнувань, яких світ ще не знав.

Вони передирали сторінки зі своїх плейбуків часів Холодної війни, і доки моє таксі їхало з Борисполя до центра Києва, я загадувалася над запитанням: яку сторінку вони оберуть наступною, і чи вдасться нам хоча б колись дістатися до місця, де можна було б очікувати їхній удар.

Суть зовнішньої політики Володимира Путіна полягала в тому, щоб послабити вплив Заходу на глобальні питання. Кожною своєю хакерською атакою чи кампанією з дезінформації цифрова армія РФ намагалася обмежити опонентів Росії у їхній політиці й відвести їх від істинної цілі російського президента: прагнення розбити статус західної демо-

[1] *Плейбук* — книга планів, тактик і комбінацій для перемоги у чому-небудь (*прим. перекладача*).

[2] *Злив інформації* — навмисне оприлюднення закритих даних з певною метою (*прим. перекладача*).

кратії і, врешті-решт, НАТО — Північноатлантичного альянсу — єдиного, що стримувало Путіна.

Чим дужче заплутувались би українці — мовляв, де ж, зрештою, допомога західних партнерів? — тим більшою була б імовірність, що вони відвернуться від Заходу в бік Росії.

А який найдієвіший спосіб спантеличити українців і змусити сумніватися в новому уряді? У розпал зими вимкнути їхнє тепло й електроенергію. Двадцять третього грудня 2015 року Російська Федерація перейшла цифровий Рубікон. Ті самі хакери, що протягом багатьох місяців закладали бекдори[1] та експлойти[2] в українських ЗМІ й державних закладах, аналогічно непомітно пролізли в системи українських електростанцій. Вони продерлися в комп'ютери, що контролювали енергосистему України, непомітно перемкнувши низку вимикачів, унаслідок чого сотні тисяч українців зосталися без електроенергії. Про всяк випадок хакери вимкнули ще й екстрену телефонну лінію. Ну і щоб закріпити вчинене, вони вимкнули резервну подачу електроенергії до диспетчерських, змусивши операторів відновлювати живлення в темряві.

Відсутність електроенергії на частині України тривала не так довго — менше ніж шість годин, однак те, що трапилося на Заході країни того дня, не мало й не має аналогів в історії. Цифрові Кассандри[3] та любителі капелюшків із фольги давно попереджали, що одного дня кіберудар буде завдано й по енергомережі, проте до 23 грудня 2015 року жодна з держав, які мають відповідні інструменти, не наважувалася натиснути на курок.

Кривдники України зробили все можливе, щоб приховати своє реальне місце перебування: вони організували атаку через хакнуті сервери в Сінгапурі, Нідерландах і Румунії, застосувавши такі рівні обфускації[4], яких кіберслідчі тоді ще не бачили. Хакери вивантажили

[1] *Бекдор* — облаштування шляхом застосування шкідливого ПЗ незаконного віддаленого доступу до ПК користувача-жертви *(прим. перекладача).*

[2] *Експлойт* — програма, що дозволяє використовувати уразливості в програмному забезпеченні для атаки на систему *(прим. перекладача).*

[3] *Кассандра* — у давньогрецькій міфології — царівна із даром пророцтва (*прим. перекладача*).

[4] *Обфускація* — в широкому сенсі заплутування коду (*прим. перекладача*).

свою кіберзброю в українські мережі в замаскованих під безневинні фрагментах, щоб обійти детектори проникнення, і ретельно рандомізували свій код, щоб перехитрити антивірусну програму. Втім, українські високопосадовці все одно відразу зрозуміли, хто стоїть за ударом: підготовка та ресурси, яких вимагала атака такої складності, для звичайного доморощеного хакера були просто недоступні.

Мотиви тієї атаки мали не фінансовий характер — установка була політичною. І протягом наступних кількох місяців спеціалісти з кібербезпеки це підтвердили: вони простежили зв'язок кібердару з російським розвідувальним підрозділом і розкрили мотиви останнього. Та кібератака була спланована, щоб нагадати українцям про слабкість їхнього уряду, про силу Росії і про глибину контролю цифровими силами Путіна систем України.

А для перевірки того, чи було засвоєно урок, ті самі російські хакери дванадцять місяців по тому — в грудні 2016-го — ще раз зоставили Україну без енергії. Тільки тепер вони вимкнули тепло й електроенергію в самому Києві, а від демонстрації своїх сил й умінь здригнулися навіть колеги в штаб-квартирі Агентства національної безпеки США (АНБ) у Форт-Міді, штат Мериленд.

Протягом багатьох років національна розвідка називала Росію та Китай найгрізнішими супротивниками США у кіберсфері.

Китай завдавав чимало проблем не так через свою особливість, як просто через те, що китайські хакери були надзвичайно вмілими в крадіжках американських комерційних таємниць. Кіт Александер, колишній директор АНБ, якось назвав китайський кібершпіонаж «найбільшим передиранням багатства в історії». Китайці витягували кожну крихту американської інтелектуальної власності, — з того, що було варте крадіжки, — передаючи все своїм державним підприємствам для копіювання.

На високих позиціях у списку кіберзагроз також були Іран і КНДР. Обидві країни ніколи не приховували бажання заподіяти шкоду Сполученим Штатам. Зокрема, Іран свого часу обвалив сайти американських банків, а коли власник казино Las Vegas Sands Шелдон Адельсон публічно закликав Вашингтон завдати по іранській землі авіаудар, іранські хакери знищили комп'ютери Las Vegas Sands. Іран також має відповідати за

блокування шахрайською програмою роботи американських лікарень, компаній і навіть цілих містечок. КНДР же, як уже згадувалося, якось знищила американські сервери тільки за те, що Голлівуд нібито образив Кім Чен Ина. Крім того, кіберсолдати Північної Кореї відзначилися тим, що викрали з банку в Бангладеш 81 млн доларів.

Водночас ніколи не було сумнівів, що в аспекті майстерності з-поміж інших завжди виділялася Росія. Російські хакери — чи то за наказом Кремля, чи то за патріотичним покликом (як це було, коли вони перевели в офлайн-режим всю Естонію, коли естонці наважилися прибрати статую радянської епохи) — проникали в Пентагон, Білий дім, Об'єднаний комітет начальників штабів, Державний департамент і російський молодіжний рух «Наши». В рамках однієї з кібератак російські кіберсолдати, видаючи себе за ісламських фундаменталістів, вимкнули від ефіру десяток французьких телеканалів. Їх викрили, коли вони намагалися обійти пристрої захисту в саудівській нафтохімічній компанії, що стало ще одним мотивом для організації глобального кібервибуху. Вони втрутилися у референдум щодо членства Британії у ЄС, хакнули американську енергомережу, 2016 року здійснили спроби повпливати на результати виборів у США, на французькі вибори, на роботу системи Всесвітнього антидопінгового агентства і, зрештою, на організацію самої Олімпіади.

Утім, попри все сказане вище, загалом до 2016 року розвідувальна спільнота США й далі думала, що можливості Америки значно перевершують ресурс супротивника. Кремль випробовував в Україні найкращі зі своїх кіберрозробок, але контррозвідка США вважала, що можливості Росії й близько не можна зіставити з американськими.

Розклад сил, можливо, був би таким і надалі (хоча як довго — важко сказати), та в період із 2016-го по 2017 роки різниця між рівнем кіберсил США та всіх інших без винятку країну світу (зокрема зловмисних сторін) значно скоротилася. Починаючи з 2016 року, кіберарсенал АНБ США — єдина причина, через яку Сполучені Штати зберігали свою наступальну перевагу в кіберпросторі, — почала зливати в Мережу загадкова група, яку не вдається ідентифікувати навіть сьогодні. Протягом дев'яти місяців таємничий хакер — чи, знову ж таки, хакери — під ніком Shadow Brokers виставляв розроб-

лені АНБ інструменти для хакінгу в загальний огляд: будь-яка держава, кіберзлочинець чи терорист могли спокійно використовувати їх у своїх хрестових кіберпоходах.

Зливи Shadow Brokers потрапили на перші шпальти, але, як і більшість новин у період 2016–2017 років, не зафіксувалися в головах американців. Розуміння громадськістю того, що відбувалося, було, м'яко кажучи, недостатнім, ураховуючи серйозність ситуації і той ефект, що зливи хакерів матимуть на АНБ, американських союзників, деякі з найбільших корпорацій США та американські містечка.

Зливи Shadow Brokers дали світові перше уявлення про найпотужніший і невидимий кіберарсенал на планеті. Хакери оголили колосальну урядову програму, про яку ви ніколи не чули: операцію зі шпіонажу та кіберозброєння, яка була такою секретною, що протягом кількох десятиліть — завдяки підставним компаніям, найманцям, чорним бюджетам, договорам про нерозголошення і на початку величезним сумкам із грошима — про неї взагалі нічого не було відомо.

На момент, коли Shadow Brokers почали поширювати кіберзброю АНБ, я вже протягом чотирьох років спостерігала за цією програмою агентства — відколи побачила згадку про неї в документах, злитих колишнім співробітником АНБ Едвардом Сноуденом. Я ознайомилась із 30-річною історією програми. Зустрілась із її Хрещеним батьком. Зустрілася з її хакерами, її постачальниками, її найманцями. Тісно познайомилася з її послідовниками (а вони з'являлися по всьому світу). Дедалі більше я комунікувала з чоловіками та жінками, життя яких зруйнували їхні ж інструменти.

Фактично єдине, чого я не бачила на власні очі, — як саме все сталося, коли надпотужна кіберзброя Агентства національної безпеки США потрапила до рук супротивника.

Отож, у березні 2019 року я поїхала в Україну, щоб власноруч ознайомитись із «руїнами».

Атаки Росії на енергосистему України відкрили світові нову главу кібервійни. Однак навіть кіберудари 2015 року меркнуть проти того, що сталося, коли два роки по тому Росія заволоділа зразковими хакерськими інструментами АНБ.

27 червня 2017 року Росія вдарила по Україні кіберзброєю АНБ у рамках того, що стало найбільш руйнівною та найдорожчою кібератакою в історії людства. Того дня практично кожен українець побачив перед собою чорний екран: багато хто не міг зняти гроші в банкоматах, розрахуватися за пальне на АЗС, відправити чи отримати е-мейл, придбати квиток на потяг, скупитися у продуктовому магазині, забрати заробітну плату. Найбільше, що лякало, — без контролю були прилади моніторингу рівнів радіації на ЧАЕС. І це, зверніть увагу, я кажу тільки про Україну.

У результаті атаки постраждало чимало компаній, що вели бізнес із Україною. Для виведення з ладу цілих Мереж потрібен був усього-на-всього один український робітник, що працював дистанційно. Постраждали всі: фармацевтичні компанії Pfizer і Merck; Maersk — конгломерат, що спеціалізується на морських вантажних перевезеннях; FedEx; шоколадна фабрика Cadbury в Тасманії. Бумерангом кіберудар навіть повернувся в Росію, знищивши дані «Роснєфті», державного нафтового гіганта та «Евраза» — сталеливарної компанії, що належить двом російським олігархам. Росіяни використали викрадений код АНБ як ракету для виведення шкідливого ПЗ на орбіту Землі. Зло, що торкнулося всього світу, тільки Merck і FedEx коштувало понад 1 млрд доларів.

На момент мого візиту до Києва у 2019 році сума збитків конкретно від цієї однієї атаки Росії перевищувала 10 млрд доларів (проте оцінки ще збільшувалися). Системи вантажоперевезень і залізничні системи все ще не повернулися до своїх звичайних показників. По всій Україні люди й досі намагалися знайти загублені після падіння систем відстеження посилки. Дехто все ще чекав на пенсії, затримані після атаки. Списки тих, хто мав отримати додаткові виплати, було стерто.

Спеціалісти з кібербезпеки дали цій атаці в буквальному сенсі не бажану назву NotPetya. Річ у тому, що спочатку вони подумали, що вірус є вже відомою шахрайською програмою Petya. Як виявилось пізніше, припущення було помилковим: російські хакери навмисно замаскували NotPetya під пересічну шахрайську програму. Навіть якщо людина все-таки вирішувала заплатити певну суму, шансів повернути дані вона не мала. Вірус був справжнісінькою санкціонованою державою зброєю, призначеною сіяти масові руйнування.

Ухиляючись від крижаних повітряних мас із Сибіру, я провела в Україні наступні два тижні. Зустрічалася з журналістами. Гуляла Майданом Незалежності разом із демонстрантами, які розповідали мені про найкривавіші дні революції. Їздила у промислову зону, щоб зустрітися з цифровими детективами, які провели мене через цифрові уламки NotPetya. Побачилася з українцями, чий родинний бізнес — програмне забезпечення для подання податкової звітності, яким користувалися всі великі українські агентства та компанії — й став нульовим пацієнтом для російського вірусу. Росіяни віртуозно замаскували свого шкідника під буденне оновлення до податкового ПЗ і тепер керівники можуть чи то плакати, чи то сміятися з ролі, яку відіграли в міждержавній кібервійні. Також я поспілкувалася з очільником кіберполіції України та з тими українськими міністрами, хто виявив бажання зустрітися.

Я відвідала американських дипломатів у посольстві США (незадовго до того, як їх було втягнуто в процедуру імпічменту Дональду Трампу). У день мого візиту вони були приголомшені останньою російською кампанією з дезінформації: російські тролі наповнювали популярні серед українських матерів сторінки Facebook антищеплювальною пропагандою. Країна тоді оговтувалася від найгострішого спалаху кору в сучасній історії. Україна мала одні з найнижчих показників вакцинації у світі, і Кремль наживався на хаосі. Ба більше: спалах в Україні почав поширюватися й на США, а тролі почали закидати антищеплювальними мемами й американців. Американські чиновники, здавалося, не розуміли, як стримати все це. (Варто сказати, що рік по тому, коли росіяни зіграли на пандемії, щоб поширити конспірологічну теорію, відповідно до якої COVID-19 є чи то біологічною зброєю американського виробництва, чи то інструментом зловісної змови Білла Гейтса з метою заробити на вакцинах, американські дипломати були підготовлені не краще.) Здавалося, що в прагненні розділяти та володарювати для Росії не існує меж.

Конкретно тієї зими 2019 року більшість погоджувалася, що NotPetya став найсміливішим творінням Кремля. В усьому Києві за два тижні перебування я не зустріла жодної людини, яка б не пам'ятала про кібератаку. Кожен згадував, де був і що робив, коли монітори погасли. Для українців той удар став Чорнобилем XXI століт-

тя. На самій ЧАЕС комп'ютери також стали «чорними, чорними, чорними», як мені розповів неговіркий технічний адміністратор станції Сергій Гончаров.

Гончаров саме повертався з обідньої перерви, коли годинник показував 13:12, і 27 комп'ютерів вимкнулися протягом наступних семи хвилин. Посипалися дзвінки; все лежало[1]. Коли Гончаров намагався запустити бекап[2] Мережі, йому зателефонували й повідомили, що комп'ютери, призначені для моніторингу рівнів радіації над сумнозвісним реактором, теж вимкнулися. Ніхто не міг відповісти, чи була радіація в межах норми, і чи це справді можна було назвати актом підступного саботажу.

Тієї миті ми були такими заклопотаними процесом відновлення комп'ютерів, що якось особливо і не думали про причини всього, — розповідав мені Гончаров. — *Та щойно ми побачили, з якою швидкістю поширюється вірус, то зрозуміли, що дивимось на щось значно фундаментальніше, а також зрозуміли, що на нас напали.*

Гончаров увімкнув гучномовець і наказав усім, хто ще міг його чути, висмикнути їхні комп'ютери з розеток. Він проінструктував колег вийти й почати вручну моніторити рівні радіації безпосередньо в серці зони відчуження.

Гончаров — людина небагатослівна. Навіть якщо він описував найгірший день свого життя, він розповідав монотонним голосом. Він не був схильним до гучних емоцій. Однак у день атаки NotPetya, за його словами, «він впав у шок». І я не була впевнена, що два роки по тому він вибрався з нього.

Тепер ми живемо в абсолютно іншу епоху, — сказав він мені у розмові. — *Життя розділилося на період до NotPetya і після NotPetya.*

Куди б протягом тих двох тижнів я не пішла, всюди українці говорили те саме. На автобусній зупинці я зустріла чоловіка, який на момент атаки саме купував авто: автосалон відмовив йому — вперше в історії продажів вживаних авто? — одразу, як системи реєстрації впали. У кав'ярні я перетнулася із жінкою, справа життя якої — невеличкий онлайн-магазин трикотажу. Вона збанкрутіла після того, як поштова

[1] *Сленг* — було виведене з ладу (*прим. перекладача*).

[2] Резервна копія *(прим. перекладача).*

служба загубила її посилки. Багато хто розповідав, як вони не могли зняти гроші чи розрахуватися за бензин на АЗС. Загалом усі, як і Гончаров, просто запам'ятали, з якою швидкістю все виходило з ладу.

Ураховуючи таймінг — напередодні Дня Незалежності України[1] — з'єднання усіх точок не зайняло багато часу. Але стара й озлоблена Росія-матінка все ж познущалася з українців знову. Втім, український народ — це стійкі люди. За 27-річну історію трагедій і криз вони розвинули в собі почуття чорного гумору. Хтось жартував, що обвалом усіх систем Вова — прізвисько Путіна — додав кілька днів до їхнього святкового вікенду. Хтось сміявся, що атака стала першою за довгі роки причиною відірватися від Facebook.

Попри психологічний шок і фінансові втрати від подій червня 2017 року, українці все ж визнавали, що все могло завершитися значно гірше. Безумовно, нормальне функціонування відділів по роботі з клієнтами було значно ускладнене. Важливі дані загубилися назавжди. Однак атака припинилася за мить до можливих смертоносних катастроф на кшталт падіння пасажирських лайнерів чи руйнівних вибухів. Фактично, крім ситуації з моніторами радіації на ЧАЕС, усі інші українські атомні електростанції функціонували у штатному режимі.

Зрештою, удару Москва все ж завдала. Як і в разі з атаками на енергомережу — коли напруги не було протягом достатнього для транслювання меседжу часу, — збиток від NotPetya був значно меншим, порівнюючи з тим, що Росія могла зробити, враховуючи диспозицію й американський кіберарсенал у її руках.

Дехто висловив припущення, що Росія застосувала викрадений арсенал АНБ, щоб втерти ніс американському агентству. Українські експерти з питань кібербезпеки, з якими я поспілкувалася, мали іншу тривожну теорію: атака NotPetya, як і удари по енергомережі до цього, були просто репетицією.

Саме це Олег Дерев'янко, експерт у сфері кібербезпеки, сказав мені одного вечора в ресторані, коли ми куштували українські страви — вареники та холодець. Фірма Дерев'янка була на передовій, коли

[1] Помилка автора — насправді атака сталася напередодні Дня Конституції *(прим. ред.)*.

Росія завдала кіберудару. Знову і знову експертиза показувала, що росіяни просто експериментували. Вони вдалися до жорстокої версії наукового методу: тестували один інструмент тут, інший — там, відточуючи свої знання в Україні й демонструючи, — водночас просуваючись вгору кар'єрними сходами, — російським лідерам, як саме можна все провернути.

За словами Дерев'янка, існувала причина того, чому атака NotPetya була такою руйнівною й фактично стерла інформацію з 80% комп'ютерів в Україні. *Вони просто прибирали за собою. Все це — новітня зброя у новій війні. Україна виступила для них полігоном. Як вони планують застосовувати їхню зброю далі? Ми не маємо відповіді*, — розповів Олег

Від моменту атаки NotPetya — протягом наступних двох років — кіберударів подібного масштабу Україна більше не зазнавала. Незважаючи на деякі свідчення про наміри Росії втрутитися у вибори-2019 в Україні, хвиля кіберруйнувань послабилася до мінімуму.

Це означає, що вони пішли далі, — сказав мені Дерев'янко.

Ми мовчки подивилися на холодець, попросили чек і вийшли на вулицю. Здавалося, вперше за тривалий час крижані вітри стихли. Хоча зазвичай жваві й вимощені бруківкою вулички старого Києва все одно були безлюдними. Ми пішли Андріївським узвозом — своєрідним київським Монмартром — повз художні галереї, антикварні лавки та артстудії до Андріївської церкви, збудованої у 1700-х роках як літню резиденцію імператриці Єлизавети.

Коли ми порівнялися з величною церквою, Дерев'янко зупинився. Він глянув на жовте сяйво ліхтарного стовпа над нами.

Знаєте, — сказав він тоді, — *якщо вони вимкнуть світло у нас, ми зостанемось без електроенергії ймовірно на кілька годин. Але якщо вони зроблять те саме з вами…*

Він не закінчив думку, але йому й не потрібно було. Я вже неодноразово чула її і від моїх джерел у Сполучених Штатах, і від його співвітчизників.

Ми всі знали, що тоді буде.

Те, що врятувало Україну, робить США найуразливішою державою на планеті.

Україна не була повністю автоматизованою. Країна значно відставала в перегонах за те, щоб приєднати все до Інтернету. Цунамі, відоме, як Інтернет Речей, що практично поглинуло американців в останнє десятиліття, тоді ще не докотилося до України. Українські атомні електростанції, лікарні, хімічні заводи, нафтопереробні заводи, нафто- й газопроводи, фабрики, ферми, міста, автомобілі, світлофори, будинки, термостати, лампочки, холодильники, кухонні плити, радіоняні, електрокардіостимулятори, інсулінові помпи тощо ще не були веборієнтованими.

Натомість у Сполучених Штатах Америки зручність уже була ознакою всього — так є й сьогодні. Ми приєднували до Інтернету все що могли зі швидкістю 127 девайсів на секунду. Ми повірили в ідею Кремнієвої долини про бездротове суспільство. В нашому житті вже не було жодної сфери, яка не була б оповита всесвітньою павутиною. Ми тепер могли контролювати і життя, і економіку, і енергомережу шляхом тільки дистанційних вебсистем. І ми ніколи не замислювалися, що таким чином створили ще й найбільший у світі простір для атакувальних маневрів.

В АНБ — чия подвійна місія полягає в збиранні розвідданих по всьому світу та захисті секретів США — напад давно став більш пріоритетним, ніж захист. На кожну сотню кібервоїнів, які атакували, припадав один-єдиний аналітик захисту. Злив Shadow Brokers став, безумовно, найбільш руйнівним в історії американської розвідки. Якщо Сноуден просто виклав ключові тези в PowerPoint, Shadow Brokers вручили нашим ворогам справжню зброю — код.

Найважливіший секрет кібервійни полягає в тому, що та сама держава, яка має найліпші кіберресурси для атаки, водночас входить до категорії найуразливіших. І наші супротивники тепер теж це добре знають.

Україна мала ще одну перевагу над США — відчуття крайньої потреби негайно реагувати. Після п'яти років блекаутів і атак із боку одного з найсильніших хижаків на планеті, в Україні вже усвідомлювали, що їхнє майбутнє залежить від сильного кіберзахисту. NotPetya в багатьох сенсах був шансом запустити все заново, вибудувати з нуля нові системи й захистити найкритичніші національні Мережі від Ін-

тернету. Через кілька тижнів після мого відльоту українці проголосують на президентських виборах на папері. Не буде жодних пристроїв для маркування бюлетенів; кожен голос буде вписано вручну. Паперові бюлетені також підраховуватимуть вручну. Звісно, це все одно не врятує від фальсифікації. Показово, що будь-кому, кого я зустрічала в Україні, ідея перенести вибори на комп'ютери здавалася справжнім безумством.

США зі свого боку ніяк не могли дійти більш тверезих висновків. Ми не помітили зсуву світу потенційної війни із суші, моря та повітря у цифрову площину. Буквально через кілька місяців після мого повернення з України американців уже хвилювали не російські атаки на Україну, а роль держави у навислому тоді імпічменті Трампа. Ми якось забули, що крім кампанії з дезінформації у 2016 році — дампінгу електронних скриньок демократів, росіян, які, щоб посіяти розбрат, видавали себе за техаських активістів Black Lives Matter, — російські хакери також зондували серверні аспекти наших виборчих систем і дані про реєстрацію виборців у всіх п'ятдесяти штатах. Вони, можливо, й не порушили процедуру остаточних підрахунків голосування, та все, що робилося на той момент, було, як зазначали американські високопосадовці, пробною підводкою до майбутнього кібератаки по американських виборах.

Трамп же безперестанку звинувачував у втручанні у вибори 2016 року то доморощеного 200-кілограмового хакера, то Китай. На пресконференції в Гельсінкі у 2018 році Дональд Трамп не лише зневажливо поставився до інформації своєї розвідки — *Я знаю президента Путіна; він щойно сказав, що це не Росія. І тому, я не бачу жодних підстав не вірити*, — але й радо погодився на пропозицію Путіна, який весело гримасував поряд із Трампом, дозволити Росії приєднатися до Штатів у полюванні на саму себе за події 2016-го. Крім того, напередодні нових виборів Путін і Трамп зустрілися знову: цього разу в Осаці у червні 2019 року, де привіталися так, ніби давні й хороші університетські приятелі. Коли журналіст запитав у Трампа: чи попередив той Росію, щоб та не втручалась у 2020 році — Трамп посміхнувся й по-доброму махнув пальцем у бік свого друга: *Не втручайтеся у вибори, пане президенте*.

ЗМІСТ