ДЖОЗЕФ МЕНН

КУЛЬТ МЕРТВОЇ КОРОВИ

Як оригінальна
хакерська супергрупа
могла би врятувати світ

ВИДАВНИЦТВО
ФАБУЛА
#PRO

Джозеф Менн

КУЛЬТ МЕРТВОЇ КОРОВИ:
як оригінальна хакерська супергрупа могла би врятувати світ

Видавництво «Фабула»
2021

Оригінальна назва твору:
CULT OF THE DEAD COW:
How The Original Hacking Supergroup Might Just Save The World

Це видання опубліковане за домовленістю з Public Affairs, частиною Perseus Books, LLC, підрозділу Hachette Book Group, Inc., Нью-Йорк, штат Нью-Йорк, США.
Всі права збережено.

Copyright © 2019 by Joseph Menn

© М. Хандога, пер. з англ., 2021

© «Фабула», макет, 2021

© Видавництво «Ранок», 2021

ISBN 978-617-09-7481-5 (epub)

Жодна частина цієї книжки не може бути відтворена в будь-якій формі без письмового дозволу власників авторських прав.

Електронна версія створена за виданням:

Джозеф Менн

М50 Культ мертвої корови: як оригінальна хакерська супергрупа могла би врятувати світ/ пер. з англ. М. Хандога. — Харків : Вид-во «Ранок» : Фабула, 2021. — 240 с.

ISBN 978-617-09-7366-5

Наше життя стрімко переїжджає в онлайн, але мало хто розуміє примарність мереживної безпеки. У цій книжці журналіст Джозеф Менн розповідає про найпершу, найбільшу і найвпливовішу хакерську групу «Культ мертвої корови», і справжні імена деяких членів цієї групи саме тут розкриваються вперше. Хакери з «Культу мертвої корови» на ти з комп'ютером з динозаврових часів першого інтернету. Саме вони непокоїлись про безпеку особистих даних користувачів, коли виробникам програмного забезпечення на це було начхати, саме вони співпрацювали з урядом США після 11/09, саме вони перші порушували етичні питання в користуванні інтернетом. Ці хакери не спрямовували свої вміння і знання на те, щоб заволодіти грошима чи з тіні

керувати країнами,— вони стали на захист прав людини і досягли в цьому неабияких успіхів.

Джозеф Менн нагадує, що ситуація з безпекою в інтернеті гіршає, і ця книжка — спосіб привернути увагу до проблеми, відкрито її назвати і обговорити. Це видання буде корисне всім, хто цікавиться сучасними технологіями, знає, хто такі тролі та боти, користується інтернет-банкінгом та любить шопінг онлайн.

УДК 004.4:316.453

Шановний читачу!

Спасибі, що придбали цю книгу.

Нагадуємо, що вона є об’єктом Закону України «Про авторське і суміжні право», порушення якого карається за статтею 176 Кримінального кодексу України «Порушення авторського права і суміжних прав» штрафом від ста до чотирьохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, з конфіскацією та знищенням всіх примірників творів, матеріальних носіїв комп’ютерних програм, баз даних, виконань, фонограм, програм мовлення та обладнання і матеріалів, призначених для їх виготовлення і відтворення. Повторне порушення карається штрафом від тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк, з конфіскацією та знищенням всіх примірників, матеріальних носіїв комп’ютерних програм, баз даних, виконань, фонограм, програм мовлення, аудіо- і відеокасет, дискет, інших

носіїв інформації, обладнання та матеріалів, призначених для їх виготовлення і відтворення. Кримінальне переслідування також відбувається згідно з відповідними законами країн, де зафіксовано незаконне відтворення (поширення) творів.

Книга містить криптографічний захист, що дозволяє визначити, хто є джерелом незаконного розповсюдження (відтворення) творів.

Щиро сподіваємося, що Ви з повагою поставитеся до інтелектуальної праці інших і ще раз Вам вдячні!

Присвячується пульмонологу Це-Мін (Бенсону) Чену, який врятував моє життя після Def Con 2014 року

ПЕРЕДМОВА АВТОРА

Технології вирішують долю світу, і ми в їхніх кайданах. Електронний нагляд, кібервійна, штучний інтелект і використовувані з корисливою метою соціальні мережі ось-ось штовхнуть спільноти за точку неповернення. Навіть ті з нас, хто це передбачив, не думали, що це станеться настільки лиховісно, настільки швидко і точно не в такий спосіб.

Протягом останніх двох десятиліть я висвітлював технологічну галузь як журналіст, і найчастіше мене цікавили питання безпеки та приватності. Вони миттєво перетинають межу між бізнесом і політикою та кидають виклик нашим уявленням про безпеку, свободу та справедливість. Захопливо спостерігати й іноді брати участь у подіях, коли уряди, компанії та люди з активною громадянською позицією намагаються подолати щоразу нові наслідки. Безпека тісно пов'язана з владою. І її стан дедалі ускладнюється, відколи інтернет вийшов з контрольованого університетського середовища у 1980-х.

Працюючи у Кремнієвій долині над своєю першою книжкою, у якій ішлося про злет і падіння *Napster*, я почав сильніше перейматися комп'ютерною безпекою — чи її відсутністю. Шон Феннінг був одним із перших хакерів, яким захоплювалася публіка, і йому допомагала досвідченіша команда, зокрема деякі люди, з якими я підтримував зв'язок і які є героями цієї книжки. Хоча звукозаписна індустрія з цим не погодилася б, члени команди Феннінга були переважно хорошими хлопцями, які експериментували, щоб навчитися, а не бути зловмисниками. Але всі підказані ними тенденції були негативними.

Коли стан безпеки погіршився та ставки зросли, я присвятив цій темі свою книжку *Fatal System Error*. Вона показала масштаб небезпеки, акцентуючи на тому, як організована злочинність і деякі наймогутніші уряди світу співпрацюють, щоб скористатися мінімальним регулюванням, недосконалими у своїй основі технологіями, нездатністю ринку створювати якісні засоби гарантування безпеки. У центрі тієї книжки була

правдива історія співпраці російської розвідки з кримінальними хакерами — сценарій, який перетворився з неймовірного на момент публікації 2010 року на широко визнаний сьогодні.

Відтоді багато книжок розглядали військово-інтернетівський комплекс, збирання розвідувальних даних, кібервійну, історію *WikiLeaks*, Едварда Сноудена та вибори в США 2016 року. Та їм усім бракує захопливої розповіді про відданих інформаційній безпеці людей, які працюють поза громадською увагою чи навіть у тіні, захищаючи наші персональні дані та свободу, а також нашу національну безпеку. У багатьох випадках ці люди набагато яскравіші за своїх супротивників. Це особливо справедливо для людей, чию історію викладено в цій книжці,— головних членів «Культу мертвої корови», які зіграли свою роль у всіх вищезгаданих серйозних подіях і явищах. Хоча їхні публічні витівки притягали увагу в минулому, до сьогодні ніхто не чув їхню справжню історію, а деякі молоді хакери взагалі про них не знають. Але «Культ мертвої корови» — це основний ключ до всієї саги сучасної безпеки, особливо до зусиль збагнути, що етично. Він допомагає багатьом іншим, хто виконує героїчну роботу поза полем зору громадськості.

Книжка *Fatal System Error* була серйозним попередженням тоді, коли багато хто перебував у невіданні. Тепер, у часи масштабнішої моральної кризи в технологіях, ця книжка — рідкісне висловлення надії та натхнення розв’язати гостріші проблеми, доки не стало надто пізно.

Джозеф Менн

Гравці

«Культ мертвої корови»

Кевін Вілер / Swamp Rat

Білл Браун / Franken Gibe

Psychedelic Warlord

Керрі Кемпбелл / Lady Carolin

Джессі Драйден / Drunkfux

Пол Леонард / Obscure Images

Кріс Такер / Nightstalker

Ден Макміллан / White Knight

Міша Кубека / Omega

Джон Лестер / Count Zero

Люк Бенфі / Deth Vegetable

Сем Ентоні / Tweety Fish

Пейтер Затко / Mudge

Лейрд Браун / Oxblood Ruffin

Джош Бухбіндер / Sir Dystic

Крістіан Pio / Dildog

Адам О'Доннелл / Javaman

Джейкоб Еплбаум / lOerror

Кемаль Акман / Mixter

Патрік Крупа / Lord Digital

Ninja Strike Force

Кріс Вісопал / Weld Pond

Віндоу Снайдер / Rosie the Riveter

Лімор Фрід / Lady Ada

Legion of Doom

Кріс Ґоґґанс

Скотт Чейсін

Masters of Deception

Еліас Ладопулос / Acid Phreak

Марк Абен / Phiber Optik

@stake

Алекс Стеймос

Роб Бек

Девід Лічфілд

Кеті Муссуріс

Розділ 1.
ВЕЧІР У САН-ФРАНЦИСКО

У жовтні 2017 року у вівторок увечері[1] близько тридцяти друзів і знайомих зібрались у таунхаусі інженера систем безпеки Адама О'Доннелла на захід із політичного збору коштів. Хоча бум нерухомості на Території затоки Сан-Франциско позбавив більшість американців доступу до пагорба в Ґлен-Парк, за місцевими стандартами будинок був скромним. Для тих, хто прийшов на звану вечерю, не вистачало стільців, і гості стоячи робили собі тако й пили вино з пластянок. Адам, уродженець Філадельфії, не був чванькуватим керівником із Кремнієвої долини. Він купив будинок перед останнім житлобудівним бумом на гроші від продажу сек'юріті-компанії, у якій він працював, гіганту *Cisco Systems*. Адам приєднався до компанії — об'єкта поглинання, коли вона купила стартап, який він співзаснував 2009 року. Цей стартап рано скористався тим, що стало відомим як «хмара», і захищав комп'ютери від вірусів швидше за конкурентів. Тепер Адам нервово походжав своїм домом, дякував гостям за їхній прихід і подумки повторював розрахунки, сподіваючись, що мінімум у 250 доларів на людину виправдає авіаподорож кандидата.

Адам не звик розважати людей[2], яких погано знав. Незабаром йому виповниться сорок. Він був дитиною з робочого класу, якій подобалося бавитися з технікою, і врешті-решт він здобув ступінь доктора технічних наук.

Навіть коли хакінг став темою незліченних заголовків новин і скандальних виборів, незадекларованим способом ведення війни, Адам залишився в тіні.

У *Cisco* Адам працював над рідкісним, спільним з *Apple* проєктом, метою якого було допомогти компаніям захистити айфони працівників. У цьому не було чогось особливо шикарного. Його найцікавішою роботою було те, про що він не розповідав. Під ніком Javaman Адам був давнім членом найстарішої, найвідомішої та найважливішої хакерської групи всіх часів — «Культу мертвої корови»[1]. Заходячи в його дім, деякі хакери старої школи бачили череп корови, що висів у холі, і розуміли послання. А якщо не розуміли, Адам не пояснював.

[x x]

Хоча в ній ніколи не було більше двадцяти членів водночас, група *cDc* має багату історію. Коли вона перетворилася з доінтернетівської спільноти на дещо схоже на хакерський мистецький гурт, члени *cDc* організували перші хакерські збори, на які запросили представників ЗМІ та правоохоронних органів. Вони розробили хакерські інструменти, якими донині користуються злочинці, шпигуни та професійні системні адміністратори. І вони вигадали термін *хактивізм*[3], який група визначила як хакінг на захист прав людини. Вона зрідка приймала нових членів, а коли це відбувалося, *cDc* зазвичай обирала людей, які вже зарекомендували себе в інших групах. Це робило її супергрупою у рок-н-рольному сенсі — групою, сформованою з учасників інших груп. Із розвитком *cDc*

його члени ставали лідерами у перетворенні хакінгу з хобі на професію, на спосіб ведення війни. В останнє десятиліття той спосіб поширився та виявив себе в очолюваній США кібератаці *Stuxnet* на ядерну програму Ірану, російському виведенні з ладу електричних систем в Україні та методичному викраденні Китаєм західних комерційних таємниць. Нестримна напівавтоматизована пропаганда, яка допомогла проштовхнути обрання Дональда Трампа 2016 року, була лише найостаннішим, найскладнішим і найефективнішим трюком. Такі інформаційні операції та саботаж погрожують тривати невідомо скільки та майже безконтрольно по всьому світу.

Більшість членів «Культу мертвої корови» залишилися анонімними, хоча шістнадцять погодилися, щоб їхні імена вперше назвали на цих сторінках, включно з усіма раніше прихованими основними учасниками. Та невидимість, яка брала початок від заснування групи 1984 року[4], посилила її таємничість. Це також надавало близько п'ятдесятьом колишнім учасникам більше свободи у керуванні світом, уникаючи суджень взагалі чи помилкових суджень зокрема, у деяких випадках вони досягали впливового суспільного положення. Втім, деякі за ці роки стали не просто публічними, а знаменитими людьми, як-от Пейтер Затко, відомий онлайн як Mudge (Мадж). У Бостоні він очолював хакерську групу «білих капелюхів»{2}, що називалася *L0pht*,— першу, яка попереджала виробників софту про вади в їхніх продуктах замість просто експлуатувати їх, щоб проникнути в комп'ютери користувачів. Потім його команда перетворила *L0pht* на першу велику консалтингову групу зіркових хакерів під назвою *@stake*.

Пізніше Мадж керував діяльністю з кібербезпеки в Агентстві передових оборонних дослідницьких проєктів США (*DARPA*), сприяючи і військовій обороні США, і досі засекреченим кібератакам, які запобігли масштабнішому насильству на Середньому Сході.

Ще більш відомим в останні роки був Джейкоб Еплбаум під псевдонімом IOerror. Харизматичне американське обличчя *Tor*, найважливішого інструмента збереження приватності в мережі, Джейк був одним з останніх лояльних помічників Джуліана Ассанжа, і він особисто викрив хакерські інструменти, розроблені Агентством національної безпеки. Коли його власні послідовники вивели на чисту воду сексуальні домагання Джейка, «Культ мертвої корови» публічно вигнав його. Але, мабуть, найвпливовішим в управлінні хакерською культурою серед членів *cDc* є Лейрд Браун, відомий більшості за своїм ніком Oxblood Ruffin. Батько хактивізму, Лейрд вигадав деякі факти і був ближчим, ніж усвідомлювали його послідовники, до фігур західної розвідки, але зробив моральні міркування центром глобальних дебатів і врятував безліч життів.

Оскільки вони були першими, хто намагався вирішити багато етичних проблем комп'ютерної безпеки, члени *cDc* надихнули легіони хакерів і професіоналів, які прийшли після них. Люди з *cDc* та їхні учні консультували президентів США, членів уряду та генеральних директорів *Microsoft*, *Apple* і *Google*. І коли питання технічної безпеки перетворилися на питання громадської безпеки, національної безпеки та врешті-решт — майбутнього демократії, «Культ мертвої корови» впливав на найважливіші рішення й національний діалог, хоча мало хто знав про його роль. У Кремнієвій

долині 2018 року *cDc* розділив непряму відповідальність за простих інженерів, які посилаючись на права людини, протестували проти співпраці своїх компаній з імміграційними органами влади, Пентагоном і Китаєм.

[x x]

Адам брав участь в інших політичних кампаніях, особливо після обрання Трампа. Зокрема, нова громадська група з Території затоки, *Tech Solidarity*, виявила деяких демократів-неофітів. І незабаром він напише програму, яка допоможе справити вплив на ймовірних виборців-демократів у «Фейсбук» так само, як Трамп цілив у республіканців. Але грати роль хазяїна вечірки було трохи лячно для такого інтроверта, як він. Тому Адам запросив одного з найвідоміших протеже «Культу мертвої корови» приєднатися до нього. Це був Алекс Стеймос — директор з інформаційної безпеки у «Фейсбук». Онук греко-кіпрських іммігрантів, які оселилися в Сакраменто, Стеймос пройшов шлях, подібний до Адама: державні безкоштовні школи, серйозна вища технічна освіта, робота хакером із принципами. Перша була в групі *@stake*, на Маджа та інших членів *L0pht*, які 1998 року вразили його свідченнями в Конгресі під своїми хакерськими ніками про катастрофічний стан кібербезпеки.

Ідучи слідами *cDc*, Стеймос здобув репутацію незалежної людини. Коли Едвард Сноуден злив документи, які показували, що АНБ співпрацювало з великими інтернет-компаніями, особливо з метою збору даних про людей в інших країнах, Стеймос виступив з щирою промовою щодо етики[5] на

найбільшій конференції хакерів, *Def Con*. Він оголосив, що, попри брак широко запроваджуваних кодексів етики, експертам з безпеки краще обміркувати своє звільнення, ніж порушити права людини. За його різкість компанія Yahoo найняла Стеймоса директором з інформаційної безпеки, що було частиною загальної публічної відповіді гігантів Кремнієвої долини на викриття співучасті. Він залишався на цій посаді до 2015 року, коли без шуму пішов через таємне сканування компанією електронних листів користувачів за секретним наказом суду. Відтоді він обійняв посаду вищого керівника з інформаційної безпеки у «Фейсбук», намагаючись обмежити шкоду, яку російські хакери завдали розповсюдженням зламаних імейлів демократів, та беручи участь в інших бійках з пропагандою, незважаючи на слабку підтримку згори.

Окремо від своєї роботи у «Фейсбук» Стеймос долучився до виборчої політики. Працюючи в *Yahoo*, він інформував Конгрес із питань безпеки і був вражений деякими представниками та розчарований іншими. Усвідомлюючи, що його посада у великій компанії надає йому особливий доступ, він скористався цим, а також особистими пожертвуваннями кандидатам з обох партій, зокрема й республіканцю Віллу Герду, щоб просувати питання, які його хвилювали. У його законодавчому списку бажань було об'єднання сил захисту кібербезпеки США в одній організації замість купи агентств, які здебільшого присвячували свою роботу атакам. Також він хотів реформувати судове переслідування за хакінг, яке наразі визначалося Законом про комп'ютерне шахрайство та зловживання, і заборонити вбудовані урядові бекдори для шпигунства в технологічних продуктах, які, на думку Стеймоса, завдадуть шкоди американським компаніям, коли від

них відвернуться інші країни. І, як колишній радник Білого дому з питань кібербезпеки Річард Кларк, він хотів надійнішого процесу ухвалення рішень щодо того, які вади програмного забезпечення приховати для нападу, а які розкрити для захисту. У «Фейсбук» Стеймос тихо допомагав розслідуванню спецпрокурора Роберта Мюллера щодо російського втручання у вибори 2016 року.

Адам бачив, що Стеймос захоче підтримати сьогоднішнього кандидата через його технологічну філософію та потенційне значення політичних перегонів для майбутнього країни. Були й глибші причини, зокрема нагода сплатити своєрідну космічну покуту Кремнієвої долини. Кандидатом був Бето О'Рурк, демократ, який сподівався пройти праймериз та в листопаді поборотися з республіканцем Тедом Крузом за місце сенатора від Техасу. Круз був серйозним фаворитом порівняно будь з ким. З 1994 року жоден демократ не переміг на техаських виборах, і Круз був одним із найбільш відомих і найкраще фінансованих членів Сенату, республіканцем номер два, коли Трамп виграв національні праймериз 2016 року. Але ім'я Круза також мало особливий резонанс для всіх, хто добре знав про Фейсбук і розслідування Мюллера, або і про те і про те, як Стеймос. Якось Круз був головним політичним клієнтом компанії *Cambridge Analytica*, яка викрала персональні дані 87 мільйонів користувачів Фейсбук (які про це й гадки не мали), коли навчала Круза, а потім Трампа, як цілеспрямовано впливати ефективною рекламою.
З повної виборчої картини було зрозуміло, що республіканці утримували в Сенаті хитку більшість і перекидання лише двох місць дозволило б демократам заблокувати автоматичне схвалення кандидатів

Верховного суду й уряду Трампа та за потреби захистити розслідування Мюллера.

Не тільки тим, хто не зміг проконтролювати бездумні алгоритми у Фейсбуку, Твіттері та Ютубі, було про що шкодувати після виборів 2016 року. «Культу мертвої корови» теж належало виправляти помилки. Він обернув творчі здібності й опозиційні панівному класу витівки хакерського світу проти популярних медіа, створюючи сум'яття на національному телебаченні та в друкованих виданнях заради розваги та привернення уваги до різноманітних тем. Підрозділ *cDc* під назвою *Ninja Strike Force*, створений з чистими намірами, але пізніше залишений без нагляду, деградував і нещодавно прийняв до себе провокаторів-расистів, які запозичили методи *cDc*, але не його погляди. Кілька нових членів підняли хейт у соціальних мережах і дали «зелену вулицю» технічному спеціалісту, автору найбільших неонацистських дописів, які активно підтримували Трампа.

Обмінявшись кількома словами з Адамом і Стеймосом, О'Рурк почав промову перед гостями. Він керував невеликою компанією, що розроблювала софт й альтернативні видання, далі у статусі непопулярного кандидата виграв вибори за місце в міській раді, відтак у Конгресі, де служив свій третій й останній дворічний термін. Стрункий і високий, вбраний у сорочку з відкритим комірцем і синій костюм, він пояснював, що вирішив балотуватися у вечір, коли Трампа обрали президентом. Він і його дружина Емі намагалися вирішити, що вранці сказати трьом своїм дітям і що вони скажуть їм у наступні роки. «Що ми зробили? Як ми пояснили свої дії?» — пригадував О'Рурк ту розмову. Він

мав залишити посаду члена Палати представників, щоб балотуватись у Сенат, але О'Рурк вирішив, що варто ризикнути. Він відвідував кожен округ Техасу, його кампанія набирала обертів, і він думав, що має шанс. Освіта, доступ до медичних послуг і робочі місця були більш важливі, сказав він, ніж блакитне чи червоне[3], і готовність виборців призначити когось, хто «підірве систему», як Трамп, можна приборкати. Найбільшою проблемою було переконати людей прийти на виборчі дільниці.

Допомогло, сказав О'Рурк, що техасці ненавидять ошуканців, тому не приховував: він проти запланованої Трампом прикордонної стіни, вважає, що Трампа слід піддати імпічменту, та підтримує права на аборт, легалізацію марихуани та контроль над зброєю, як і більшість технологічних працівників Території затоки Сан-Франциско. Він уже боровся в Палаті представників за скасування рішення Федеральної комісії зі зв'язку та відновлення мережевого нейтралітету, який не дозволяє інтернет-провайдерам надавати певному контенту перевагу над іншим. О'Рурку не потрібно було порівнювати свою відвертість із гнучкістю Круза. Всі присутні знали, що нинішній сенатор від Техасу відмовився підтримати кандидата Трампа після того, як той відпустив шпигачки щодо зовнішності дружини Круза та припустив, що його батько був причетний до вбивства Джона Ф. Кеннеді. «Ми просто прийняли відповідальність за все, чим ми є та у що віримо»,— сказав О'Рурк. Відмова від грошей з комітетів політичних дій була неприємною, але захід Адама та Стеймоса допоміг. Кілька гостей, які відвідали його, також організували власні вечірки для збору коштів. У Бостоні

вірний послідовник *cDc*, Сем Ентоні, доктор наук з Гарварду, який працював над покращенням безпечності безпілотних автомобілів, улаштував для О'Рурка фінансовий захід, який так само надихнув подальші пожертвування на Східному узбережжі.

Хоча багато інших теж прагнули допомогти О'Рурку, коли він посилив свою позицію, виграв праймериз 2018 року та отримав майже однакові з Крузом результати на виборах, рання підтримка у Сан-Франциско та Бостоні прийшлася до речі. У тих двох містах мешкала більшість членів *cDc*. І так склалося, що група почала свою діяльність у рідному штаті О'Рурка — Техасі.

Розділ 2.
ТЕХАСЬКІ Т-ФАЙЛИ

Як і багато найперших послідовників інтернету[1], Кевін Вілер з ентузіазмом намагався опанувати новий і незграбний спосіб комунікації через глибоку потребу в спілкуванні. Захоплений комп'ютерами син університетського адміністратора та вчительки музики чудово проводив час із друзями зі схожими інтересами в Кенті, Огайо, граючи в *Dungeons & Dragons*. Але потім, 1983 року, родина переїхала в Лаббок, Техас, і тринадцятирічна дитина зазнала культурного шоку.

Немов мало бути підлітком-бунтівником у самому серці рейганівської республіканської ери. Тепер, у новій неповній середній школі, Кевін загубився серед культурно консервативних християн-євангелістів, чиїм уявленням про бунтарство був міський герой Бадді Голлі{4}. Кевін спробував поспілкуватися з дітьми багатіїв, але вони були бундючними й непривітними. Тоді він пішов до бідних дітей, і вони шокували його оповідками про секс і наркотики. Але дозволили йому сидіти з ними, тож він залишився.

Кілька дітей, чиї батьки працювали на великому техаському інструментальному заводі, теж цікавилися технологіями. Інші почали замислюватися, що може статися з комп'ютерами, після перегляду фільму «Воєнні ігри», який вийшов того ж року, коли Кевін приїхав у місто. У фільмі підліток, якого зіграв Метью Бродерік,

довільним чином набирав номери, використовуючи громіздкий пристрій під назвою «модем», що був підключений між його комп'ютером і домашньою телефонною лінією. Герой Бродеріка випадково проник у воєнний суперкомп'ютер. Хакери-початківці Лаббока не шукали собі неприємностей. Кілька старших дітей створили електронні форуми, відомі як електронні дошки, на яких відвідувачі, використовуючи модеми для дзвінків на звичайні телефонні лінії, могли читати або залишати повідомлення й текстові файли. Місцеві називали їх т-файлами. До повсюдного використання веббраузерів залишався ще десяток років.

Кевін уже два роки користувався *Apple II*, до переїзду в Лаббок, тому дуже швидко відшукав місцеві електронні дошки. За його районним кодом 806 їх було небагато, і більшістю керували любителі, які обговорювали комп'ютерні теми. У деяких підлітків були дошки, що пропонували більше свободи, і Кевін з друзями деякий час там теревенили, поки старші діти не втомилися від непроханих гостей і позбавили їх доступу. Кевін був обурений. «Ми маємо зробити власні дошки й по-справжньому бути елітою»[2],— заявив він друзям. Він та інші створили кілька дощок і наповнили їх текстовими файлами про хеві-метал, пародії на «Зоряні війни» та інші теми поп-культури, а також сатирою на операторів серйозніших електронних дощок і пихатих хакерів. Дошки мали перехресні посилання на заголовки та телефонні номери одна одної і групувалися під назвою *Pan-Galactic Entropy*.

Відвідування цікавих електронних дощок поза своїм районним кодом означало чималенькі рахунки за міжміське користування домашнім телефоном. Усім, хто

не мав багатих і схильних пробачати батьків, була потрібна чиясь кредитна картка, або п'ятизначний код від компанії міжміського зв'язку, як-от *MCI*, або деякі справжні хакерські здібності. Найлегше було здобути п'ятизначний код, який могли зламати вручну серією спроб і помилок ті, хто дійсно був цим захоплений. Цифри-переможці розповсюджувалися немов гарячі плітки у шкільній їдальні та в дописах електронних дощок уночі. Вони працювали, доки не з'являлося забагато користувачів і *MCI* не помічала це та не відкликала номер. Зазвичай це забирало місяць. Потім ентузіасти відшукували та поширювали новий код.

Якщо ви приділяли цьому достатньо часу, то могли знайти електронну дошку на свій смак і з саме тим типом контенту, що вам подобався. Більшість дощок надавали змогу завантажувати матеріали та копіювати їх на власну дошку, якщо у вас був досить швидкий модем чи ви могли залишити його працювати на всю ніч, аби видобути великий файл,— за умови, що нікому не було потрібно зробити звичайний дзвінок. Здавалося, батьків Кевіна не турбує, що він захоплює телефонну лінію та допізна не лягає спати, завантажуючи файли.

Як і більшість однолітків, Кевін полював на нові програми для свого *Apple II*, що означало обмін зламаними версіями, у яких видалено засоби обмеження користування. Але читання та невдовзі написання текстових файлів було тим, що цікавило Кевіна найбільше. Для нього це був спосіб творчого самовираження, і він мав аудиторію. Він хотів зробити свої текстові файли кумедними чи принаймні провокаційними, щоб можна було підключатися до комп'ютерів інших дітей, які розуміли ті самі жарти. Після

того як робота в комп'ютерному магазині влітку 1985 року принесла достатньо грошей, щоб купити жорсткий диск за 715 доларів, Кевін запустив власну електронну дошку, *Demon Roach Underground*. Одним з її перших файлів була абсурдна імпровізація в усталеному жанрі «підривних» файлів, схожа на надруковані у «Куховарській книзі анархіста», з інструкціями виготовлення небезпечних і незаконних предметів.

Ідеєю Кевіна була «Бомба з корму для піщанок»[3]. Вона містила покрокові інструкції та радила читачам подрібнити гранули корму, покласти їх у скляну банку та витрусити. Потім слід налити в банку бензин, запалити ґніт і з криками втекти. Це був поширений юнацький гумор. Але хоча він кепкував з анархістських кредо, він підіймав на глум і поліцію, яка б відповіла на вибух фразою «Поліцейські — ваші друзі!». Й у файлі розповідалося, як весело вдарити пакет корму битою та вдати, що це республіканська перша леді Ненсі Рейган, авторка кампанії боротьби з наркотиками «Просто скажи "Ні"». Сам Кевін узагалі не цікавився наркотиками чи навіть пивом, але це не означало, що Рейгани не заслуговували висміювань.

Онлайн усім був потрібен нік. Кевін обрав Swamp Rat, тому що любив гратися біля болота поруч зі своїм домом. Невдовзі нік перетворився на вишуканіше Swamp Ratte і зрештою на Grandmaster Ratte. Один з його найперших онлайн-помічників узяв собі прізвисько Сід Вішез на честь найбільш патетичного наркозалежного члена однієї з перших панк-груп *Sex Pistols*. У реальності Сід був восьмикласником на ім'я Брендон Брюер, який жив у сусідньому місті Френдшип.

На відміну від блідого та відлюдного Кевіна Брендон займався спортом. Він і його старший брат Тай з ніком Graphic Violence вели електронну дошку KGB — за назвою радянської спецслужби. Серед іншого, вона містила справжні інструкції з виготовлення бомби. Однак ведення дошки допомагало братам уникати пияцтва та халеп на вулицях. Пізніше Кевін розповів другу, що на дошці *KGB* були «схибнуті речі про секс і насильство[4] та дещо про фрикінг *MCI*», маючи на увазі телефонний еквівалент комп'ютерного хакінгу.

Брендон мав більше технологічних амбіцій, ніж Кевін. Він нишпорив у сміттєвих контейнерах за офісами великих компаній, шукаючи будь-що, що допомогло б йому проникнути туди. І він користувався «блакитними коробочками» — головними пристроями для фрикінгу. Вони видавали потрібні тони на телефонних лініях, видурюючи безоплатні міжміські дзвінки. Улюбленою грою Брендона було продовжувати передавати дзвінки зі станції на станцію в одному напрямку, роблячи коло планетою, аж поки не дзвенів другий телефон у його ж домі. Такі телефонні трюки досі були легшими, ніж програмування, хоча насувалися великі зміни. Коли брати Брюери отримували нові програми для свого комп'ютера, їх досі було потрібно вводити вручну. Один диктував рядок коду, інший друкував. Коли в зайнятого друком починали боліти пальці, вони мінялися місцями.

Брендон і Кевін не хотіли справляти грізне враження серйозних хакерів — таких, які можуть потрапити за ґрати. «У нашому колі[5] не було нічого зловмисного; туди ніколи не приходили з наміром завдати шкоди чиїйсь системі,— сказав Брендон.— Суть була в тому,

щоб пробитися крізь стіну». Втім, вони хотіли, щоб їх сприймали серйозно. І назва «Пангалактична ентропія» створювала недостатньо лячне враження. Вона була надто нудною, у стилі «Путівника по Галактиці для космотуристів». Хлопці покрутили в голові можливі нові назви, пробуючи зібрати докупи свою маленьку спільноту електронних дощок і написання текстів, і вирішили, що щось зі словом культ звучатиме досить лиховісно й таємниче. Культ чого? Деякі слова, як-от полуниця, були надто безглуздими. Але було б непогано вигадати щось трохи безглузде. «Ми хотіли, щоб назва була чудернацькою,— поділився Брендон.— Просто намагалися поглузувати з істеблішменту». Це місце було схоже на клуб, відділ вільних мистецтв у хакерському андеграунді. Кевін подумав про моторошне місце зустрічей неподалік — покинуту бійню, неприємні залаштунки найбільш канонічної галузі техаської економіки. Тоді він додумався: «Культ мертвої корови».

Хоча Брендон і допоміг з назвою групи та поділився своєю хакерською майстерністю, остання невдовзі завдала йому неприємностей. Причиною став телефонний фрикінг. Друг Брюерів доглядав за чиїмось домом, знайшов абонентську картку *MCI*, записав її номер і повідомив його братам. Вони підключилися до інших електронних дощок і запропонували читачам завітати на їхню дошку. Після того як на рахунку власника картки з'явилося забагато незрозумілих витрат, він викликав поліцію, яка відвідала друга, а той назвав імена. Незабаром у вітальні Брюерів сиділи чоловіки в костюмах. Тридцять з чимось років по тому Брендон сказав, що не пам'ятає, що саме сталося далі. Можливо, ті люди забрали комп'ютер як доказ. Можливо, батько жбурнув його у сміття. Так чи інакше, це був кінець Сіда

Вішеза. Брендон Брюер пішов у старші класи та відкрив для себе нове захоплення — дівчат.

Він покинув групу навіть до зустрічі з хлопчиком, якого Кевін вважає третім засновником «Культу мертвої корови». Він мав нік Franken Gibe і часто відвідував ті самі дошки, що й Кевін. Насправді його звали Білл Браун. Навесні 1986 року Білл набрав номер *Demon Roach Underground*. Дошка не відкрилася, тому що Кевін працював над софтом, щоб вона краще функціонувала чи мала дивніший вигляд. Витріщаючись на порожній екран з діалоговим вікном, Franken Gibe надрукував «привіт» і відправив повідомлення. «Ти хто?» — з'явилося в наступному рядку. Білл сподівався, що спілкується напряму з системним оператором, або сисопом. Йому пощастило: це був Кевін. Вони трохи побалакали. Врешті-решт вони з'ясували, що мешкають лише за кілька кварталів один від одного, і зустрілися.

Білл більше цікавився альтернативною культурою,— НЛО, таємними спільнотами та малобюджетними фільмами,— ніж написанням комп'ютерного коду. Після виходу «Воєнних ігор» йому довелося благати про комп'ютер своїх нетямущих батьків, які не мали навіть телефонного автовідповідача аж до кінця 1990-х. «Я нічого не знав про комп'ютери,— пригадував він,— але мені була до вподоби ідея електронної дошки, цієї прославленої доінтернетівської мережі». Обидва хлопчики були в Лаббоку аутсайдерами з точки зору культурних вподобань і на ранній інтернет-сцені, яка прославляла хакерські трюки. Вони були наче ранні панк-рок-гурти, які не збиралися тихо сидіти тільки тому, що не вміли добре грати.

Уникаючи призначеної йому роботи в католицькій школі, Білл допоміг міфологізувати «Культ мертвої корови» в псевдорелігійних рядках, склавши епічну «Книгу Корови»[6], свій перший текстовий файл. Це була безглузда та пафосна пародія обсягом 1100 слів на обидва заповіти Біблії. «Прогурчав звір, і все було жуйкою та міазмами тварини. Це був початок. І від Моменту Корови пішло все, що ми називаємо світом»,— виголошував текст на початку. Наприкінці було: «Культ квітнув у ті безплідні часи, і здібні розуми пожинали плоди справедливості та правди. Культ вийняв з піхов осяйний меч знання й у битву вирушив, прекрасний у сліпучих шатах ідеалів».

Пізніше Білл розмірковував над тим, що ввійшов у хакерський світ у ролі своєрідного королівського блазня. «Я сприймав свою дурість дуже серйозно[7] і дражнив деспотичну ієрархію Освіченої Аристократії,— писав він.— До cDc існувала еліта та лузери. Це була проста, феодальна, незріла система класової дискримінації на основі зв'язків (переважно) чи досвіду у мистецтві х/ф [хакінгу/фрикінгу]... *cDc* була по-справжньому визвольною силою». Згодом Кевін і Білл вирішили, що суттю групи не може бути тільки нісенітний гумор і химерні повчання, що їй потрібна деяка хакерська репутація. І так склалося, що помітно не зацікавлений у технологіях Білл пішов у бібліотеку Технічного університету, проштудіював книжку з операційних систем Unix й оприлюднив гідний перелік програмованих команд[8], які потім циркулювали онлайн роками.

Більшість файлів тоді були шпаргалками з комп'ютерних мов або інструкціями, які навчали читачів, як і де підключитися, часто безоплатно. Але далі вони нікуди не йшли. Білл просував етику *cDc* під гаслом «Телекомунікаційні технології як засіб, а не кінцева мета»[9]. Гумор дітей клав край будь-якій зарозумілості в групі та зробив її доступною. *cDc* потроху поглинала інші дошки та встановлювала зв'язок з новими віддаленими. Серед їхніх власників був підліток з Ель Пасо з ніком Psychedelic Warlord і хтось у Мічигані на прізвисько G. A. Ellsworth, чиє справжнє ім'я було Метт Келлі. Обидва додали власні текстові файли до «флагманського корабля» і були прийняті в члени. Оприлюднені з 1987 до 1990 року, вісім т-файлів *cDc*, які написав Psychedelic Warlord, містили тексти пісень смішного панк-гурту *The Dead Milkmen*. У файлах була фантазія про видіння, які підбурювали оповідача до вбивств: «Більше не можу придушувати це сильне бажання у моїй голові. Визнай цей факт: моєю єдиною метою в житті стало вбивство всього вільного й сповненого любові»[10]. Перший *cDc*-файл, розміщений Psychedelic Warlord (у рік, коли йому виповнилося п'ятнадцять)[11], просив читачів уявити кращий світ, чи принаймні кращу країну, без грошей. Після ненасильницького усунення уряду він бачив кінець голоду та класових відмінностей.

У ще одному файлі, оприлюдненому наступного року, був текст інтерв'ю зі самопроголошеним неонацистом[12], який стверджував, що Гітлера

неправильно зрозуміли й насправді він не хотів винищення євреїв. Psychedelic Warlord і його друг-єврей взяли під сумнів теорії чоловіка та дозволили йому верзти дурниці. Після інтерв'ю Warlord написав: «Ми намагалися збагнути, що наштовхнуло його на такі жахливі думки». Він додав, що виступає проти цензури, тому якщо люди хочуть дізнатися більше про того чоловіка та його арійську церкву, можуть написати листа на його поштову скриньку в Ель Пасо. Він сподівався, що читачі завалять її повідомленнями чи контраргументами або просто поконфліктують з хлопцем. «Їм точно сподобалася б фанатська пошта», — написав він.

Хоча його родина жила з комфортом і, як вважалося, мала високий статус, Psychedelic Warlord почувався маргіналом. Він теж зловживав телефонними картками та завантажував піратські ігри. «Коли тато купив *Apple II* та модем на 300 бод, я почав відвідувати електронні дошки, то був Фейсбук тих часів,— казав він.— Ти просто хотів бути частиною спільноти».

Завербовуючи лідерів інших дощок, *cDc* почала діяти немов супергрупа, якою вона стане десятиліттям пізніше. Але в ті прості дні кінця 1980-х головними критеріями членства в *cDc* було таке: (1) бути знайомим з чинним членом групи, (2) не бути нудним і (3) не бути засранцем. Дівчина з ніком Lady Carolin, насправді на ім'я Керолін (Керрі) Кемпбелл, познайомилася з Psychedelic Warlord на його дошці та приєдналася до *cDc*, коли їй було п'ятнадцять. Це зробило групу однією з небагатьох, у складі яких були жінки. Obscure Images, артистичний підліток Пол Леонард з чиказької агломерації, регулярно відвідував дошку Метта, *Pure*

Nihilism, до того як стати ще одним основним членом cDc.

Пізніше Пол сказав про себе: «Я доволі типова, дещо дурна, примхлива, відлюдна та відчужена дитина». Пол вештався дошками, які спеціалізувалися на обміні піратським софтом, і товаришував з однією з зірок цієї сцени, поки той молодий чоловік не став першим, кого засудили за Законом про комп'ютерне шахрайство та зловживання 1986 року. Після цього Пол шукав чогось веселішого та більш законного. «До кінця 1990-х члени *cDc* цікавилися переважно написанням текстів, музикою, мистецтвом тощо,— казав Пол.— Технічні питання були другорядними». Він з ентузіазмом прийняв культуру публікування «зроби сам», яка перетиналася з музикою та журналами на кшталт *Boing Boing*, що змінив паперову форму на електронну та є одним із небагатьох, які існують відтоді до сьогодні. Як художник-графік, Пол оцінив та поліпшив ілюстративні матеріали cDc, створені з текстових символів, які були максимумом, що могли дозволити модеми того часу. Стилізоване під дитячий малюнок зображення мертвої корови з X для очей залишалося емблемою cDc ще довго після того, як члени отримали можливість надсилати відеокліпи з високою роздільною здатністю.

Керрі Кемпбелл докладала багато зусиль, щоб згуртувати членів групи. Коли Psychedelic Warlord у телефонному дзвінку переконався, що Lady Carolin — з тих рідкісних людей з жіночими ніками, які дійсно жінки, він і пізніше решта групи *cDc* прийняли її та ставилися до неї з повагою. Керрі вела електронну дошку в Сан-Дієго і, так само як інші, займалася фрикінгом просто для спілкування. А ще вона писала старомодні листи

Psychedelic Warlord і деяким іншим. Вона ніколи не називала себе хакером, але була розумною, доброю та завжди знала, коли в кого день народження.

За винятком засновників у Лаббоку, до 1990 року члени *cDc* зрідка зустрічалися особисто. Хоча їхні різноманітні дошки розміщували офіційні файли *cDc*, вони спілкувалися між собою у таємній частині *Demon Roach Underground*. Навіть Білл зрідка з'являвся особисто, тому що поїхав вчитись у школі закритого типу, а потім у коледжі на півдні Каліфорнії. Psychedelic Warlord закінчив приватну школу на Східному узбережжі. Не маючи там комп'ютера, він передав Метту Келлі свою дошку, *Tacoland*. Улітку 1992 року Метт відвідав Лаббок. Він і Білл поїхали в Сан-Франциско окремими машинами, спілкуючись через рацію. Опинившись в Ель Пасо, вони поїхали за адресою Psychedelic Warlord, щоб здивувати його. Квартали мали дедалі вишуканіший вигляд, і врешті-решт хлопці зупинилися перед величним особняком. Коли економка відчинила двері, хлопці спантеличено перезирнулися. Psychedelic Warlord ніколи не згадував, що його батько — бізнесмен зі зв'язками та колишній представник округу. «Я припускав, що він з середнього класу, як і всі ми»,— казав Метт. Їм не довелося турбуватися про своє втрачене самовладання, оскільки виявилося, що того дня їхнього друга не було вдома.

Кількох членів групи об'єднувала музика, особливо музика андеграунду. Psychedelic Warlord грав у кількох маленьких гуртах, а Кевін робив демозаписи для амбітних музикантів і став невіддільною частиною музичного світу Лаббока. Метт у Мічигані теж дуже любив альтернативну музику, яка зробила дошки Кевіна

та Psychedelic Warlord особливо привабливими: «У вісімдесяті було важко знайти інформацію про все, що виходило за рамки панівного напряму». Метт узяв участь в інтерв'ю з пост-панк-гуртами *Mudhoney* і *Big Black*, які очолював майбутній продюсер гурту *Nirvana* Стів Альбіні. Він узявся створювати маленьку звукозаписну студію та публікувати музику й культурний журнал *Cool Beans*, який отримав свою назву від одного з висловів Кевіна.

Кевін залишився там, де був, відвідуючи Техаський технологічний університет та працюючи діджеєм на його радіостанції. Він обожнював метал, панк і реп, але був вимушений використовувати плейлисти, надані - керівництвом. Тому він підробляв запити фанатів на пісні, щоб вмикати те, що хотів. Він і сам грав у багатьох гуртах, і 1995 року поїхав з Біллом та власником місцевого магазину скейтбордів на майданчик живої музики *Motor 308*. До переїзду до Нью-Йорку 1999 року він змінить п'ять місць.

Ще навчаючись у коледжі, Кевін відвідав курси з медіа та реклами. Це допомогло йому скласти серйозну стратегію експансії *cDc*. Природжений «хайпмен», як він себе називав, Кевін збере близько десяти нових текстових файлів і надішле їх в інші електронні дошки. Сама нумерація файлів була блискучою ідеєю. Оператори електронних дощок по всій країні знали, чи бракує в них чогось, і багато хто спеціально приділяв час, щоб зібрати повний комплект.

Золоте десятиліття текстових файлів тривало з 1985 до 1995 року, коли компанія *America Online* та веббраузер *Netscape* зробили незграбні дзвінки на електронні дошки

непотрібними. Стратегія Кевіна, бачення Білла й еклектичні таланти інших, що приєдналися до них, зробили «Культ мертвої корови» найвідомішим і найпопулярнішим взірцем мистецтва написання т-файлів.

[x x]

Кевін хотів навчитися і в попереднього покоління хакерів. Головною ранньою знахідкою був Кріс Такер, який дзвонив з дошки в Род-Айленді[13] під ніком Nightstalker і став другою людиною поза Техасом, яку запросили приєднатися до «Культу мертвої корови». Кріс поїхав у В'єтнам як підрядник ЦРУ під час війни та повернувся з похмурими поглядами щодо уряду. 1971 року дорогою додому він прочитав у журналі *Esquire* проривну статтю Рона Розенбаума «Секрети маленької блакитної коробочки». Розенбаум провів багато часу з телефонними фрикерами, попередниками сучасних хакерів, і пояснив простою мовою, що вони роблять. Фрикери були різноманітною групою. Серед них виділявся Джон Дрейпер, який називав себе «Капітан Кранч» відтоді, як дізнався, що свистки з пачок цих сухих сніданків можуть видавати звук частотою 2600 герц, що надавало змогу робити безоплатні дзвінки. Технічні загадки фрикінгу привернуть увагу майбутніх інноваторів, зокрема засновників Apple Стіва Джобса і Стіва Возняка — вони продавали «блакитні коробочки» для безоплатних дзвінків, коли навчалися в коледжі.

Політичний розкол в Америці наприкінці 1960-х був найгіршим до 2000-х, і це підштовхнуло фрикінг у радикальному напрямку. Телефонні компанії цілком

певно були частиною істеблішменту, а *AT&T* — ще й монополістом. Це робило її ідеальною мішенню для супротивників війни та всіх, хто вважав, що красти в деяких компаній етичніше, ніж в інших. У червні 1971 року їппі{5} Еббі Гоффман та фрикер Al Bell — знайомий Гоффмана та колишній студент-інженер Алан Фірштейн — оприлюднили перший інформаційний бюлетень Міжнародної молодіжної партії *(Youth International Party Line)*[14]. Він починався з перелічення таємних кодів телефонних карток і перейшов до публікації відвертих інструкцій з виготовлення «блакитних коробочок» й інших штучок для безоплатних дзвінків. Втомившись від витівок Гоффмана, автори перейменували видання у *TAP (Technological American Party)* і продовжили по максимуму користуватися положеннями Білля про права щодо свободи преси. *TAP* видавали до 1984-го, того самого року, коли почав виходити друком важливий хакерський журнал «2600».

Кріс здобув свою першу «блакитну коробочку» в січні 1972 року, майже за десять років до знайомства з Кевіном. Він познайомився з ще одним молодим ветераном, Робертом Осбандом, на науково-популярній конференції в Бостоні на початку 1970-х, і двоє чоловіків заприятелювали на ґрунті політично забарвлених історій. Більш відомий як Cheshire Catalyst, Осбанд був радіоаматором, фрикером і давнім редактором *TAP*. У нью-йоркських офісах TAP саме Осбанд запропонував проводити регулярні збори в першу п’ятницю кожного місяця — традицію, яку пізніше продовжить журнал *«2600»* у багатьох містах. «Ми завжди прагнули ділитися знаннями,— розповідав Осбанд.— Ділитися знаннями та допомагати людям створювати речі».

У Лаббоку Кевін уважно читав фотокопії випусків *TAP*. Тепер завдяки Крісу він знав декого, хто був частиною цього. Кріс розповідав історії та терпляче відповідав на всі запитання Кевіна. Він розпочав комп'ютерний хакінг у 1975-му, задовго до того, як *TAP* почав розглядати цю тему, й обожнював збирати та налагоджувати старі комп'ютери і допомагати початківцям. Кріс намагався вплинути на всіх, хто прислухався би до поради застосовувати суворе шифрування та інші інструменти приватності, коли їх розробили, та оприлюднював у *cDc* суто політичні файли проти рейганівських консерваторів. Він вітав нерегульований інтернет не тільки як чудову річ, а також як те, що потребує активного захисту в політичній царині. Вважаючи лібертаріанство, популярне серед багатьох технічних спеціалістів, «бездонною ямою», у файлі *cDc* «Політична проповідь № 1»[15] Кріс написав: «Комп'ютерний андеграунд, колись створений з людей, зацікавлених тільки в безоплатному софті, безоплатних дзвінках і критиці "заліза" одне одного, тепер стикається з потребою подумати про політику та стратегії. Вони мають узяти участь у політичному процесі та, можливо, вийти й проголосувати, чорт забирай!»

Кевін хотів навчитися максимуму з минулого, щоб прокласти подальший шлях. Але найкращий спосіб зробити це — зустрітися з іншими хакерами, а він був у Лаббоку, далеко від усіх.

Розділ 3. КОНФЕРЕНЦІЇ

Для Кевіна й інших членів *cDc* 1990-ті почалися набагато краще, ніж 1980-ті. 1989 року розвалилася Берлінська стіна, Джордж Г. В. Буш був не таким поганим, як вони боялися, і незабаром Білл Клінтон, якого вони вважали розсудливим південним демократом, стане хазяїном Білого дому. Комп'ютерні технології досі були загадковими, але все більше входили у вжиток, наближаючи людей до знань.

Група молодих хакерів у Техасі справляла враження напрочуд сильної. Крім мистецького флангу хакерської спільноти, представниками якого були найперші члени «Культу мертвої корови», було багато інших ентузіастів, які керували скромними електронними дошками заради коментарів, створення спільноти та, у деяких випадках, конспірації. На темнішому краю спектра були ті, хто спеціалізувався на піратських програмах і кредитних картках, а також порадах з проникнення в комп'ютери телефонних компаній, корпорацій та урядових агентств. Але Техас — велика територія, і там хакерам було важче зібратися, ніж групам у Нью-Йорку, Бостоні чи Сан-Франциско. Це заважало їм проводити час разом так само, як це робили їхні колеги в інших місцях, що означало менше веселощів, довіри, тісної співпраці та розвитку.

1990 року хакер з Г'юстону Джессі Драйден[1] вирішив змінити це. Власник хакерських дощок, зокрема *K0de Ab0de*, і на той час два роки як член *cDc*, Драйден був унікальною людиною: гіперінтелектуальною та захопленою музикою, як деякі інші, але з сильною особистістю і в житті, і за комп'ютерною клавіатурою. Пристрасть Драйдена до музики виникла в найприродніший спосіб: його батько Спенсер Драйден був ударником гурту *Jefferson Airplane*. Він об'єднався зі співачкою та своєю романтичною партнеркою Грейс Слік і відігравав значну роль у художніх смаках гурту. Мати Джессі, Саллі Манн, у 1960-ті втекла в Лос-Анджелес, а потім у Сан-Франциско. Манн була дотепною, смішною та настільки шалено вродливою, що могла немов чарами пробитися крізь будь-яку перешкоду, що стояла між нею та рок-зіркою, з якою вона хотіла зустрітися. Її фотографію використали в статті *Rolling Stone* про групі{6}, але вона була деким набагато більшим. Вона стала найближчою подругою Слік, ухопилася за старшого Драйдена, коли він розійшовся з Грейс, і 1971 року народила Джессі Джеймса Драйдена.

Хоча *Jefferson Airplane* зажив власної слави, він ще й був партнером гурту *Grateful Dead*, центру контркультури епохи на Території затоки. Гітарист *Grateful Dead* Джеррі Гарсія особисто схвалив приєднання Драйдена до *Jefferson Airplane*, і члени обох гуртів та їхні спільні друзі мешкали разом у Гейт-Ешбері та інших районах Сан-Франциско. Разом зі спільною творчою роботою та опозиційним ставленням до істеблішменту той тісний союз означав експериментальну соціальну структуру, раннє прийняття технологій і, як висловилася Манн, «краще життя

завдяки хімії»[2]. Ще до того, як *Grateful Dead* отримав свою назву, його учасники належали до «Веселих Бешкетників» Кена Кізі, еклектичного та ідейного гурту, який подорожував Америкою, щоб каверзувати та розповсюджувати «гарні новини» про ЛСД.

Ще один Бешкетник, письменник-візіонер і маркетер Стюарт Бренд, теж допоможе поширити новини про прийдешню еру комп'ютерних технологій. У доробку Бренда був екологічно-орієнтований журнал *Whole Earth Catalog* і *The WELL* — одна з перших онлайн-спільнот Західного узбережжя. Серед друзів Манн був автор текстів *Grateful Dead* і майбутній завсідник *The WELL* Джон Перрі Барлоу. У роки навчання у Весліанському коледжі він почав відвідувати гуру «кислоти» Тімоті Лірі та 1967 року познайомив з ним музикантів *Grateful Dead*. Пізніше він написав для них пісні, зокрема *Cassidy*, яку присвячено Нілу Кессіді — іконі бітників і ще одному Бешкетнику. Члени *Grateful Dead* відвідували «кислотні тести» Кізі й іноді виступали на цих вечірках, вони стали технологічними ентузіастами, заохочуючи запис живих виступів на плівку. Обмін тими плівками поглибив зв'язки *Grateful Dead* з фанатами та передвістив появу файлообмінних сервісів на кшталт *Napster*.

Своєрідний спадок Джессі добре підготував його до запровадження найбільшої інновації у *cDc* і хакерському світі: сучасної хакерської конференції. На думку Барлоу, це було однією з причин, з якої Джессі допоміг перетворити *cDc* на наступників «Веселих Бешкетників» у 1990-ті. Подібно до Бешкетників, група випромінювала ідеалістичну радість від висміювання істеблішменту й опису світу, який бурхливо розвивався на їхніх очах. Гумор — одна з величних речей, що об'єднують світ, -

казав Барлоу, і спільною рисою *cDc* і Бешкетників був гумор з метою поставити під сумнів легітимність влади. Проводячи аналогію з хакерами, Барлоу висловлювався так: «Особливість “кислотників” у тому, що вони вважають владу кумедною».

Хоча батьки багато в чому дали Джессі Драйдену приголомшливий старт,— інтелектуальний, соціальний і артистичний,— стабільність була цілком іншим питанням. Манн пішла від Драйдена та повернулася з Джессі до Техасу, але провела короткий час у тюрмі. У дванадцять років Джессі вмовив пустити його в гастрольний автобус метал-гурту Dokken і надовго зник. Потім він чотири місяці вдавав, що ходить до школи. Комп’ютер Джессі допоміг йому дати раду конфлікту між сором’язливістю та потребою у самовираженні. «Він набув деякої популярності та зміг скористатися нею, щоб з’являтися на публіці та спілкуватися з музичними гуртами»,— пригадувала Манн. Джессі часто відвідував рок-клуби та розвинув раннє підприємницьке чуття. Він привіз з Каліфорнії приладдя для скейтбордів і продавав його в місцевих парках, а потім — рідкісні відеоплівки концертів. Дещо з тих прагнень повернуло на лихе, і його звинуватили в хакінгу кредитних карток. За словами Манн: «З цього нічого не вийшло, але в Джессі відібрали дуже класний Mac».

Коли підліткові стосунки Джессі з матір’ю зіпсувалися, він подружився з менеджером місцевої музичної крамниці, Вінсом Гутьєрресом, і час від часу жив разом із ним і його дочкою. Він багато розповідав про «Культ мертвої корови» та познайомив друзів з Гутьєрресом під фальшивими іменами або їхніми онлайн-ніками.

Псевдонім самого Джессі утворився від його опису лос-анджелеського метал-гурту, який він охарактеризував як «п'яні засранці» *(drunk fucks)*. Поступово він став відомий як Drunkfux або dFx — ретельно стилізований нік, дотепний і незрозумілий чужинцям. «У нього проблеми з самооцінкою,— пояснював Гутьєррес.— Він не відчуває, що вписується в певний тип людей. Для нього *cDc* була чимось на кшталт *Jefferson Airplane*: ці хлопці були абсолютним андеграундом. Не у кримінальному сенсі, а в тому, що ти не знав, що це за світ, поки не став його частиною. Він складний, наче братерство».

[x x]

1990 року, коли Джессі було дев'ятнадцять, він стратегічно пробовкнувся[3] на дошках, що «перша щорічна» конференція XmasCon, незабаром відома під ліричнішою назвою *HoHoCon*, відбудеться протягом трьох днів на різдвяні вихідні у готелі *La Quinta Inn* біля аеропорту Г'юстона, де одномісні номери коштують 44 долари за ніч. Анонімне оголошення було стислим, але являло собою зразок стилю Джессі й тодішньої *cDc*. У тексті стверджувалося, що, поки один журналіст не виказав секрет, *XmasCon* планували як приватний захід. Попри це, повідомив Джессі, *XmasCon* буде відкритою для публіки. Попередня хакерська конференція *SummerCon*, що була приватною та сподобалася Джессі, відбувалась тричі протягом трьох років. Перші *SummerCon* організували у Сент-Луїсі редактори започаткованого 1985 року онлайн-журналу *Phrack*, чия назва поєднала слова *phreak* і *hack* у щось схоже на

лайку. Оголошення Джессі з'явилося у несанкціонованій переробленій копії *Phrack* у листопаді 1990 року.

«Ми плануємо влаштувати найбільші збори хакерів і федералів з часів *SummerCon-88*!»,— написав Джессі, запрошуючи «всіх хакерів, журналістів і федеральних агентів». Жарт полягав у тому, що хоча це перша хакерська конференція, на яку запросять федералів, вона не перша, на якій вони були присутні. На *SummerCon-88* учасники переважно випивали, вихвалялися та проводили час з людьми, з якими були знайомі онлайн. Але на заході того року шпигували агенти Секретної служби. Нічого зловмисного не виявили, але арешти все одно потяглися. Це була частина того, що 1990 року стане першою правоохоронною облавою на хакерів по всій країні.

cDc пережила ці рейди, тому що була радше соціальним простором, притулком для хакерів, які хотіли дати вихід своїй енергії, ніж місцем, де замишляють справжні хаки, що порушують закон. Вона пережила й іншу серйозну хакерську подію тієї епохи — першу велику бійку між двома групами: *Legion of Doom (LoD)* і *Masters of Deception (MoD)*. Ці події допомогли *cDc* сформуватися та вижити. Арешти становили виразне нагадування бути обережними, коли йдеться про закон. Вони також дали початок *Electronic Frontier Foundation*, видатної правозахисної групи для хакерів і дослідників, чия діяльність перетинатиметься з *cDc* і її справами. Що стосується дуелі між групами, вона зміцнила наміри *cDc* обійняти позицію миру серед хакерських кланів.

LoD виникла навіть раніше *cDc* і розвинулася на початку 1980-х[4] завдяки вихідцю з Флориди з ніком Lex Luthor.

Організація була недбалою, членство — скороминущим, а регіональні відділення — мало пов'язаними одне з одним. Цікаво, що найразючіші хакерські пригоди *LoD* помітно перетиналися з історіями у *Phrack*, який виріс з електронної дошки, що спеціалізувалася на розповідях про діяльність андеграунду. Статті *Phrack* поширювалися іншими електронними дошками так само, як файли *cDc*, але матеріали містили комерційні таємниці безпеки. На відміну від іншого великого хакерського видання, *«2600»*, *Phrack* був онлайновим, що робило його вразливішим до судового переслідування у часи, коли суди не поширювали свободу преси на цифрову галузь. Наслідки збігів в історіях *LoD* і *Phrack* виявляться важливими та навчать членів *cDc*, як залишатися у безпеці, тому що Phrack складався з хакерів і видання на додачу, тоді як колекція файлів *cDc* залишалася насамперед виданням з хакерами на додачу.

Головна попередниця *HoHoCon* мала менший масштаб і була ближче до кримінального світу. *SummerCon* зібрала для особистої зустрічі лише кілька десятків працівників і читачів *Phrack*. Керівником видання 1988 року був його співзасновник Крейґ Нейдорф, у якого були друзі в *Legion of Doom*. Відвідувач Дейл Дрю з Аризони[5] допоміг Секретній службі записати зі своєї кімнати на плівку, як напиваються учасники зборів. Те шпигування було частиною масштабної роботи, кульмінацією якої стали арешти підозрюваних, серед них і самого Нейдорфа. 1989 року Нейдорф оприлюднив версію посібника з системи *Enhanced 911* компанії *BellSouth*, внутрішній документ з поясненнями, як працювала модернізована система екстрених дзвінків.

Його надав член *LoD* з Атланти, який теж потрапив під арешт і визнав себе винним. Нейдорфа звинуватили в участі у схемі обдурення *AT&T*. У липні 1990 року Нейдорф вивчав політичні науки в коледжі та не хотів співпрацювати зі слідством. Він знав, що документ вкрадений, але не зламував комп'ютери особисто і ніяк не нагрів руки на крадіжці — *Phrack* був безкоштовним для читачів.

Суд над Нейдорфом став вирішальним моментом для хакерів і їхніх захисників переважно завдяки сімейному другу Джессі Драйдена — Джону Перрі Барлоу, фривольному автору пісень *Grateful Dead* і ранньому фанату онлайн-спільнот, який справить неабиякий вплив на *cDc*. 1985 року приятель Барлоу і «кислотник» Стюарт Бренд[6] популяризував онлайн-спільноту *The WELL*, і Барлоу був її плідним і яскравим учасником. Для людей із примітивним онлайн-доступом через модеми, університетські мережі чи інші засоби це була мегадошка, поділена на теми. Барлоу цінив діалог і можливість спілкуватися з цікавими людьми навіть зі свого ранчо у Вайомінгу.

Знайомство Барлоу з неприємною стороною інтернету відбулося наприкінці 1989 року, коли він узяв участь у груповому чаті *The WELL* на тему природи хакінгу. Журнал *Harper's* був куратором чату і надрукував уривки з нього. Серед тих, хто протягом тижня наводив факти і думки, були прихильник вільного програмного забезпечення Річард Столлман, редактор *«2600»* Ерік Корлі (під псевдонімом Еммануель Ґолдштейн, взятим після засудження) та Кліфф Столл, астроном з Берклі, який відстежив хакерів, що працювали на Росію, та описав свою роботу у книжці «Яйце зозулі». Основну

драму влаштували двоє нахабних нью-йоркських хакерів, які називали себе Acid Phreak і Phiber Optik.

Після скарг Столла, що хакерів не слід пускати в мережі, щоб вони витягали фінансові історії з великих кредитних бюро, Барлоу сказав, що набагато більше стурбований тим, що непідзвітні корпорації взагалі зібрали такі дані. Він прирівнював це до крадіжки: «Всякий, хто хоче перешкодити цій крадіжці електронними капостями, має цілковиту мою підтримку». Але коли Барлоу назвав Acid Phreak «панком» за відсутність бачення, Phiber Optik дістав кредитну історію Барлоу та жбурнув її в онлайн-чат. «Усі відплачують, коли їх ображають; ми теж»,— надрукував він. Пізніше Барлоу написав: «Я сидів у барах реднеків[7], коли носив довге закручене волосся до плечей, був на “кислоті” під вартою у поліції та у Гарлемі за північ, але ще ніхто так мене не налякав, як Phiber Optik».

Попри це він продовжував говорити, що його набагато більше непокоїть уряд, який обмежує чи контролює користування комп’ютерами, ніж панки. Він зустрівся з двома хакерами за китайською їжею, знову запевняючи, що вони не є головними ворогами. Потім він переконав бостонського програмного інженера Мітча Капора, винахідника сучасної електронної таблиці, та інженера-лібертаріанця Джона Гілмора заснувати разом із ним *Electronic Frontier Foundation*. (Гілмор невдовзі організує список розсилки *Cypherpunks*, який у наступні два десятиліття буде домом для більшості патріотично налаштованих криптографів, а також хакерів, різноманітних вільнодумців і ймовірного винахідника біткойну.) Тріо поставило довгострокову мету — поширити свободу преси, свободу від необґрунтованого

обшуку та затримань і максимально можливий обсяг інших прав на цифрову галузь. Короткостроковою метою був захист хакерів, які просто стикалися з повним набором наслідків завзятого судового переслідування, починаючи з Нейдорфа.

До суду над ним висвітлення хакінгу в пресі було сповнене емоцій і неправильного розуміння. Репортери вторували великим компаніям, які воліли обвинувачувати у своїх неприємностях злих геніїв, а не свої погані інженерні рішення. До того ж вони брали приклад з ФБР і Секретної служби, де багато нетямущих агентів та інспекторів, які шукали слави, побачили більші загрози для світу, ніж було насправді. Але цього разу в Нейдорфа були гарні адвокати, і вони продемонстрували суду, пресі та публіці головні слабкі місця справи, а зрештою — розгромний факт, що ту саму інформацію в посібнику, яку *BellSouth* оцінила у 79000 доларів, можна було вільно купити за 13 доларів. Уряд закрив справу, і *EFF* почав набувати величезної ролі в дискусіях наступних трьох десятиліть.

[x x]

Справжніми іменами Acid Phreak і Phiber Optik були Еліас Ладопулос і Марк Абен. Ладопулос був першим з групи, що з часом перетворилася на *Masters of Deception*, пізніше Абен перейшов до неї з *LoD*. Обидва були першокласними хакерами з особливим інтересом до комп'ютерів телефонних компаній. Коли MoD розпочала хакінг під своїм ім'ям, Кріс Ґогганс, техаський друг члена *LoD* Скотта Чейсіна, оголосив про свою лідерську роль у *LoD*. (І Чейсін, і Ґогганс по черзі будуть

редакторами *Phrack*.) *MoD* насміхалася зі старшої *LoD*, й обидві групи атакували одна одну в першій великій хакерській війні. Вона посилювалися, доки *MoD* не проникла у *Tymnet*, систему, яку компанії застосували для мережевих підключень, щоб шпигувати за Ґоггансом і Чейсіном.

Коли Джессі започаткував конференції *HoHoCon*, вони стали природною територією техасців з *Legion of Doom*, серед яких були й друзі Джессі, готові до бійки Ґогганс і Чейсін. Поки інші учасники конференції вживали наркотики, пили та обмінювалися історіями, ці двоє сиділи навпочіпки та плели інтриги. Вони вирішили, що єдиний спосіб взяти гору над *Masters of Deception* — стати професіоналами. Вони створили компанію *ComSec* і невдовзі переконали *Tymnet*, що її програми зламують і що вона потребує їхньої допомоги. Озброєні тим особливим доступом, приятелі шпигували за членами *MoD*, а потім перейшли межу: вони зателефонували у ФБР. Ладопулоса й Абена заарештували та засудили[8]. Кожен відсидів рік тюрми. Але для *ComSec* це теж був провал, частково тому, що преса та клієнти просто не могли проігнорувати хакерську біографію її засновників. «По суті, спільнота фахівців з безпеки внесла нас до чорного списку»[9],— скаржився Ґогганс. На одній *HoHoCon* він розповів[10] аудиторії, в якій налічувалося багато його шанувальників, про роздратованість своїми труднощами: «Я дуже розлючений. Сьогодні ти спілкуєшся з президентами корпорацій, а потім сидиш на дні, намагаючись наскребти грошей собі на споживок».

Це ставлення змінилося, коли більше компаній усвідомили, що хакери володіють знаннями, які їм потрібні. Чейсін заснував три компанії, пізніше придбані великими фірмами сек'юріті-галузі, та працював у вищому керівництві компанії номер два з розробки антивірусного софту *McAfee*. Багато їхніх друзів улаштували хлопцям з *LoD* «веселе життя» за те, що вони покінчили з хакерським минулим, та особливо за дзвінок копам. Але більшість з них і самі кинули хакерство. «Всі, хто міг зробити на цьому кар'єру, зробили її на цьому,— зауважив сусід Джессі по квартирі у 1980-ті, Майкл Беднарчик, у ті дні відомий онлайн як Arch Angel.— Ти можеш почати з "дамо тому хлопцю прочухана", але потім ти й сам той хлопець, і починаєш бачити все в іншому світлі». Згодом багато найкращих і найяскравіших членів *cDc* залишать хакерство, коли це буде легше зробити. Але загалом вони уникатимуть контрударів від друзів й інших хакерів внаслідок співпраці з поліцією та ФБР, натомість звертаючись до розвідувальних агентств і Пентагону.

Попри всі конфлікти навколо кар'єрних шляхів, альянсів і поглядів щодо правозастосування *HoHoCon* була приголомшливою подією для тих, хто її відвідав, і це був великий крок до розуміння спільноти, яку намагалися розвинути *cDc* та інші. Оскільки всюди були інформатори, побудувати довіру було важко, особливо онлайн. На особистих зустрічах це було легше. «Навколо було повно наркотиків, багато людей під "кислотою", але попри це тобі вдається налагодити знайомства,— пояснював Беднарчик.— Тепер у тебе є хтось, кого ти знаєш і кому довіряєш, і це формує міцні стосунки». У тих стосунках люди надавали інформацію

та отримували її. Всі дізнавалися докладніше, що здійснено та як.

Незважаючи на тісні стосунки з лідерами *LoD*, Джессі та *cDc* не стали на чийсь бік у війні з MoD, яка завершилася розвалом обох груп. Вони засвоїли урок: від сутичок з колегами та порушення закону не буде ніякої користі, та й дзвінок у ФБР не був мудрим рішенням. Їм вистачило далекоглядності, щоб зрозуміти, що все це завдасть шкоди, навіть якщо ти хотів зробити для світу щось конструктивне.

Джессі вирішив, що *HoHoCon* має бути ще вище конфлікту, ніж *cDc*. Він запросив не тільки різних хакерів, але й також професійних правозахисників і копів, навіть після кількох арештів на конференції. «*Я* організував *HoHoCon*, тому що вважаю дуже важливим зібрати людей з усіх куточків комп'ютерної галузі та телекомунікацій, хакерів, фрикерів і фахівців телефонних компаній і сек'юріті-фірм,— казав він.— Вони можуть зустрітися та розпочати корисні обговорення»[11].

cDc було легко зберігати нейтралітет, адже вона була не кримінальною електронною дошкою, а місцем, куди злочинці та всі інші заходили відпочити. Відмова від причетності до злочинів була філософським вибором засновників і перших членів групи, зробленим з огляду на досвід Нейдорфа та поглинуті суперництвом хакерські банди. Але була й щаслива випадковість: найбільш технічно обізнаним з трьох засновників був Брендон Брюер, й у нього зі старшим братом Таєм був комп'ютер *Atari* без жорсткого диску, а це означало, що вони не могли зберігати щось великого розміру — лише

текстові файли, жодних програм. Хай там як, Брюери зійшли зі сцени, щойно на ній почалося дійство, залишивши «Культ мертвої корови» у руках відносних «голубів миру» Кевіна Вілера та Білла Брауна. «Ми були немов донори сперми,— казав Тай Брюер.— Ми значно вплинули на роботу на початку, а потім пішли. Це була наша ДНК, та й тільки».

[x x]

Ще один майбутній член *cDc* прийшов з *LoD*, і в ньому було більше від досвідченого злочинця та візіонера, ніж у більшості тих, хто приєднався раніше. До *LoD* Патрік Крупа був членом деяких з найперших піратських груп, що спеціалізувалися на продукції *Apple*. 1991 року він став засновником новаторської компанії-постачальника інтернету *MindVox*, яка була для Нью-Йорку тим, чим спільнота *The WELL* була для Території затоки Сан-Франциско — раннім онлайн-аванпостом для вдумливих людей. На думку Патріка, це була третя організація, яка пропонувала американській публіці комерційне підключення до інтернету в режимі реального часу.

Патрік був знайомий з Кевіном з 1980-х, коли мав нік Lord Digital і присвятив себе фрикінгу, щоб утекти від кепського життя в іспанському Гарлемі. Він робив це заради цікавого завдання — видалення захисту з ігор, а потім заради відчуття контролю, який надавав можливість диктувати свою волю машинам по всьому світу. Щоб соціалізуватися, з чотирнадцяти років він відвідував зустрічі *TAP*, на яких загадкові покупці платили йому сотні доларів за здобуту хакінгом інформацію щодо різних людей. У підлітковому віці

Патрік підсів на героїн і залишався на голці до тридцяти років. Він покінчив із залежністю за допомогою галюциногену під назвою «ібогаїн» і пізніше допоміг зробити те саме десь сотні інших наркоманів, серед яких було багато його колег-хакерів.

1992 року, досі на важких наркотиках, Патрік здивував людей з дуже різними поглядами. Того року він розповів про *MindVox* в епічному текстовому файлі[12], який у скороченій формі оприлюднили в журналі *Wired*. У ньому він подякував *cDc*, розповів особисту історію про кіберпростір, відверто оцінив зарозумілість і злочинність багатьох хакерів і визнав свій потяг до опіатів й інших залежностей. Патрік написав, що зрештою усвідомив, що єдина варта зусиль справа — допомагати людям. Після того, за його словами, він знайшов спільну мову з тими в хакерському андеграунді, хто пережив рейди та почувався так само.

1992 року, за чотири роки до того, як Барлоу складе один із найвідоміших політичних документів в історії інтернету, свою «Декларацію незалежності кіберпростору», Патрік напише дещо дуже схоже, екуменічний та ідеалістичний маніфест: «Кіберпростір дає всім свободу співіснувати без шкоди для чийогось світогляду або системи переконань». Він сказав, що *MindVox* надасть користувачам змогу взаємодіяти з піонерами комп'ютерних наук, мистецтва та політики. «Наш головний пріоритет — створити та постійно розвивати середовище, що сприяє атмосфері динамічної творчості, з доступом до інформації та ідей, який надає вам набагато більше розмаїття можливостей».

Есе Патріка використовувало матеріали нью-йоркських медіа, і він, рекламуючи сервіс, дарував безоплатні акаунти в *MindVox* музикантам і акторам. Протягом кількох років MindVox залишався популярним, поки веббраузер *Netscape* та прості постачальники доступу не ускладнили стягнення грошей за вишукані пакети підключення та контенту. 1995 року світанок зручної у користуванні мережі також буде кінцем переважної більшості електронних дощок.

У цей період Патрік надихнув інших у *cDc* і допоміг групі залишатися згуртованою. Однієї чи двох конференцій на рік було недостатньо, щоб підтримувати цілісність групи, і не всі мали можливість увійти до ретрансльованого інтернет-чату *#cDc*, щоб встигати за розмовою. Патрік надав усім безкоштовні акаунти електронної пошти, і Пол Леонард та Керрі Кемпбелл склали список адрес, щоб тримати всіх у курсі.

[x x]

Щороку *HoHoCon* збирала ще більше видатніших спікерів і відвідувачів. Другого року *Hilton* г'юстонського аеропорту прийняв сотню гостей протягом трьох днів. Після відкладеного похміллям початку офіційних процедур у суботу Джессі відрекомендував програмного спікера Брюса Стерлінга, письменника-фантаста, чия книжка про арешти хакерів 1990 року мала незабаром вийти друком. Наступними спікерами були хакери-що-стали-професіоналами Ґогганс і Чейсін, які похвалилися, що на початку місяця жертвами рейдів стали п'ять членів *MoD*. До загальної гульні[13] приєдналися стриптизерки, які влаштовували танці на колінах

у чотирнадцятирічних хлопчиків і надавали секс-послуги в номерах. Менеджери готелю неодноразово погрожувати вигнати всіх геть.

Були присутні щонайменше п'ятеро членів *cDc*, серед них засновник Кевін Вілер і Метт Келлі. Вони зібралися, щоб написати дещо з того, що незабаром стане двохсотим т-файлом *cDc*. Після поверхового згадування *Phrack*, журналу для дівчат-підлітків *Tiger Beat* і таємниць у дитячих книжках «Енциклопедія Браун» файл описував танцівниць гоу-гоу, наркотики та розгардіяш заходу, а також розповідав абсурдну історію культу, у якій фігурували монстр-траки. Небагато з цього мало сенс, утім, файл № 200 виявиться найпопулярнішим серед членів *cDc*.

Інші спонтанні зустрічі вплинули на майбутнє онлайн-безпеки. Беднарчик спускався сходами з другого поверху, коли з ним зіштовхнувся худорлявий хлопчик. Той сказав, що хтось, граючи у пиво-понг, влучив м'ячиком в обличчя Стерлінга і поліція вже їде, тож можна він сховається в номері Майкла? Беднарчик погодився, і підліток відрекомендувався як Джефф Мосс, Dark Tangent. Інші хакери вже тинялися кімнатою, і вони назвали себе за ніками, вже легендарними для - Мосса[14]. Один із них контролював перемикачі у великій телефонній компанії. В іншого були програми-експлойти, які могли проникнути в обчислювальні системи. Мосс, вибалушивши очі, почувався наче загнана в кут мишка. «Ці п'ятеро могли б захопити світ, якби захотіли»,— подумав він. Невдовзі Мосс використає те, що побачив, зв'язки, розмови та футболки, і започаткує *Def Con*, організовувану волонтерами хакерську конференцію

в Лас-Вегасі, яка стане найбільшою з подібних на планеті.

Коли масштаб *HoHoCon* виріс до сотень учасників, приїхало ще більше нових і майбутніх членів *cDc*, щоб зустрітися з людьми, якими вони захоплювалися здалеку. Одним з новачків був талановитий бостонський хакер з ніком White Knight, якого насправді звали Ден Макміллан. Він прийшов повчитися та розважитися зі старими друзями й знайти нових, і, подібно до багатьох інших у *cDc*, йому було байдуже, хто мав більше престижу в хакерському андеграунді. Ден був для *cDc* вирішальним поповненням, тому що привів за собою більше технологічно обізнаних людей. «Ми не шукали хакерські таланти спеціально,— зауважував Кевін.— Важливішими були особистість і вміння писати. Тривалий час тестом або оцінюванням членів було написання текстів. Цього очікували від усіх. Якщо ми і прагнули зібрати більше захоплених хакінгом людей, то це тому, що були б раді більшому різноманіттю т-файлів». Ден підтримував бостонця Мішу Кубеку, і до них приєднаються інші вихідці з Нової Англії: Джон Лестер і Люк Бенфі.

Розвиток конференцій означав більше роботи й менше веселощів для Джессі. Він ділив тягар клопоту зі співспонсором *Phrack* чи *cDc*, а потім нарешті зупинився після 5-ї *HoHoCon*, наприкінці 1994 року. На той момент *Def Con* Джеффа Мосса взяла на себе те, що розпочав Джессі. Вегас пропонував усі незаконні розваги, яких могли захотіти молоді хакери, і буйні відвідувачі конференції могли вилетіти з одного готелю та вільно вибирати з багатьох інших. У *cDc* дізналися, що якщо хтось залишав наркотики у номері, то покоївка охайно

складала їх у купку. Мосс надав членам *cDc* безоплатні перепустки та регулярну платформу, і це створить деякі з найефектніших моментів, притягаючи більше уваги та більше людей. Чверть століття по тому *Def Con* і її дорожче відгалуження для професіоналів, конференція *Black Hat*, будуть головними хакерськими зборами у світі, запросять голову Агентства національної безпеки як програмного спікера та приваблять до пустелі понад двадцять п'ять тисяч відвідувачів.

[x x]

Здавалося, Джессі ніяк не знайде собі місця. Він писав деякі програми на замовлення та протягом року піклувався про свого смертельно хворого батька-музиканта неподалік від Сан-Франциско. І він пережив кілька нещасть: пожежу, яка знищила більшість пам'ятних речей, що залишилися від батька, повінь, яка зруйнувала звукозаписну студію його вітчима. Джессі почав надовго зникати, а його мати і давні друзі в *cDc* ламали голову, де ж він. Хай у чому полягала проблема, це був не алкоголь чи наркотики: пам'ятаючи про проблеми батьків, він ніколи їх не вживав.

Якщо з Джессі дійсно відбувалася якась руйнація, мабуть, тому, що його історії більше не мали єдності. У юності, прожитій під впливом травми, він знайшов притулок онлайн і серед друзів, які вважали його розумним, класним і веселим, яким він і був насправді. Але він засвоїв, що, якщо історії кращі, люди думали, що він ще крутіший. Він сказав багатьом своїм друзям, що грає у рок-гуртах, з *L. A. Guns* та іншими, але нікому не надіслав навіть касети з ярликом звукозаписної студії.

Говорив, що грає у професійний футбол, і деяким це здалося дивним з огляду на його маленький зріст. Він розповів купу історій, і багато з них не були правдою[15].

Дещо з цього було захистом — психологічним захистом для когось, хто подорослішав у тіні знаменитих та успішних людей, та ще й фізичною обороною. Багато друзів-хакерів Джессі були інформаторами. Розповідаючи різні історії різним людям і змішуючи правду з брехнею, він обмежував знання про себе, у такий спосіб захищаючись від зради. «Твій кібердруг може будь-якої миті стати твоїм кіберворогом,— казав Беднарчик.— Ти хочеш відокремлювати свої особистості».

Але це був і напад. Джессі досконало вмів формувати стосунки, як його матір. Він вражав і зачаровував людей, спонукав їх щось розповісти й саме так дізнався більше про хакінг — достатньо, щоб започаткувати перші найважливіші конференції. Джессі був різким і красномовним, з аурою рок-зірки, яка змушувала людей прислухатися. «Він міг передбачити твої думки, перш ніж ти їх промовляв, і за лічені секунди повернути розмову на інше»,— пригадувала Анджела Дормідо, його подруга, яка вела електронну дошку. У хакерів є термін для цього — «соціальна інженерія». Саме вона зробила таким успішним Кевіна Митника та багатьох інших, менш відомих авантюристів. Ти граєш роль, виплітаєш брехню і змушуєш людей робити те, чого хочеш. Міша пригадав Джессі одну історію, якої ніколи не було, і Джессі більше з ним не розмовляв.

Його мати, двоє людей, з якими він жив у різний час, і талановиті пізніші хакери cDc з ресурсами та зв’язками

активно шукали Джессі після його останньої появи 2009 року. Ніхто не зізнався, що в курсі, де він, і деякі з його близьких вважають його мертвим. Можливо, вони мають рацію. Але в середині 2018 року база даних показала, що він має дійсні водійські права в Техасі, які потрібно поновлювати кожні шість місяців. Імовірніше, Джессі використав свої віртуозні навички соціальної інженерії, щоб зникнути з обрію. Хоча він, мабуть, мав той талант у надлишку, це зробило Джессі важливою фігурою у розвитку хакінгу.

Так само як було з текстовими файлами, соціальна інженерія старої школи втратила своє значення через зростання технічної майстерності. З завершенням часу Джессі Драйдена у променях слави центр тяжіння *cDc* перемістився до Бостону, і тут група починала свій шлях до нових великих досягнень.

Розділ 4.
БОСТОНСЬКИЙ АНДЕГРАУНД

У ретроспективі здається очевидним, чому так багато відвідувачів *HoHoCon* приїхало з Бостону і чому це неперевершене студентське місто принесе «Культу мертвої корови» стільки нових людей. До того як більшість американців почула про Кремнієву долину, територія шосе 128 навколо Бостону майоріла комп'ютерними компаніями та розробниками софту, де працювало багато випускників місцевих освітніх закладів, зокрема Гарвардського університету й особливо його суперника, Массачусетського технологічного інституту. Політики називали це Масачусетським Дивом. Кембридж був базою багатьох інноваційних технологічних компаній, включно з двома, які мали в штаті членів *cDc* і їхніх близьких партнерів. Найвідомішою була *Lotus Development Corporation*, яку 1982 року заснував інженер Мітч Капор. Хоча *Lotus* створила свою першу програму для комп'ютерів *Apple*, її хітом була *Lotus 1-2-3*, перша електронна таблиця з графікою. Застосунок працював з ранніми версіями операційних систем *Microsoft*, установлених на персональних комп'ютерах IBM, і для багатьох це стало переконливою причиною купити ПК. Також він приніс Капору достатньо грошей, щоб повністю фінансувати *Electronic Frontier Foundation*, групу захисту цифрових прав, що врятувала редактора *Phrack* від тюрми.

За кілька миль звідти люди, які тяжіли до правої частини ідеологічного спектра, поралися коло техніки тихіше. Заснована 1948 року двома професорами та колишнім студентом *MTI*, компанія *BBN Technologies* спеціалізувалася на інженерній акустиці до того, як уклала нові контракти з Пентагоном і перейшла до роботи в мережі. Вона допомогла розробити робочі версії базових методів інтернет-комунікації, відомих як *TCP/IP*, а також ранні версії електронної пошти та інші програми, що залишаються засекреченими.

Так само як у Техасі, електронні дошки були першими місцями онлайн-зборів у Бостоні. Більшість із тих, які були відкриті для всіх відвідувачів, перешкоджали обговоренню хакінгу, що робило їх менш привабливими для членів *cDc*. Абсолютним винятком за районним кодом 617 у Бостоні була дошка The Works, яку створив майбутній історик електронних дощок Джейсон Скотт Садофський. Він почав вести дошку 1988 року, коли навчався в старшій школі в Чаппаква, Нью-Йорк. Два роки по тому він передав управління нею користувачеві, коли переїхав у Бостон навчатися в коледжі.

The Works, звісно, публікувала файли *cDc*. І це був портал до серйозніших хакерських дощок. На The Works заповзятлива людина могла знайти згадування закритих дощок, де точилися ризикованіші розмови чи які були б ризикованими, якби власники не перевіряли відвідувачів, щоб відсіяти копів, донощиків і занадто балакучих. До доступних тільки за запрошенням дощок, де обговорення могли піти в юридично сірому напрямку, належали *Black Crawling Systems*, *Calvary* та одна під назвою *Democracy*, яка перетворилася на *ATDT* за ім'ям команди модему для набирання дзвінка. Останньою

керували двоє сусідів по кімнаті під ніками Magic Man і Darby Crash. 1991 року випускник Бостонського університету Darby Crash залишив місто заради роботи в *Microsoft*. Під ім'ям Джей Аллард він переконає Білла Ґейтса додати інтернет-функціонал до *Windows 95* і пізніше керуватиме *Xbox*-підрозділом компанії.

Джон Лестер роками відвідував електронні дошки в домі свого дитинства в Дартмуті, Массачусетс. Він навчався в *MTI* та згодом повернувся заради нових онлайн-розваг під ніком Count Zero, за назвою роману Вільяма Ґібсона. Працюючи в Гарвардській загальній лікарні з дослідження хвороби Альцгеймера, він писав технологічні статті-пояснення для *«2600»* і *Phrack*. Magic Man зробив Джона співоператором *ATDT*, коли Darby Crash переїхав на захід країни, а коли Magic Man оселився в Колорадо, Джон успадкував дошку повністю. Дошка *Black Crawling Systems* Браяна Гассіка була вельми технологічною. У *Calvary*, якою керував хтось під ніком Golgo13, була більш злочинна аудиторія: її власник любив зламувати програми. Стартова сторінка містила зображення Ісуса на хресті та слоган «Ви приносите молоток, у нас є цвяхи».

Один день у серпні 1991 року[1] зібрав усіх, передвіщаючи те, що стане відомо як *L0pht* — перший спільний хакерський простір у країні та потужний символ позитивного потенціалу хакінгу. Джон Лестер і Darby Crash жили в одному багатоквартирному будинку поблизу Фенвей Парк, де проводилися домашні матчі «Бостон Ред Сокс». Вони вирішили влаштувати барбекю-вечірку на даху, щоб зібрати постійних відвідувачів своїх дощок, і назвали її «Гриль-до-виснаги». Усім веліли принести свої продукти. Більшість

гостей взагалі хоча б побачили одне одного, навіть якщо вони спілкувалися онлайн роками. Саме тоді Джон зустрів таємничого Golgo13, який справив неабияке враження, бо більшість були худорлявими та блідими підлітками зі зовнішністю ботанів. Golgo13 був дорослим чоловіком, який приїхав на нереально крутому мотоциклі, маючи вигляд викидайла рок-клубу, яким він пізніше і виявився. Потім прийшов Люк Бенфі, відомий як Deth Vegetable. Він був вищий за Golgo13, хоча не з такою агресивною манерою поведінки. Майбутні члени *cDc* Ден Макміллан і Міша Кубека теж були присутні, як і чотирнадцятирічний підліток з нахилом до злочинності Джо Гранд з ніком Kingpin.

Почалася гра в американський футбол, і Люк повів м'яча. Golgo13 спробував збити його з ніг, коли інший хакер зробив те саме з іншого боку. Люк впав, і Golgo13 піднявся з порізом над бровою, який так сильно заливав око кров'ю, що чоловік не міг поїхати додому мотоциклом. Натомість він пройшов кілька кварталів до шпиталю Бет-Ізраель, де його рану зашили, та повернувся випити ще пива. Тим часом Гранд скидав шматки вугілля на голови пішоходів унизу, і один із них викликав поліцію. Ліфт не працював, тому коли бостонські поліцейські дісталися до даху, вони були задихані та дуже злі. Джон та інші попросили вибачення та вмовили їх скуштувати ковбасок. Поліцейські прийняли частування, але попередили: «Якщо нам доведеться повернутися сюди, хтось піде в тюрму».

Навіть без «кровопролиття» та копів це був би незабутній день. Знайомство зі справжніми особистостями людей зміцнило стосунки, які

триватимуть десятиліттями; станом на 2018 рік щорічні «Грилі-до-виснаги» досі проводять.

[x x]

Невдовзі Джон переїхав до будівлі, де жив Гассік, у районі Саут-Енд. Обидві їхні подруги скаржилися на всюди розкидані комп'ютери та інше дивне обладнання, переважно придбане задешево на барахолці списаної електроніки *MTI*. Жінки намагалися почати власний бізнес,— шиття прикрас для капелюхів,— й у квартирі просто не вистачало місця для обох проєктів. 1992 року Джон знайшов лофт з потрісканою підлогою та особливим стилем за кілька кроків, на Волтем-стрит, і всі четверо почали користуватися ним для своїх захоплень. Це був лофт, але, коли вони згадували його письмово, Джон іронічно називав його *L0pht*, з нулем замість О та «ph» від слова *phreaking*. Це була *leet*, жартівлива «елітна» мова хакерів.

Пізніше Джон і Гассік надали столи в оренду своїм друзям, зокрема Golgo13, Дену та Гранду, якого привели туди, щоб не дати піти шляхом злочинця. Гранду більше подобалося бавитися з пристроями, ніж з програмами, і він випереджав галузь безпеки чипів. Але він не повністю кинув свою панківську поведінку, коли познайомився зі старшими хакерами. Він отримував доступ до кредитних агентств за допомогою зламаних паролів, витягав інформацію про лікарів і стоматологів, а потім телефонував у банки з проханням оформити нові кредитні картки на ті імена. Переломний момент настав 1992 року, коли він проник у мічиганський офіс *AT&T* й уникнув тюрми тільки тому, що був неповнолітнім.

Батьки дозволили йому й далі проводити час у *L0pht*, усвідомлюючи, що старші хлопці можуть позитивно вплинути на нього, що вони і зробили.

Коли капелюховий бізнес провалився й жінки забрали свої робочі матеріали з *L0pht*, вивільнилося місце для кількох нових людей. «Ми з Браяном бачили це чимось схожим на клубну анархічну навчальну лабораторію, куди люди можуть приносити техніку та розбирати її. Ми могли використовувати досвід одне одного, а також наявне обладнання,— казав Джон.— Ті, хто має великий потенціал у певних сферах, можуть зустріти людей, які можуть їх навчити та познайомити з кимось ще»[2]. Джон і Гассік щойно заснували перший стабільний хакерський простір в Америці. Протягом наступних восьми років *L0pht* буде однією з великих «гарячих точок» у хакерській історії. Він розмістить перший вебсайт *cDc* і у свого роду коеволюції врешті-решт матиме чотирьох спільних з ним членів. Його прихильники заснували подібні простори по всій країні. Джон вважав це чимось на кшталт тривимірної електронної дошки, постійним мостом між цифровим і реальним світами: «комунальний клуб/мозковий центр/місце зустрічей/ місце зберігання обладнання/комунальна бібліотека» та місце, де можна переночувати.

Джон прочитав файли *cDc* на дошці *The Works* і приєднався до Міши та Дена в бостонській делегації на *HoHoCon* наприкінці 1992 року. Він зупинився в номері, який охрестив «Люкс для еліти», найбільшому та спільному готельному номері, що стане стандартною рисою будь-якої конференції за участю cDc. Там був і Кевін Вілер, Swamp Rat власною персоною. Було пізно, вони втомилися та обговорювали різні теми. Джон нібито

між іншим спитав: «А як узагалі потрапити у *cDc*?». Кевін пояснив, що відтоді, як він заснував групу, це просто: «По суті, якщо я скажу, що ти в “Культі”». «О,— сказав Джон.— Я міг би бути в “Культі”?» Не вловивши зміст запитання та відповідаючи теоретично, Кевін відповів: «Так, міг би». Джон закотив очі та спитав його ще раз: «Можна мені бути в “Культі”?» І Кевін порушив правило не допускати людей, які попросили про вступ: «Так, гаразд. Ти в “Культі мертвої корови”».

[x x]

Попри спільні риси, групи *cDc* і *L0pht* мали важливі відмінності. Перша не мала фізичного простору, не стягувала орендну плату та була різноманітнішою. Відсутність адреси також допомагала *cDc* залишатись у тіні, бути загадковішою та легше асоціюватися з кримінальним андеграундом, особливо коли вона вирішувала зіграти таку роль. Але насправді *L0pht* приваблював людей з різним ставленням до діяльності, яка наближалася до межі закону або перетинала її. У групі не було нікого, чиєю головною метою був хакінг заради прибутку, але це допускало співіснування різних підходів. Джон Лестер визнає, що коли був підлітком, як і багато інших, користувався викраденими телефонними кодами, щоб телефонувати на віддалені дошки. Його найкращий друг і партнер у заснуванні L0pht, Браян Гассік, зізнався, що теж купував речі на вкрадені кредитні картки. І Golgo13 казав, що *ATDT*, яка перемістилася у *L0pht* з Джоном, була «справжнім лігвом хакерів», включно з деякими, хто обговорював «кардінг» — шахрайство з використанням платіжних карток. На дошках закритого типу люди

розповсюджували «коди виходу» — коди, за допомогою яких можна було проникнути в телефонні мережі місцевих компаній, щоб робити безоплатні міжміські дзвінки. «У мене немає шляхетної мети щось поліпшити, хакінг — це спосіб отримати більше інформації,— казав Golgo13.— Я це роблю, тому що мені подобається процес».

Як і набагато молодший Джо Гранд, Гассік намагався залишити свою темну біографію позаду. Він узяв собі нік Brian Oblivion, з фільму «Відеодром». Син пенсильванського сталевара й танцівниці гоу-гоу, Гассік зламав телефонну лінію сусідів і міг телефонувати з автоматизованих модемів на дві телефонні лінії водночас, щоб побачити, хто чи що прийме підключення. Він втручався в роботу опалювальних та інших систем й одного разу вимкнув освітлення ринку. Він пішов з дому в п'ятнадцять років, але продовжував відвідувати школу до випуску, коли їздив поїздами в Сіетл для зміни місця. 1989 року він повернувся на Східне узбережжя. Попри наявність гідних технічних навичок Гассік улаштувався на нічну зміну в магазинчик у Чарльстоні, суворому ірландському районі Бостону, показаному у фільмах на кшталт «Відступники». На його зміні магазин пограбували дванадцять разів. Гассік був добре знайомий з правилами вулиці. Він пальцем не поворухнув, щоб завадити грабіжникам.

Гассік та інші, хто приєднається до *L0pht* і *cDc*, народились у період з 1969 до 1971 року. Через це вони мали ідеальний вік, щоб скористатися магічним вікном між виходом фільму «Воєнні ігри» 1983 року та моментом, коли 1986-го Закон про комп'ютерне шахрайство та зловживання зробив несанкціонований

доступ до комп'ютерів кримінальним діянням. Загалом було дуже ймовірно, що в народжених у ті роки дітей були молоді батьки з критичним ставленням до уряду США. Ден Макміллан, перший бостонець у cDc, народився 1969 року та об'єднував у собі обидва чинники. Його батько, який походив з робочого міста--сусіда Кембриджу, Сомервіля, мав багато друзів в ірландській кримінальній групі «Вінтер Гілл». Щоб уникнути тієї самої долі, батько Макміллана вступив на службу у військово-морському флоті, вивчаючи азбуку Морзе та криптографію на посаді молодшого офіцера розвідки. Після цього він отримав місце аналітика в ЦРУ. Він побачив забагато бюрократичної політики всередині агентства, розчарувався та пішов, вважаючи за краще працювати на самого себе механіком, ніж бути частиною гігантської аморальної машини.

Ден виріс незалежним мислителем у Броктоні, тому ж робочому передмісті, що й засновник *Napster* Шон Феннінг. Його батько був не проти витрачати гроші на комп'ютери для своїх дітей. У Дена було життя офлайн, бігова доріжка та гра у волейбол, але він проводив багато часу на електронних дошках і набув достатніх навичок, щоб у старших класах на платній основі створити бази даних для місцевих підприємств. Він кинув школу, щоб отримати сертифікат еквівалентності освіти, і технічні курси в коледжі Вермонту теж не утримали його увагу надовго. Сумнівна електронна діяльність Дена перед закінченням школи містила епізод, коли глибокою зимою він вимкнув опалення у школі в день, коли не хотів іти на уроки. Крім того, він здобув деяке комп'ютерне обладнання, за яке не заплатив, і користувався «червоними коробочками» для безоплатних дзвінків з телефонних будок. Згодом разом

з Мішею Кубекою та іншими членами *ATDT* Ден проник у різні організації, щоб навчитися всього, що тільки можна.

Оскільки закони досі були на стадії формування, корпоративний захист — слабким, рольових моделей, за винятком Кріса Такера,— мало, а інші мали опозиційні їппі-настрої, люди складали власні етичні кодекси. Ден говорив, що ніколи б не читав чужі електронні листи. І, так само як Гассік, він настільки був стурбований приватністю як серйозним соціальним питанням, що 1992 року разом з Мішею написав текстовий файл для Phrack, звертаючи увагу на слабкі засоби контролю у великого брокера даних того часу, *Information America*. Але на додачу до обвинувачень у незадовільній безпеці стаття містила чіткі підказки для хакерів, які, можливо, захотіли б отримати персональні дані. Серед іншого, у тексті зазначалося, що «первинні паролі, які надають за першого створення акаунту, зазвичай складаються з імені власника акаунту або з імені плюс перша літера другого імені чи прізвища». Згодом Ден пошкодує, що був таким відвертим. Навіть після публікації файлу він досі мав легкий доступ до брокера даних. Одного разу він скористався базою адрес, щоб допомогти своєму дядькові доставити купу унітазів комусь, хто погано з ним обійшовся. Іншого разу Ден відшукав персональні дані актриси, з якою, на його думку, він міг би зустрічатися, але сказав, що не скористався цими даними.

Ці хакери старої школи ставилися з антипатією до сталкерів, професійних злочинців чи інформаторів на кшталт Джастіна Таннера Петерсона, який приїхав на *SummerCon* і таємно записував на плівку розмови членів

cDc, але не зміг зловити їх на зізнанні у злочинах. Це вдалося йому з Кевіном Митником, майбутнім журналістом Wired Кевіном Поулсеном та іншими. Все це, як висловився Ден, «здешевило сцену». «Досліджувати концептуальні питання безпеки набагато цікавіше, ніж допомагати арештовувати людей». Він познайомився з Кевіном Вілером на дошці *Demon Roach Underground*, а потім у видурених конференц-дзвінках. Компанія *Alliance Teleconferencing* була їхньою улюбленою мішенню. Маючи зламаний акаунт, Ден та інші уникали сплати, створюючи лінії для конференц-дзвінків, що були безоплатними протягом днів чи тижнів. Іноді до них запрошували тільки друзів і союзників. Часом заради веселощів організатори підтримували інтерес до конференції, приєднуючи до неї зірок радіошоу, диваків і повій.

Після того як 1990 року Кевін приєднав Дена у *cDc*, Ден висунув кандидатуру бостонця Міши Кубеки, відомого як Omega. Міша мав хист до письма та взявся редагувати текстові файли cDc, допомагаючи створити загальний стиль. Подібно до інших, Міша дотримувався девізу, сформульованого раннім хакером Mentor[3], який наполягав на дослідженні, а не руйнуванні. Пізніше, засмучений тим, скільки персональних даних зібрала *Information America*, Міша почав дуже серйозно ставитися до питань приватності, водночас упевнений, що технічну інформацію слід розповсюджувати: «Існувала можливість отримати будь-яку інформацію про кого завгодно. Для White Knight, мене та інших це був шок, і відтоді приватність мала для мене величезне - значення».

Останнім поповненням до першої бази *L0pht* був Кріс Вісопал, який не дивлячись ткнув пальцем у мапу Массачусетсу, щоб вибрати нік, якого не буде ні в кого іншого. Так він став Weld Pond. На той момент усі столи в L0pht надавали в оренду за 200 доларів на місяць. Тому він розділив одне місце з Джо Грандом — вони платили по 100 доларів кожен. На відміну від інших, Кріс виріс у традиційніших умовах і мав менш бунтарські манери. Вісопал був сином інженера *General Electric* і відвідував католицьку школу в районі Норт-Шор за Бостоном, потім навчався в Політехнічному інституті Ренселера в Трой, штат Нью-Йорк, який у якості викладання комп'ютерних наук поступався тільки Массачусетському технологічному інституту та Каліфорнійському технологічному інституту. Там він вів електронну дошку на хакерську тематику, яка привернула увагу деяких членів Legion of Doom, але неприємності його обійшли. Повернувшись у район Бостону 1987 року, Вісопал отримав бажану роботу в Lotus Development Мітча Капора та зосередився на ній. Але кілька років по тому він знову почав полювання на електронні дошки та знайшов *The Works* і хардкорну хакерську дошку Гассіка, *Black Crawling Systems*. За кілька місяців Гассік запросив Вісопала приєднатися до *L0pht*.

Тепер, маючи у своєму складі Джона, Гассіка, Golgo13, Дена, Гранда і Вісопала, команда *L0pht* почне «копирсання у смітті», риючись у смітниках центральних офісів телефонних компаній чи будівель корпорацій. Вони не шукали зроблені через копіювальний папір квитанції з кредитних карток, відомі як «чорне золото». Їм було потрібне придатне для користування обладнання та посібники і, можливо, внутрішня

телефонна директорія — будь-що, що перелічить, яке обладнання та програми використовують у будівлі, та підкаже, як підключитися та діяти, опинившись у мережі. Але вони також продовжували свій шопінг на барахолці *MTI*. Вони хотіли, щоб їхній хакінг максимально залишався в межах закону, та працювали з технікою, якою володіли самі. «Це було вподобання *L0pht*, яке люди зрозуміли не одразу,— казав Вісопал.— Ми могли вчитися на власних комп'ютерах без потреби щось красти».

Відмова від злочинної діяльності була особливо важливою зі зростанням відомості досліджень групи, які переважно викликали тривогу, оскільки стан безпеки був жахливим. Одного разу група виявила вразливість у програмі Microsoft і збентежила репортерку, яка завітала до них. «Ви хочете сказати, що за допомогою цього можете зламати *Microsoft*?» — «Ну, так»,— сказав їй Вісопал.— «Але ж, користуючись цим, ви здатні зламати будь-який комп'ютер у світі».

[x x]

Щорічні «Грилі-до-виснаги» продовжувалися та поширилися на Західне узбережжя. Але були й інші заходи, що відбувалися частіше. У січні 1991 року за наполяганням Міши група *The Works* Джейсона Садофського почала проводити маленькі щомісячні зустрічі на Гарвард-сквер. Під керівництвом Джона Лестера ті зустрічі розвинулися до зборів спільноти *«2600»*. Вони почались у *Café Aventura* на другому поверсі торгового центру *Garage*. Якщо погода була гарною, учасники переміщувалися до вуличних столиків

у *Au Bon Pain*, через дорогу від Гарвард-ярд. Пізніше, коли приходило забагато людей, зустрічі в першу п'ятницю місяця перенесли в Пруденшал-центр у діловій частині Бостону. Це була неструктурована соціальна година у форматі «покажи та розкажи». Після зборів менші групи часто йшли на Гарвард-сквер або в *MTI*, щоб бавитися з телефонами-автоматами, досліджувати коридори або зловживати інтернет-терміналами в лабораторії. *MTI* був домом для фаната вільного програмного забезпечення Річарда Столлмана, який не вірив у паролі, і це уявлення було частиною ситуації з дуже слабкими практиками безпеки. Серед них була недбало охоронювана таємниця, що будь-які лабораторні термінали нададуть інтернет-доступ на логін *«root»* і пароль *«mrroot»*, пізніше змінений на *«drroot»*. Доволі часто стара гвардія завершувала вечір у квартирі Садофського. В одному з тих епізодів Міша та Ден Макміллан усвідомили, що знайомі онлайн уже два роки.

Серед шанувальників *The Works* і *«2600»* було багато підлітків. Одна дівчина, Лімор Фрід, почала приходити, коли їй було дванадцять. Відома під ніком Lady Ada, вона стане піонеркою maker-культури та першою жінкою-інженером, яка з'явиться на обкладинці журналу Wired і допоможе навчити й надихнути інших своєю компанією *Adafruit Industries*. Ті, хто володів секретною інформацією, як-от неоголошені вади програмного забезпечення, не могли довіряти дванадцяти- чи тринадцятирічним. Тому досвідченіші хакери чекали на збори спільноти *«2600»*, а після йшли в найближчий бар для проведення *«2621»* — зустрічі тих, хто за віком мав право купувати алкоголь. Тільки тоді вони витягали та показували роздруківки зі своїми знахідками. Власник

найкращої отримував безкоштовні напої. «Нікому це не розказували. Це було схоже на “Бійцівський клуб”»,— ділився учасник Джордан Ріттер[4], який належав до хакерської групи *w00w00* і розробив серверну архітектуру у *Napster* для свого колеги Шона Феннінга.

Навіть без доступу до квартири Садофського чи зборів *«2621»* щомісячні зустрічі були чудовим способом дізнатися про інші електронні дошки, спланувати поїздки на конференції чи знайти, з ким розділити орендну плату за житло. Одним із найпримітніших неповнолітніх учасників був буйний здоровань Deth Vegetable, який пізніше стане одним із лідерів *cDc*. Люк Бенфі народився 1973 року та ріс у кількох містах Нової Англії. Він умовив, щоб його зробили співоператором дошки The Works, і складалося враження, що йому цікаво майже все на світі. Це було продовження свободи, яку він уперше відчув онлайн. Він бавився з комп’ютерами з семи років завдяки тому, що його батько працював у компанії-виробнику комп’ютерів серії *VAX — Digital Equipment Corporation*. Попри престижну роботу та минулу службу у військово-повітряних силах, батько Люка був давнім ліваком і вважав себе бітником. Він пережив Голокост і приїхав в Америку підлітком, тому мав підстави м’яко ставитися до конфронтації свого сина з владою, яка почалася невдовзі після того, як двоюрідний брат показав йому *Phrack*. 1987 року батьки Люка отримали телефонний рахунок на 600 доларів і влаштували синові неприємну розмову. Як майже всі його майбутні друзі, Люк знайшов інші та менш законні способи комунікації. Магія раннього інтернету означала, що інші люди стикалися з тією самою проблемою, з’ясовували, що робити, та писали текстові файли-

посібники. Люк поглинав їх та інші матеріали на технологічні теми й будь-що провокаційне чи смішне. У п’ятнадцять років він копіював те, що вважав цікавим, на власну новеньку дошку, включно з купою анархістських файлів з інструкціями виготовлення саморобної бомби.

Люк став фанатом *cDc*, прочитавши її файли на дошці *The Works*. Члени *cDc* володіли навичками, але не сприймали себе серйозно: у спільноті хакерів ті тексти були величезним жартом «для своїх». Будь-яка галузь має власних лідерів, мову та, можливо, навіть фірмовий гумор. Але сторонні особливо не розуміли хакерів, тому багато хто з них скаржився на помилкове уявлення, нерозуміння й тупість. *cDc* вдавалося висміювати і пихатих хакерів, і нетямущу публіку, надаючи своєму гумору невимушеності. Це було круто.

Люк і сам трохи вдавався до хакінгу, серед іншого бавлячись із багом у програмі електронної пошти *Sendmail*. На початку 1991 року він захопив кілька файлових директорій з військової бази США у бухті Субік на Філіппінах. Він побачив дещо схоже на нотатки з брифінгу Розвідувального управління Міністерства оборони. Вони описували майбутнє вторгнення з метою забрати Кувейт в іракців та перелічували залучені підрозділи. Після початку повітряних ударів Люк усвідомив, що дивився на справжній документ, а не на один з багатьох сценаріїв. Хоч він і був супротивником війни, він усвідомив, що розповсюдження цих планів може призвести до обвинувачень у шпигунстві.

Наступного року завдяки підтримці Міши та інших *cDc* прийняла Люка до своїх лав, і 1993 року він уперше

в житті поїхав на *HoHoCon*. «White Knight, Міша та Golgo13 відвідали *SummerCon* і попередні *HoHoCon* й повернулися з дивовижними історіями»,— розповідав Люк. «Вона була темною та загадковою» — конференція для людей, яким, мабуть, не слід проводити конференції. Опинившись там, Люк намагався не почуватися надто ошелешеним, проводячи час у компанії Джессі та Кевіна, який виставляв напоказ своє довге рудувато-русяве волосся, приборкане бейсболкою з логотипом cDc. «Я був частиною *cDc*, але вони робили це роками та були мені за приклад».

Ситуація з житлом у Бостоні була мінливою. 1993 року Люк переїхав до місця під назвою «Месіанське Село» та ділив простір з групою хакерів, готами та диваками, серед яких був майбутній член *cDc* Сем Ентоні, відомий онлайн як Tweety Fish. Сем навчився деякій соціальній відповідальності у своєї матері, Емі, яка була керівницею з питань житлобудівництва за губернатора Майкла Дукакіса. Сем був навіть молодший за Люка; він народився 1975 року та не мав модему до 1989. Але він швидко навчався і наступного року спромігся потрапити на зустрічі *The Works*.

Одного дня у «Месіанське Село» приїхала команда шоу *Dateline* з телеканалу *NBC*. 1988 року п’ятнадцятирічний Люк написав текстовий файл, який поєднував формулу виготовлення саморобної бомби з безглуздими віршами про схуднення через втрату кінцівок, створивши дещо схоже на файл Кевіна Вілера про корм для піщанок. Оператор дошки в Коннектикуті скопіював його. Поліція стежила за ним, і після того як файл завантажила чотирнадцятирічна дитина, вони заарештували оператора. Новини про той арешт розпалили інтерес до

файлу Люка. Його шукали діти, серед них троє підлітків у Монреалі, які отримали травми у двох інцидентах із саморобною бомбою. Один частково втратив два пальці. Хвиля таких випадків привернула неабияку увагу преси, популярність електронних дощок зросла, а батьки усвідомлювали, що їхні діти отримують доступ до анархістських файлів і порнографії.

Цілком розсудливо більшість причетних до сумнівних дощок, з якими зв'язалися представники Dateline, відмовилися говорити. Але Люк вважав, що ці питання слід активніше обговорити і що було б весело потрапити на телебачення. В епізоді шоу, що вийшов у вересні 1994 року, Люк сказав, що пригнічений тим, що діти покалічилися, пояснив, що файл був жартом, і навів обґрунтовані аргументи проти державної цензури. У Dateline сказали, що нік Люка — Deth Vegetable. Викриття та наступні голосіння з боку обурених політиків, звісно, нічим не допомогли, тільки підказали більшій кількості підлітків, де шукати сумнівні матеріали.

Другий прихисток хакерів у районі Мішн-Гілл мав назву «Пекло»: у ньому мешкали майбутній майстер електроніки *cDc* Чарлі Родес, відомий як Chuk E, й уродженець Сан-Франциско Ділан Ші з ніком FreqOut, який теж приєднається до *cDc*. Ділан приїхав зі свого другого рідного міста Медісон, Коннектикут, і вважав, що йому дуже пощастило потрапити в групу «2600». Хтось, з ким він познайомився на одному зі збіговиськ, навчив його, як виготовити «червону коробочку» для дзвінків куди завгодно з телефонів-автоматів. Він і Чарлі навчалися у Вентвортському технологічному інституті та мали доступ до лабораторії, де вони виготовляли друковані плати для масового виробництва цих

пристроїв, продаючи їх іншим студентам за 30 чи 50 доларів, чого якраз вистачало на купівлю нового приладдя. Вони вирішили не шукати більших прибутків і доклали зусиль, щоб не продавати свої «коробочки» наркодилерам — природний ринок, але неприємний. За поетичною іронією долі, у «Пеклі» сталася пожежа через підпал сусіднього триповерхового будинку.

1995 року дві групи об'єдналися в Олстоні у місці, яке назвали Нью Хак Сіті. У ньому оселилися Люк, Ділан, Чарлі та Віндоу Снайдер — онлайн Rosie the Riveter. Випускниця коледжу Шоет Розмарі Голл і дочка програмістів, Снайдер мала аналітичний розум, була яскравою, ущипливою, але доброю. До того ж вона як чорношкіра жінка була дуже рідкісним явищем у тодішніх американських хакерських колах. Пізніше Снайдер працюватиме на серйозних посадах з інформаційної безпеки в *Microsoft* та *Apple*. «Те місце [Нью Хак Сіті] було по коліно завалене обгортками від *Taco Bell*,— розповідала Снайдер.— Воно було найогиднішим з місць, де я колись мешкала, але також найвеселішим».

Компанія *Nielsen*, що обчислювала телевізійні рейтинги, вирішила розмістити в їхньому будинку один зі своїх пристроїв, і група з цілковито зрозумілих причин вирішила використати свій вплив. Єдиний телевізор, який на думку працівників *Nielsen* був у домі, налаштовувався на станцію громадського мовлення, за винятком епізодів, коли заїжджий хакер хотів підтримати інше улюблене шоу. Снайдер не залишилася там надовго, тому що хвалькуватий хакер з ім'ям u4ea зламав інтернет-провайдера у Пітсфілді та погрожував новими атаками. У наступній істерії, що охопила місцеві ЗМІ, газета *Boston Herald* назвала[5] Нью Хак Сіті однією

з п’яти найбільших хакерських груп Бостону та додала, що її членів допитувала поліція. Мешканець-підліток, який дружив зі Снайдер, потрапив під арешт і більше не хотів неприємної уваги, тому вони обоє з’їхали.

Інтернет і Microsoft ось-ось мали бути всюди. *Netscape*, перший браузер, спростив користування мережею. Але момент масового зараження настав у серпні 1995 року, коли ведучий ток-шоу Джей Лено та Білл Ґейтс разом запустили *Windows 95* у телевізійній виставі, що стане звичним явищем у релізах споживчих технологій. Телевізійна реклама з піснею *The Rolling Stones “Start Me Up”* звучала звідусіль. Газети та журнали рясніли запаморочливими поясненнями. Кожна бабуся знала, як увійти в інтернет через комп’ютер. На жаль, ніхто не говорив, що вона має бути в цьому обережною.

Зі зростанням технологічної майстерності членів «Культу мертвої корови» мав поліпшитися й рівень соціальних навичок. Не всі в бостонських колах мали серйозну роботу в інженерно-технічних компаніях, але почали частіше отримувати її, коли загальнодоступний інтернет спричинив безпрецедентний технологічний бум. Однак багато хто бавився злочинною діяльністю, і в дуже багатьох були друзі серед людей, які постійно перебували по той бік закону. Життя з прийняттям і визнанням в обох світах, хакерському та звичайному, скидалося на ходу канатом, натягнутим над мінним полем.

Твої приятелі-хакери хотіли, щоб ти приніс вихідний код для «аудиту безпеки», просто щоб знати, що ти не зіпсував чи не продав його. Твій чинний чи майбутній роботодавець хотів від тебе досвіду, але йому не

належало забагато знати, як ти його отримав. І нікому не подобалися зрадники, за винятком ФБР, єдиного елемента, здатного кинути тебе у тюрму, якщо ти не казав, що знаєш про своїх друзів.

У 1990-ті була одна людина, якій чудово вдалося досягти визнання у світах напівкримінальних хакерів і безпеки, та ще й в уряді. Його найвідоміше ім’я — Мадж.

Розділ 5.
BACK ORIFICE

Пейтер «Мадж» Затко вступив у Музичний коледж Берклі у Бостоні 1988 року, щоб вивчати написання та виконання гітарної музики. Належало робити або це, або десь в іншому місці вивчати технології, а тоді кафедри комп'ютерних наук не викладали те, що його цікавило: як насправді працюють речі на противагу тому, як їм належить працювати. Але його заняття протягом дня не дуже заважали вивчати те, що він хотів. Мадж уже багато знав завдяки експериментуванню та електронним дошкам, які він відвідував роками та де познайомився з Деном Макмілланом й іншими. Одразу після переїзду з дому батька у Пенсильванії до Бостону Мадж дізнався про збори спільноти *«2600»* та виявив, що студенти *MTI* так само зацікавлені у використанні звукозаписних студій Берклі, як він — у лабораторних комп'ютерах *MTI*. Бартерні угоди чудово розв'язували обидві проблеми.

Мадж багато в чому виділявся навіть серед ексцентричних хакерів. Він виріс на самому краю Півдня, де його батько Девід викладав хімію в Алабамському університеті, і був надзвичайно обдарованим музикантом. Мадж розповів, що з двох з половиною років батьки примушували його носити затиснуту підборіддям коробку від сигар, щоб він звик прикладати туди скрипку. На момент свого приїзду в Берклі він практикувався по п'ять годин на день — рутина, яку він порівнював з суворим тренуванням китайських

акробатів. Але він ніколи не цікавився винятково музикою. Девід Затко брав участь у державному проєкті з конструювання космічного шатлу та приносив своїй дитині частини комп'ютерів.

Отримавши 5000 доларів спадщини від дідуся Маджа, його родина, що належала до середнього класу, купила *Apple II Plus* для освітніх цілей. Магазин поблизу пропонував софт, який покупець міг швидко повернути за часткове відшкодування. Це зробило зламування захисту від копіювання нагальною потребою для Маджа та його батька, і це був перший урок про помилкові стимули — тема, на яку Мадж одного дня дискутуватиме в Пентагоні. «Зламування програм *Apple* та ігор на кшталт *Ultima IV* було нашою головоломкою,— казав Мадж,— ми робили це і зламували замки».

До ухвалення Закону про комп'ютерне шахрайство та зловживання 1986 року і особливо до того, як «Воєнні ігри» перетворили відкриті мережі на переповнені місця розваг, Мадж мандрував десь далеко від дому. Заходячи в мережу компанії, зазвичай він залишав повідомлення про свою присутність. Іноді адміністратор гнівно вимагав, щоб він пішов. Іноді працівники просили його уникати певної ділянки. Але найчастіше ніхто не скаржився. Зважаючи на погляди й навички Маджа та членів груп *LoD* і *MoD*, з якими він спілкувався, багато його друзів вважали, що він робив й інші речі, які було б складніше захищати у світлі дня. Офіційно він заперечує, що порушував закон, навіть завантажень піратських програм на обмінні сайти не було. Він лише визнає, що своїми дослідженнями привернув небажану увагу органів влади. Іншим, хто, можливо, не погодився б, було б важко довести, що це дійсно був той

Мадж, з яким вони мали справу. Коли настав час заповнити форми для допуску до державних секретних документів, перелік псевдонімів Маджа охопив десять сторінок[1].

Очевидно, Мадж щось затівав — такою мірою, жартував він, що коли 2015 року китайці вкрали анкети допуску до секретної інформації *SF-86*, що належали йому та мільйонам інших людей, вони, мабуть, подумали, що їх пошили в дурні: ніхто, маючи його історію, не міг отримати допуск. Щоб нагадувати собі про ризики перетину межі, він зберігав над своїми комп'ютерами фотографію, на якій його друга Байрона Йорка[2], відомого як Lou Cipher, заарештовують у Техасі. Мадж познайомився з ним через Дена Макміллана та Джессі Драйдена. Для нього це була хороша людина, якій довелося багато що пережити. На фотографії Йорк лежав долілиць на траві, а поліцейський тиснув йому коліном у спину.

Фотографія спонукала Маджа бути обережним. На *HoHoCon* 1992 року тимчасово звільнений під заставу Йорк розповів хакерам, що його підставив інформатор, який полював на його друзів після того, як один із них зізнався про злочини на зустрічі Анонімних Алкоголіків. «Він чіплявся до нас десь шість місяців, поки ми врешті-решт нібито не сказали "так" щодо схеми підробляння державних чеків,— розповідав Йорк.— Метод провокування тут не застосовується, тому що він не співробітник правоохоронних органів». На задньому плані фотографії арешту видно донощика, його ніхто не чіпає. Фотографія переїжджала з офісу в офіс разом з Маджем — «постійне нагадування ніколи не втрачати

свої моральні орієнтири, чому я все це робив, і що для цього потрібна постійна пильність». У нього був власний кодекс етики: дбати про інформацію. Йому було байдуже, від кого він її отримав, навіть від злочинців, і щедро нею ділився, включно з урядовими службовцями. Але він ніколи б не назвав імена.

Коли в дитинстві Мадж переїхав у Пенсильванію, гірке розлучення батьків надало можливість йому особисто контролювати свій час. Він переконав керівників своєї школи у передмісті, що є дієздатним неповнолітнім і може виправдати випадки своєї відсутності. Мадж вважав за краще спілкуватися зі старшими музикантами й хакерами, наприклад з Робертом Осбандом та іншими, з ким він познайомився через *TAP*.

Потім був Бостон, зустріч з хакерами на Гарвард-сквер і місце стажиста в *BBN Technologies*, де він співпрацював з людьми, які допомагали створювати інтернет. Мадж почав з тимчасової посади в техпідтримці в підрозділі суперкомп'ютерів. Йому пообіцяли, що він може залишитися в іншому підрозділі, якщо там погодяться його прийняти. Натомість він вирішив створити підрозділ безпеки. На той момент він уже допоміг Дену працевлаштуватися в іншій комп'ютерній компанії. Протягом наступних років він допоможе Браяну Гассіку, Крісу Вісопалу та кільком іншим отримати роботу в *BBN*.

1994 року Ден познайомив Маджа з *L0pht*, і через два роки, коли споживчий інтернет захоплював зовнішній світ, він приєднався до групи. Приблизно в той самий час група переїжджала в більше приміщення на складі у Вотертауні. Мадж негайно почав розробляти ідеї, як

зробити *L0pht* стійкішим. Він подумав, що замість просто клубу це місце могло б бути дослідницькою лабораторією. Вони могли б розробляти інструменти гарантування безпеки та продавати їх, використовуючи гроші для продовження хакерської діяльності. Зрештою, якщо все буде добре, можна кинути основні місця роботи й зламувати все, що вразить їхню уяву.

Є одна перешкода[3], сказали чинні члени групи: Джон Лестер з *cDc*. Він не хотів перетворення їхнього хобі на бізнес і вважав, що це негативно позначиться на взаєморозумінні в L0pht. Одного вечора, коли всі, крім Джона, зібралися, вони надіслали йому з акаунту Гассіка, співзасновника *L0pht*, боягузливого листа з проханням не приєднуватися до них у Вотертауні. За наступною вечерею з ним, на якій обговорювалося це рішення, Мадж узяв на себе більшу частину тяжкої розмови. Його роль у вибутті Джона закріпила його новий статус як лідера *L0pht*.

Група, новозареєстрована як *L0pht Heavy Industries*, почала випускати інструменти, включно з тим, створення якого почалося на постійній роботі Маджа. Він звик до *Unix*, але в *BBN* використовували обладнання з *Windows*, і йому доводилося досліджувати питання безпеки і на ньому теж. Бажаючи перевірити надійність користувацьких паролів, він виявив, що *Microsoft* ділить довгі та сильні паролі на дві частини з семи символів кожна, що полегшувало їхнє зламування. Він написав програму з розгадування та спитав *BBN*, чи хочуть щось із нею зробити, але програма мала недбалий, доморобний вигляд, і в *BBN* відмовилися. Тому Мадж приніс її у *L0pht*, де її випустили під назвою *L0phtCrack*. Вісопал написав другу версію, додавши графічний

користувацький інтерфейс, і *L0pht* почав продавати її за невеликі гроші.

Крім того, *L0pht* оприлюднив низку оповіщень, попереджаючи громадськість про вади в різних програмах, зокрема у *Sendmail*, *Lotus Domino* та *IIS Microsoft*. Консультанти з комп'ютерної безпеки взяли їх до уваги, а споживачі почали скаржитися, змушуючи виробників продукту виправити проблеми. Оповіщення привернули першу велику увагу до *L0pht*, і всередині галузі це вилилось у дебати, що роками клекотіли за зачиненими дверима. Багато компаній стверджували, що це безвідповідально — розповідати людям про вади у програмах, які вони продають, адже це навчить хакерів, як проникнути в комп'ютери споживачів. У деяких випадках виробники навіть пред'являли проти дослідників позови за обхід захисту в програмах, які вони купили, щоб «зазирнути всередину». Але коли хакери розповідали про вразливості тільки компаніям, зазвичай їх ігнорували. Єдиним способом дійсно форсувати події та добутися виправлень було публічне розкриття інформації.

[x x]

Зважаючи на досягнення Маджа в *L0pht*, Міша Кубека та Ден Макміллан натиснули на Кевіна, щоб той прийняв його у *cDc*. «Він той, на чию думку слід зважати, і мати його в нашому таборі — гарна ідея»,— написав Міша в листі до групи. В інших склалося враження, що Мадж зламав комп'ютери інших світил сек'юріті-галузі. Але загалом він дозволяв людям думати, що вдається до хакінгу більше, ніж насправді. У *BBN* він мав повну

свободу дій щодо всього, що підтримувала компанія, включно з військовими та фінансовими системами. Це зробило довільні проникнення менш спокусливими. Одного дня до *L0pht* завітав провідний спеціаліст з безпеки[4], і Мадж спитав його, чому система моніторингу електронної пошти Білого дому, яку створив відвідувач, конфігурована у певний спосіб. Під час своєї відповіді гість усвідомив, що Мадж мав побувати всередині системи, щоб поставити це запитання. Інші присутні припустили, що Мадж зламав Білий дім, хоча насправді йому як представнику *BBN* просто надали дозвіл оглянути проєкт.

У L0pht Мадж також діяв як захисник. Він установив бекдор на серверах Unix, щоб упевнитися, що ними не зловживатимуть гості, чи принаймні не дуже сильно. Але поза його домашньою територією діяли інші правила. Мадж писав експлойти та роздавав їх і захисникам, і нападникам. «Я давав певним командам, групам і людям ранній доступ до деяких своїх програм та інструментів. Іноді до інструментів, які були трохи надто потужні та спеціально розроблені для мене, щоб випускати їх публічно»,— казав він. Іноді ті нападники робили йому подарунок у відповідь, як-от безцінний код основних операційних систем. Мадж про це не просив і не прагнув обміну, й хоча теоретично його можна було б обвинуватити в отриманні вкрадених програм, цього не було.

«Тоді бартерною системою для хакерів були tar-архіви авторського вихідного коду й приватна інформація. Іноді нові інструменти вважали ціннішими, тому на мене дивилися як на справжнього авторитета,— пояснював Мадж.— Для мене було важливо, щоб мене вважали

людиною, яка ділиться зі спільнотою, тому що я в це вірив. І так, це елементи спільноти, які явно робили незаконні речі. Це не було ані моїм пріоритетом, ані моєю метою. Я хотів надихнути більше людей на створення новітніх інструментів і проведення прикладних досліджень, щоб ми могли зрозуміти та налагодити кіберсвіт, що розвивався навколо нас».

Хоча бостонці, Джессі та інші були в захваті від Маджа, за Кевіном було останнє слово щодо всіх нових членів, і це ось-ось мало викликати сум'яття, тому що Джон Лестер теж був членом групи. Але Мадж зміцнить перетворення групи з жартівників-самовидавців на авторитетних спеціалістів у галузі безпеки. Кевін дав свою згоду.

Мадж теж дещо отримав від цього союзу. За його словами, він хотів «зробити вм'ятину в Усесвіті». Він хотів розібрати речі на частини і дізнатися, як вони насправді працюють, а потім або пояснити їхній механізм, або, якщо це можливо, зібрати кращими, ніж раніше. Він застосовував той самий спосіб мислення до інших аспектів світу — комп'ютерної галузі як цілого, політики та медіа. Панівні медіа розвивалися разом з можливістю висловити свою думку в мережі, але досі були домінантною і таємничою силою у світі. Як вона вирішувала, що є правдою і які правди найважливіші? Як впливали інші чинники, як-от привабливість історії, обсяг потенційної аудиторії та прагнення до вселюдного блага?

Коли популярність *cDc* зросла, вона перейшла до етапу «глушіння культури», граючи з медіа. Таємничі злочинці, які бавилися не просто з домашніми комп'ютерами

незнайомців, а з центральним пристроєм *NORAD*, являли собою чудовий матеріал для публікацій, і *cDc* вирішила допомогти з поясненнями технологій незалежно від рівня досвідченості репортера. Якщо репортери ставили серйозні запитання, вони отримували серйозні відповіді. Якщо нетямущий телекореспондент хотів лише піарити щось як лячне, *cDc* відповідала і на це. Група усвідомила, що репортаж спонукав до нових репортажів, коли стільки людей так мало знали про комп'ютери. «У правильному вакуумі група на кшталт *cDc* може процвітати. Це їхній талант», — казав засновник The Works Джейсон Садофський. Кевін, який описував себе як «хайпмен», думав про розповсюдження текстових файлів, коли більшість людей про це не замислювалася. Тепер усюди з'являлися телекамери, у членів *cDc* був деякий престиж, і вони, за словами Садофського, бігли їм назустріч: «Ми тут! Ми хакери!».

Мадж побачив у цьому нагоду навчитися. «Це був експеримент — з'ясувати, наскільки легко маніпулювати пресою та медіа, і тепер це дійсно дуже важливо,— сказав Мадж 2018 року.— Якщо ми щось скажемо, чи будуть це повторювати? Хлопці вкидали інформацію, щоб побачити, наскільки далеко вона зайде. Я подумав, це дивовижно. Це змусило по-іншому поглянути на медіа». Мадж застосував отримані знання у *L0pht*, яка мала декілька спільних із *cDc* членів і працювала над схожими проблемами, але отримувала більше поваги від репортерів і телевізійників. У світі безпеки йому доводилося грати роль і хорошого, і поганого поліцейського.

[x x]

Хоча поява всюдисущої мережі 1995 року знищила більшість електронних дощок, *cDc* успішно здійснила перехід завдяки своїй дедалі більшій команді справжніх експертів з безпеки та фізичній базі у *L0pht*. Просто виживання було половиною справи. Щойно вони впоралися з цим, історія cDc змусила людей звертатися до них, коли вони хотіли дізнатися, звідки походить інтернет-культура, що означає мережа та наскільки вона безпечна. Ті, хто зустрічався з *cDc*, потім посилено рекламували її іншим.

Від медіа, звісно, найбільше вимагали пояснень пов'язаних із мережею питань, і вони робили це часто та від самого початку. Шукаючи новини про хакерів до появи *Google*, вони знаходили інтерв'ю Люка Бенфі для шоу *Dateline* 1994 року[5] або епізод ток-шоу *Geraldo* під назвою «Комп'ютерне зло», який поєднав усе погане та непристойне: від історії про серійного вбивцю Джеффрі Дамера до текстового файлу *cDc* 1988 року «Секс із сатаною». Ведучий Херальдо Рівера назвав *cDc* «купою психів». Сама *cDc* розповсюджувала таку думку та інші зауваження медіа, усвідомлюючи, що журналісти не ризикуватимуть, посилаючись тільки на наявні джерела.

Інсайдери на кшталт редактора журналу *Boing Boing* Марка Фрауенфельдера рекламували *cDc*, а у добре дослідженому (зі зрозумілих причин) фільмі «Хакери» 1995 року на задньому фоні видно стикери з емблемою *cDc*. Час від часу впевненість медіа про те, що діяльність *cDc* — це тільки хакінг, призводила до дивних

заяв. Стаття в газеті *San Antonio Express-News* 1996 року[6] про місцевий військово-повітряний центр кібероперацій, наприклад, смішно починалася з твердження, що підрозділ «захищає національні секрети від членів “Легіону долі” та “Культу мертвої корови” у битві, що охоплює весь світ».

У серпні 1996 року виходець із Середнього Заходу Пол Леонард оголосив про відвертий проєкт *cDc* з глушіння культури під назвою *cDc Paramedia* з таким завданням: «світове панування через винищення медіа». Ентузіастами проєкту були Міша, Кевін і Люк, й останній отримав титул «міністр пропаганди». За два тижні після оголошення група написала: «Ми прагнемо приборкати та дестабілізувати медіа[7] де тільки можна. Інформація — це вірус. І ми плануємо заразити вас усіх». Міша з задоволенням написав на сайті групи: «Ми неомарксистський, анархо-соціалістичний диверсійний підрозділ, створений винятково з метою потрапити на телебачення»[8]. Група вважала те, що вона робила, виконавським мистецтвом. Тоді правда не була в небезпеці настільки, як сьогодні, тому намір каламутити воду здавався їй етично прийнятним. «Одна річ, якщо є державний спонсор дезінформації та пропаганди, який прагне досягти конкретного політичного результату, й інша річ, якщо ця пропаганда намагається підвищити обізнаність про деяке питання, яке за інших обставин не отримало б уваги,— казав один член *cDc*.— Обставини мають значення»[9].

У той самий час група розмірковувала над відмовою від своїх старих рецептів виготовлення бомб з відчуття соціальної відповідальності. Але більшість, включно

з Кевіном, проголосувала проти винищення свідчень «анархічного періоду розвитку кіберпанку», за його висловом у груповому електронному листі. Натомість він запропонував додати заяву з відмовою про відповідальність, у якій буде сказано: «Якщо ви досить розумні, щоб використати комп'ютер і знайти сайт *cDc*, у вас має вистачити розуму, щоб не дурникувати з рецептом бомби, повним орфографічних і граматичних помилок. Якщо автор не знає правопису та пунктуації, якого чорта ви вважаєте, що він може описати створення бомби, яка вас не вб'є?»

cDc стала першою хакерською групою, яка випускає пресрелізи, і Міша склав список адрес електронної пошти сотень журналістів. В екстравагантній витівці Люк скористався незаконним доступом до різноманітних баз даних і розіслав роздруківки знаменитостям, серед яких були Шон Коннері, Гаррісон Форд, Ума Турман і кумир Люка, мускулиста й манірна зірка телесеріалу «Команда А» Містер Ті. Тим часом група зберігала таємничість, використовуючи у своїх комунікаціях і публічних промовах тільки псевдоніми.

Відверте прагнення *cDc* до уваги справило незвично щире враження у час, коли інші хакери вдавали з себе кримінальних геніїв чи візіонерів. Вони були високоефективними трикстерами, найчастішими об'єктами інтересу медіа та їхніх аудиторій. Кульмінація настала, коли японська телерепортерка поскаржилася, що продюсери відхилили її ретельний матеріал про хакерство через те, що в ньому бракувало емоційності. Сховавши обличчя під масками чи сонячними окулярами та намагаючись мати лячний вигляд, Люк і двоє інших погодилися дати інтерв'ю перед камерами

та розповіли кілька небилиць. Вони заявили, що здатні змінювати напрямок руху поїздів і супутників. «Вони були шоуменами галузі,— казав про *cDc* засновник *Def Con* Джефф Мосс.— Вони чудово вміли обрати тему й привернути до неї увагу». Що стосується розповідання правди, Люк вважав своєю рольовою моделлю організацію *The Yes Men*, політично вмотивованих активістів, які говорять, що використовують «публічну виставу, щоб вплинути на публічні дебати»[10].

Коли браузер Netscape й операційна система Windows 95 зробили інтернет масовим явищем, проблеми безпеки, що раніше впадали в очі хакерам, раптово поставили під загрозу всіх. Група *L0pht* могла привернути увагу до кількох вад з тисяч, які могли виявити експерти в будь-який час. Але інформація навіть про них зрідка досягала звичайного користувача. Телевізійна реклама, сплачена венчурним капіталом і монополістичними прибутками *Microsoft*, розхвалювала дивовижний онлайн-світ. Але ні в кого не було сильної фінансової мотивації вказати на приховані небезпеки. Майже ніхто з панівних медіа не висвітлював безпеку на постійній основі, а тих, хто робив це поверхово, змушували писати про величні досягнення комп'ютерних технологій, а не про складні потенційні проблеми, недоступні розумінню їхніх редакторів. Граючись із легковір'ям медіа, *cDc* дізнавалася більше, як вони працюють. Група зондувала пресу так само, як досліджувала програми, й поступово усвідомила, що найбільшою загрозою для безпеки було слабке розповсюдження правдивої інформації.

Найкращим місцем, де *cDc* могла почати роботу над цією проблемою, була *Def Con* у Лас-Вегасі. На третій

Def Con, 1995 року, Люк виступив з мініатюрним курсом зі стосунків із медіа. Він переповів історію з *Dateline*, пояснюючи, що кореспондент чіплявся до нього з питанням, чи відчуває він каяття, і що той досвід багато чого його навчив. Здебільшого «медіа огидні,— попередив він.— У них ви дуже зрідка бачите позитивну чи справедливу точку зору щодо хакерів». Люк радив довідуватися про погляди журналістів та оголошувати, які запитання є «забороненою зоною». Але він вважав, що спілкування з серйозними журналістами може бути того вартим, тому що хакери мають найкращу можливість висловитися через медіа та розповісти людям, як захистити себе і як компанії продають софт, у якому повно дірок. Громадські думки були вкрай важливі для них і для споживачів, адже політики зважували рішення з погляду закону та правозастосування, які вирішуватимуть, доведеться хакерам припинити дослідження чи піти в тюрму.

[x x]

Промова Люка на *Def Con-1995* й інші появи в медіа трохи зробили його зіркою серед хакерів, що полегшило знайомство з новими людьми, особливо з тими, хто хотів приєднатися до *cDc*. Але *cDc* не хотіла бути лише соціальним клубом. Саме тоді з'явилася *Ninja Strike Force*. Сем Ентоні вигадав цю ідею після занять кунг-фу та став першим лідером підгрупи. «До *cDc* хотіли приєднатися жахливі люди»,— сказав він. *cDc* хотіла залишатися маленькою, як найкращі електронні дошки, до яких можна було приєднатися тільки за запрошенням. Компромісним рішенням було залишити *cDc* елітною, але розширюватися через *NSF*. Отже, Сем

скопіював дизайн снікерів, написав сатиричну історію походження та замовив футболки. Першими членами були люди, яких група вподобала та поважала, наприклад Кріс Вісопал, Віндоу Снайдер, Лімор Фрід та інженер *Apple* та *Netscape* Том Делл, який написав програми для MindVox і непримітно керував Rotten.com, попередником сайту 4chan.

Того року на *Def Con* приїхали триста учасників, і серед них було важко не помітити здорованя Люка Бенфі. Оклендський хакер Джош Бухбіндер, який був знайомий з ним тільки онлайн, уперше зустрівся з Люком у казино — той тримав підлітка за щиколотки донизу головою та трусив, доки з його кишень не вивалилися монети. Хлопець був настільки наляканий, що, коли Люк його відпустив, із зойком утік. Хтось сказав, що отримати струсана від Deth Vegetable — це велика честь. Тієї ночі Джош приєднався до Люка та його друзів: вони каталися пустелею, вживали наркотики та стріляли всю ніч, наче герої Гантера С. Томпсона. Дивовижно, але ніхто не постраждав.

Протягом наступних двох років Джош підтримував зв'язок із членами cDc і вдосконалював свої навички. 1997 року Ден Макміллан посприяв його приєднанню до *cDc* під ніком Sir Dystic. На той момент Джош навчався в джуніор-коледжі після того, як вилетів зі школи. Він відчував, що технологічно відстає, оскільки всі його друзі з Території затоки бавилися з *Linux*, проривною вільною операційною системою з відкритим кодом, яка кидала виклик *Microsoft* у серверних великих компаній. Коли Microsoft випустила версії *Windows*, які могли працювати з інтернет-підключенням, Джош дослідив їх. Хоча його друзі вважали *Windows* гіршою та нецікавою, Джош

дізнався, що нею користуються досить багато звичайних людей, тож варто провести дослідження. Те, що він виявив, було жахливо. Безпеки взагалі не було. Кожен, хто використовував *Windows*, щоб читати електронну пошту чи переглядати вебсторінки, міг легко втратити контроль над своїм комп'ютером. У системі можна було запустити ззовні майже будь-яку програму, і ті, хто знали, що роблять, могли зробити це непримітно для користувача. Щоб заразити свій комп'ютер, користувачеві було потрібно лише клікнути на файл з невинною назвою.

Джош був далеко не єдиний, хто хотів здійняти тривогу щодо манери Microsoft ховати голову в пісок. 1997 року Кріс Такер розіслав членам *cDc* чернетку тиради, у якій заявляв, що Microsoft — зло, бо продає непотріб, який має шанс на виправлення у майбутніх версіях, тільки якщо поскаржиться достатньо людей. «Ви, йолопи, платите Біллу Ґейтсу, щоб провести бета-тестування його паскудних програм»,— писав Кріс. Проблема була складною, тому що *Microsoft* продавала свої продукти низці виробників комп'ютерів, а не кінцевим користувачам, і мала повну владу над тими відносинами.

Джош знав, що може написати програму, яка послужить доказом, програму, яка надасть невидимий контроль будь-кому, хто зможе встановити зв'язок. Він і сам міг використовувати такий інструмент, щоб шпигувати чи красти. Але це порушить антихакерський закон 1986 року. Жодних веселощів. З іншого боку, оприлюднення програми — з усіма можливими фанфарами — змусить Microsoft визнати проблему та вдіяти щось, щоб захистити своїх клієнтів. За теперішніх

обставин продавати Windows 95 і 98 було, за словами Джоша, все одно що «роздавати дітям заряджені рушниці». «Я вважав, що якщо ми можемо це зробити, може кожен. Компанії потрібно сприйняти це серйозно». До того ж за підтримки медіа за цим буде дуже весело спостерігати.

Він написав усім членам *cDc* листа і спитав їхню думку. Керрі Кемпбелл була проти. Вона перейшла від написання технічних текстів до управлінської роботи в інтернет-провайдера й зараз мешкала поблизу головного кампусу *Microsoft*, де в неї було багато друзів. Крім того, вона знала, що програма наділить новою владою тисячі відносно недосвідчених «скриптомалюків»[7]. Вона розуміла аргумент громадського обов'язку, але вважала, що ймовірні небажані наслідки переважують. «Це завдасть шкоди звичайним людям»,— сказала Керрі. Але вона була в меншості. Інші надали Джошу всю підтримку, якої він потребував. Просто щоб упевнитися, що на ньому не застібнуть наручники лише за написання зловмисної програми, Джош узяв слухавку та зателефонував у місцевий офіс ФБР. Він попросив з'єднати його з агентом з кримінального підрозділу. «Чи виникли б у мене проблеми, якби я написав програму, за допомогою якої люди можуть зламувати чужі комп'ютери?»[11]. «Вам краще спитати в юриста»,— відповів агент. Це не зупинило Джоша. «Ні, ви ж ФБР,— наполягав він.— Ви б заарештували когось, хто зробив це, чи ні?» Агент попросив його зачекати. Через деякий час він повернувся до розмови. «Ми б воліли, щоб ви не робили цього,— сказав він хакеру,— але з формальної точки зору це не протизаконно». Для певності Джош

перепитав ще раз: «Отже, зі мною все гаразд?». «Так», — зітхнув агент.

Відтак почалася тяжка робота: понад рік дослідження незадокументованих інтерфейсів програмування, гачків, що давали програмам змогу брати гору над *Windows*. Джош ще ніколи не писав чогось настільки амбітного. Але він знав, що це можливо; він вважав, що безпека Microsoft межує зі злочинною некомпетентністю, та хотів справити враження на Маджа й інших своїх нових друзів у cDc. Він курив багато марихуани та продовжував уперто працювати методом спроб і помилок.

1998 року Джош отримав багато особистої підтримки. 1992 року Міша переїхав у Сан-Франциско і хвалився про це Люку й іншим на Східному узбережжі за кожної можливості. Одним із перших контактів Міши була редакторка журналу *Mondo 2000*. Вона передрукувала його статтю про *Information America* та познайомила зі своїм хлопцем, Еріком Г'юзом, який збирався активувати список розсилки Cypherpunks, розміщений Джоном Гілмором. Міша розповів про це хакерам. Бум доткомів, який почався з первинного розміщення акцій *Netscape* на біржі 1995 року, привабив до Каліфорнії нові хвилі членів і друзів cDc. 1996 року Ділан Ші отримав роботу в штаб-квартирі Netscape в Маунтін-В'ю, і коли компанія запропонувала оплатити його переїзд, зі своїми речами він привіз і приладдя Люка. Люк відтворив у Сан-Франциско нежилу частину своєї хакерської бази в Олстоні, Нью Хак Сіті. Так *cDc* стала групою з відділеннями на обох узбережжях. Спочатку з'явився хакерський простір на старій консервній фабриці на межі району Догпатч, занедбаної частини міста. Потім — місце на Маркет-стрит і 6-стрит, настільки проблемне,

що одного разу Люк піймав жінку, яка ховалася за його величезною фігурою, щоб курити крек на тротуарі. На дороговказі до квартири був напис *“Setec Astronomy”*, натяк на фільм про хакерів «Пограбування замовляли?» та анаграма словосполучення *“too many secrets”*. Одного дня «відкритих дверей» хтось, не знаючи про жарт, спитав, чому астрономи працюють у підвальній квартирі.

[x x]

У *cDc* вважали, що реакція *Microsoft* на програму Джоша відповідатиме масштабу галасу, якого вона наробить. Тому, тепер краще розуміючи медіа, *cDc* не гаяла часу у створенні інтересу до інструмента, який назвала *Back Orifice* — грубе обігравання назви пакету програм *Back Office*. Вони письмово пояснили, на що здатна програма, задовго до фактичного релізу, який запланували на найбільшу *Def Con*, 1998 року. Хакер міг вирішувати, як встановлювати програму на цільовому комп’ютері, але її можна було сполучати з будь-якою бажаною виконуваною програмою, як-от текстовий редактор чи калькулятор, та надіслати жертві в електронному листі. Пресреліз Люка перелічував функції, які могли зареєструвати натиски клавіш на цільовому комп’ютері та зашифрувати трафік для хакера, який надіслав програму. Інші розробники софту могли додати модулі для розширення функцій. *cDc* не афішувала той факт, що змилосердилася над *Microsoft* і молодою антивірусною індустрією, встановивши стандартний порт для вхідного трафіку як *31337 — eleet* хакерською мовою, тобто *“elite”*. Щоб зупинити стандартні інсталяції, треба було лише блокувати трафік у той порт.

Люк координував основні статті у Wired й інших виданнях, а Кевін та інші зосередилися на тому, щоб зробити презентацію на *Def Con* максимально театральною. У суботу, коли триденна конференція була на піку, Кевін і Ділан вигадали деякі останні трюки якраз перед початком групової дискусії о 16:15. Джош піднявся на сцену та пробубонів кілька нудних речень. Підісланий критикан, який кричав, що *Back Orifice* — це розіграш, вибіг на сцену та схопив мікрофон. Люк накинувся на чоловіка та виштовхав його зі сцени. Потім вискочила решта команди *cDc*. Тил замикав Кевін, одягнений у футболку з написом *Grandmaster Ratte*, з товстим ланцюжком на шиї та у джинсах, прикрашених кролячим хутром. Він застрибнув на стіл і почав читати реп про *cDc*.

«Я відчуваю любов у залі! — скрикнув він.— Ми любимо наших людей!» Він підбурив натовп відповідати відгуком на заклик: «Коли я кажу “мертва”, кажіть “корова”!» — «Мертва!» — «Корова!» Кевін передав мікрофон Сему Ентоні, який говорив спокійніше. Сем мав натягнуту на обличчя в’язану шапку з візерунком у вигляді черепа корови і відверто закликав одержувачів *Back Orifice* до хакінгу за праве діло. «Ми хочемо, щоб ви віддали *cDc* належне,— оголосив він.— Ми робимо це настільки легким, що навіть восьмирічна дитина може принести користь, тобто влаштувати хаос». Керрі сказала кілька слів. Потім уперед вийшов Джош, продемонстрував функції програми та отримав оплески, коли показав діалогове вікно Windows з текстом на свій вибір. Він відповів на запитання, а наприкінці група жбурнула диски з програмою в натовп. Джош дав інтерв’ю для *Businessweek*, *CNN*, *NPR* і *BBC*, і всі вони були шоковані тим, що він не назвав своє справжнє ім’я. Наступного

дня вийшли статті в *USA Today* й інших виданнях. *New York Times*, яка вже згадувала *cDc* в об'ємному матеріалі про *Def Con*, повернулася зі статтею винятково про *Back Orifice*[12]. У другому абзаці вона зазначила: *cDc* сказала, що намагається змусити Microsoft зосередитися на проблемі безпеки. Джош фігурував у статті як Sir Dystic.

Ще ніколи не траплялося нічого подібного. У період такого сильного занепокоєння проблемою хакінгу, на найбільшій конференції з цієї теми, найвідоміша хакерська група безкоштовно поділилася серйозною програмою. Принаймні в короткостроковій перспективі це, звісно, справило враження, що буде ще більше хакінгу. «Вони пожартували над найсильнішою комерційною силою у світі,— сказав Джейсон Садофський.— Захотіли потрапити на телебачення та зробили це».

Однак замість здійняти тривогу чи закликати до спільної боротьби з хакерством чи підвищення безпечності програм, *Microsoft* діяла так, немов ледве зауважила те, що сталося в Лас-Вегасі. Маркетолог *Microsoft* Едмунд Мут заявив *New York Times*: «Це не той інструмент, який нам чи нашим клієнтам слід сприймати серйозно». Компанія стверджувала, що з *Back Orifice* не пов'язані ніякі нові вразливості. Але та заява призначалася для неосвічених людей і медіа. Якби *Back Orifice* спиралася на нещодавно виявлені дірки у *Windows* чи іншому програмному забезпеченні *Microsoft*, компанія усунула б їх в оновленні, і на ризик наражалися б тільки ті, хто не використав патч. Але проблема полягала в основній архітектурі Windows.

Контраст між тим, що говорила *Microsoft* і що говорили красномовніші хакери, був різким і змусив багатьох людей уперше ретельно обміркувати серйозні проблеми. Хоч *«Microsoft* скаржиться, послуговуючись професійними жаргонізмами»[13], як казав Мадж одному інтерв'юеру, вона лише нещодавно створила групу реагування: «Майже несправедливо постійно їх бити, тому що вони не здатні захищатися».

Протягом кількох місяців *Back Orifice* завантажили сотні тисяч разів тільки з вебсайту *cDc*, а скільки поширилося піратських версій — невідомо. Жертвами програми стали тисячі невинних людей. Після того як інтернет-провайдер *MindSpring* поскаржився, що виявляє щодня як мінімум два випадки зараження серед своїх клієнтів, місцевий офіс ФБР в Атланті[14] відкрив кримінальне розслідування щодо *cDc* та особисто Люка. Воно ґрунтувалося на теорії, що заражені комп'ютери передавали вкрадені дані на сервери під контролем *cDc*. Оскільки вони цього не робили, справа розвалилася до свого формального закриття 2003 року. Серед жертв були й хакери. Якщо вони вставляли *CD* з програмою у свої комп'ютери та читали інструкції, могли безпечно завантажити вірус і почати планувати його відправлення жертві. Якщо налаштовували комп'ютер автоматично запускати будь-який диск, миттєво заражалися самі.

У *cDc* рікою полилися і захоплені, і гнівні листи. Один підтримувальний лист надійшов від порнозірки Бренді Александр, яка повідомила, що хтось хакнув журналіста під псевдонімом Люк Форд, який писав про порнофільми, і видалив його файли. «Слава мертвій корові!» — написала вона, пояснюючи, що Форд карав

порноакторів, розкриваючи їхні справжні імена. «Я ваша рабиня, якщо ви регулярно знищуватимете його список імен,— повідомила вона.— Що я можу зробити для вас у відповідь, майстре?» cDc отримала фанатські листи від матерів підлітків, службовця АНБ, британського письменника Ніла Ґеймана та актора фільму «Техаська різанина бензопилою-2». Але не все було так чудово — Джош отримав й анонімні погрози смертю.

У *Microsoft Back Orifice* стала найбільшим головним болем її сек'юріті-спеціалістів. Коли преса усвідомила, що *Back Orifice* — не дрібниця і що компанія не має захисту, *Microsoft* повернулася з новою заявою: тоді як все одно немає про що хвилюватися, ті, хто абсолютно переконаний, що потребують найкращої безпеки, можуть купити прийдешню, повністю перебудовану операційну систему, *Windows NT*. Та система, сказали в *Microsoft*, містить «повний набір функцій безпеки, який робить її найкращим варіантом для найважливіших застосунків корпоративних користувачів»[15].

Зважаючи на все планування *Back Orifice*, група була шокована тим, наскільки сильним був вибух. Тепер набагато більше людей усвідомили, що хакінг — чітка та наявна проблема. Це було чудово. Але фальшива відповідь *Microsoft* досі зберігала поточний стан справ для більшості своїх великих клієнтів. Компанії не мали права подавати позов щодо програмного забезпечення, адже подія, коли програма змінює власника, не визначалася як продаж. Добре фінансовані галузеві юристи переконали численних суддів, що правила користування, які закінчувалися кліком на «Я погоджуюся», призначені для ліцензування угод. Відповідно до закону, за неякісний продукт не було

відповідальності, тому що не було продажу; єдиний засіб правового захисту полягав у скасуванні ліцензії, і це був глухий кут. Хоча *Linux* добре підходив для об'ємних завантажень, звичайні офісні працівники не мали альтернатив для *Word* та *Excel*.

Що більше часу минало, то більше злилися члени *cDc*. Навіть Керрі, яка спочатку не підтримала *Back Orifice*, погодилася: це дурість, що *Microsoft* досі ховає голову в пісок після демонстрації її слабких місць. *cDc* доручила одному зі своїх найновіших і найкмітливіших членів, Крістіану Ріо, взятися за Windows NT і довести, що група не є одноразовим дивом, задушеним маркетинговим відділом *Microsoft*. Цього разу Керрі була за.

«Вони досягли дивовижних результатів, хоч і не знали, що далі з цим робити. Могли б зупинитися,— казав Садофскі.— Але вони пішли тим шляхом та заявили: "Погляньмо, куди він поведе"».

Розділ 6.
МІЛЬЙОН ДОЛАРІВ І МОНСТР-ТРАК

У той час як *L0pht* і «Культ мертвої корови» привертали більше технологічно досвідчених членів, деякі з перших лідерів відходили на задній план. Фанат альтернативної культури та співзасновник Білл Браун підтримував з групою безсистемний зв'язок, коли навчався в коледжі мистецтв і коли почав працювати над експериментальними документальними фільмами, деякі з яких потрапили у великі музеї. Потім він побачив, як *cDc* стала частиною випусків новин. Це добре для суспільства, подумав він, але не дуже підходить для мене. «*cDc* стала цікавою саме тоді, коли я почав менше цікавитися нею». Тепер у складі *cDc* була еліта хакерського світу, хоча її найраніші текстові файли висміювали таких людей як особливо пихатих. «Вона ставала дедалі більше схожою на те, що мала висміювати».

Кевін Вілер поділяв його думку[1]. Коли 1999 року група обговорювала потенційних нових членів, він поскаржився: «Ці хлопці — технарі. Де команда cDc зі скейтбордингу? Чому в *cDc* немає порнозірок? Жодних моторошних військових загонів у Монтані? Чому 95 % нас — білі чоловіки?» Це було правдою: у *cDc* залишалося менше контркультури та дивацтв. Нові таланти залучали переважно схожих на самих себе —

допитливих техногіків з вищою освітою та скептичними поглядами на світ. Останній член і *L0pht*, і *cDc* був саме такою людиною. Батько Крістіана Ріо був професором музикознавства у Льюїстоні, штат Мен. Він приносив додому книжки з програмування, намагаючись опанувати софт для оброблення музики. Як і Мадж, Крістіан навчився зламувати захист у дитячих комп'ютерних іграх, щоб продовжувати в них грати. Родина переїхала у Монмут, Мен, щоб улаштувати Крістіана в освітню програму для обдарованих дітей. Попри це він пропустив восьмий клас і провів останній рік старшої школи в Бейтс-коледжі. Цей коледж мав доступ до ретрансльованого інтернет-чату та мережі *Usenet*, і 1992 року Крістіан натрапив на текстові файли *cDc*. 1994 року, коли йому було шістнадцять, його прийняли у MTI з повною стипендією.

Як той, хто завжди був найрозумнішою дитиною у своєму колі та раніше не жив у Бостоні, Крістіан мав багато що збагнути. Йому сподобалося, що *MTI* припинив ставити оцінки першокурсникам після надто багатьох самогубств студентів. Щоп'ятниці проводилися вечірки з іншими талановитими студентами, і новачок став головою свого братерства. Крістіан також узяв на себе підключення братерства до університетської мережі та уважно стежив за тим, як розвивається інтернет. Він думав про себе як про програміста комп'ютерних ігор, коли прочитав статті Маджа й інших про виявлення вад програмного забезпечення, які можна експлуатувати, і був зачарований цією ідеєю. Серед перспективніших категорій прорахунків у програмуванні була неможливість зупинити те, що називалося переповненням буфера. Якщо кодер не обмежував як слід кількість даних, які можна ввести у буферизовану

ділянку пам'яті, хакер міг ввести забагато й переповнити його. У деяких випадках це надавало хакеру можливість узяти комп'ютер під контроль. Проблеми переповнення буферу виявили в низці високопродуктивних систем, хоча не в ранніх версіях Windows. Крістіан виявив переповнення буферу в *Internet Explorer 4*, браузері, який *Microsoft* 1997 року не належно поєднав з Windows, щоб обігнати першопрохідця *Netscape*.

Крістіан схвильовано написав про свої знахідки у журнал *«2600»*, але той відмовився оприлюднити їх. Тоді він узяв роздруківки на збори спільноти *«2600»* у Пруденшал-центрі, сподіваючись вразити хлопців з *L0pht*. Це спрацювало, і вони опублікували оповіщення про IE4 під новим ніком Крістіана — *Dildog*, за ім'ям собаки Догберта, персонажу серії коміксів «Ділберт». *Microsoft* надіслала електронного листа й холоднокровно попросила, щоб у майбутньому *L0pht* відкладав публікацію даних про вади до моменту, коли буде готовий патч. «Можливо, це непогана ідея»,— висловився Кріс Вісопал.

За словами Крістіана, раніше, якщо компанії скаржилися, що їх заскочили зненацька, *L0pht* стандартно відповідав, що дбає про користувачів, а не про постачальників. Але йому було важко стверджувати, що з виходом патчу справи у більшості користувачів підуть на лад. Тому група почала переговори з *Microsoft* та іншими компаніями. Вона пропонувала сповіщення за місяць до оприлюднення інформації, а компанії просили більше часу. Часто вони досягали компромісу, і запрацював чинний стандарт координованого розкриття. Читання заяв з розкриттям інформації допомагало зловмисним хакерам швидше дізнатися, що

їм потрібно, щоб почати атаку на основі вад, але всі, хто одразу скористався патчем, були в безпеці. Без розкриття тільки хакери, які здійснювали зворотний інжиніринг патчів, могли влаштувати атаки, але громадськість була б менш обізнаною про проблеми. Мадж і Кріс, які написали багато оповіщень, стали найвідомішими та найкрасномовнішими пояснювачами на боці дослідників. «Я хотів, щоб *L0pht* був як *Consumer Reports*, Рейчел Карсон і Ральф Нейдер,— казав Мадж. — Таким було моє бачення».

Попри молодість Крістіана, група взяла його з собою на збори в Нью Хак Сіті, базі серверів *cDc*. Мадж вразив його трюками з монетками у чверть долара, скочуючи їх зі свого носа в кухоль пива. Як студент передостаннього курсу *MTI* Крістіан відвідував заняття з соціальних питань у комп'ютингу та дізнався, що здебільшого вони стосуються безпеки. Першим завданням було проаналізувати переповнення буферу, й інструктор показав слайд з прикладом, що приписували хакеру Dildog. «Це буде набагато легше, ніж я думав»,— сказав собі Крістіан. Наприкінці 1998 року, після випуску, *L0pht* запросив його приєднатися і використав гроші від продажу своїх інструментів, щоб заплатити йому за написання наступної версії своєї найвідомішої програми, зламувача паролів *L0phtCrack*. Це було значне поліпшення, яке принесло групі майже 500000 доларів і підштовхнуло її зробити Крістіана своїм першим працівником на повну ставку. «Призначенням *L0phtCrack* було витягти всіх зі звичайних робочих місць»,— сказав він.

Коли Вісопал привів до групи Крістіана, *L0pht* уже була відомою. Про неї написали *Wired* і *Washington Post*[2],

а оповіщення та інструменти привертали увагу до негативної сторони одержимих маркетингом технологічних компаній без юридичної відповідальності та слабкого ринкового покарання за недостатню безпечність їхніх продуктів. Ні в кого іншого не було достатньої мотивації крикнути «А король — голий!».

[x x]

Річард Кларк у федеральному уряді — організації, що була найбільшим клієнтом *Microsoft*,— усе більше нервував. Здавалося, ніхто не говорив про ризики хакінгу. За президента Буша-старшого Кларк став експертом з боротьби проти тероризму у складі Ради національної безпеки. 1998 року президент Білл Клінтон призначив його національним координатором з питань безпеки, захисту інфраструктури та контртероризму.

В усіх важливих процесах у країні використовували софт, переважно придбаний на відкритому ринку, і Кларк продовжував читати історії про хакерів, які робили з програмами все, що хотіли. Жодних сумнівів, конкурентні уряди могли робити це в Америці. Підозри Кларка посилилися після проведення Міністерством оборони навчальної операції *Eligible Receiver* 1997 року[3]. Червона команда АНБ, яка отримала завдання проникнути в мережі Пентагону, грубо вторглася, використовуючи тільки стандартні інструменти. Кларк тоді про це не знав, але Москва вже проводила таку саму, але реальну операцію, яку пізніше розкрили та назвали *Moonlight Maze*. Успіх *Eligible Receiver* підштовхнув Міністерство оборони створити

спільну оперативну групу — Захист комп'ютерної мережі, що працюватиме в інтересах усіх родів військ.

Проте лідери АНБ продовжували заявляти Кларку, що йому немає про що хвилюватися. Він зустрівся з гендиректорами *Microsoft*, короля мереж *Cisco* та гіганта баз даних *Oracle*, і вони сказали йому те саме. «Вони всі стверджували, що їхнє лайно не смердить, і мені було важко узгодити це з фактом упевненості *Oracle*, *Microsoft* і *Cisco* в реальності хаків,— казав Кларк.— Здавалося очевидним, що мені потрібно поговорити з хакерами. Але вони, можливо, злочинці. То я спитав, чи є серед них хтось не такий». Кларк поспілкувався зі службовцем ФБР, якого перевели з бостонського офісу. «Він зателефонував мені за кілька днів, сказав, що бостонський офіс знає перевірену групу хакерів. На їхню думку, ці люди чесні, і до них звертаються з технічніми запитаннями». На початку 1998 року Кларк узяв із собою команду з НРБ[4]. Хлопці з *L0pht* запропонували випити в барі John Harvard's, а потім тихо спостерігали, скільки службовців там є і скільки вони сидітимуть до того, як піти. За годину, коли вони нарешті підвелися, Мадж привітався.

Після пива члени групи запросили команду з НРБ у *L0pht*. Вони показали трохи того, над чим працюють. Збираючись іти, Кларк та інші службовці з'юрмилися на парковці. Трохи налякані, хакери попросили Маджа сказати їм, що шепотітись у їхній присутності неввічливо. Він підійшов і так і зробив, вимагаючи сказати, що обговорює група. Всі подивилися на Кларка, а він поглянув Маджу в обличчя. «Ми обговорювали, що все це не було б можливим без деякої урядової підтримки,— сказав він.— Ви отримали її?» — «Ні,—

відповів Мадж та пожартував: — Якщо у вас є пропозиція, ми вислухаємо»[5]. Трохи повагавшись, Кларк розсміявся.

Відтоді він підтримував з Маджем зв'язок. Поза групою той був особливо відкритий до обговорень. Деякі давні члени *cDc* досі відчували інстинктивну неприязнь до уряду чи принаймні до деяких його законів, як-от до незграбного Закону про комп'ютерне шахрайство та зловживання, чи до певних його відомств, тобто ФБР. Але родина Маджа отримувала заробітну платню від держави, і він працював урядовим підрядником у *BBN*. До того ж він вважав, що всім варто знати те, що знає він. Він усвідомив, що уряд, можливо, продовжить ухвалювати хибні рішення, але це буде хоча б не через невігластво. Була ще одна, менш благородна причина зіграти в цю гру. Він розраховував на військових, які можуть поручитися за нього, якщо ФБР занадто розхвилюється та раптом здійснить рейд у *L0pht*. «Якби я опинився в суді разом з хлопцями з *L0pht*, обвинувачений у порушенні миру чи чомусь такому, я б хотів мати можливість зробити дзвінок і щоб на лаві свідків сиділа група людей в уніформі та з орденами»,— пояснив Мадж.

Кларк без шуму готував наказ, який буде відомий як Директива про рішення Президента № 63 щодо захисту найважливішої інфраструктури, що надасть уряду більше влади в заходах безпеки в приватному секторі. Щоб мати зброю в міжвідомчих битвах і відвернути скарги з боку Торгово-промислової палати США, Кларк звернувся до свого нового союзника в Бостоні, і невдовзі сенатор Фред Томпсон формально запросив сімох чинних членів *L0pht* дати свідчення в очолюваному ним

комітеті з питань загроз хакінгу. Мадж сказав, що вони зроблять це тільки під своїми хакерськими іменами,— все, на той момент відоме про них громадськості,— щоб захистити свої основні робочі місця. Томпсон погодився. Рада національної безпеки отримала повідомлення, яке вони хотіли передати, і, за виразом Маджа, для *L0pht* це була нагода взаємодіяти з урядом «не маючи на собі тавра злочинців».

Усі, в кого ще не було костюма, купили чи позичили його, й у травні 1998 року вони дали свідчення. Це були Кріс Вісопал, Браян Гассік, Джо Гранд і троє інших членів *L0pht*, а в центрі сидів Мадж, своїм довгим волоссям схожий на музиканта хеві-метал-групи. Він був єдиним присутнім з «Культу мертвої корови». Ден Макміллан переїхав на захід, Джона Лестера вигнали з *L0pht*, а майбутній член *cDc* Крістіан Ріо приєднається до *L0pht* за кілька місяців. «Якщо ви хочете комп'ютерної безпеки, в інтернеті ви її не знайдете,— заявив Мадж сенаторам[6].— Як ви можете очікувати, що ми захищатимемо систему та мережу, коли всі семеро осіб, які сидять перед вами, можуть зруйнувати фундамент, на якій вона збудована?» Найдраматичніша заява, яку вони зробили, полягала в тому, що вони можуть обвалити інтернет за тридцять хвилин, використовуючи проблему, виявлену в протоколі маршрутизації — Протоколі граничного шлюзу[7]. Пізніше Мадж повідомив, що *L0pht* уже зв'язався з виробниками роутерів щодо цієї проблеми. Присутні сенатори були значно більше схвильовані тим, що почули від хакерів, як порівняти зі словами керівників військових і розвідки. Вісопал казав: «Ми були грубим втіленням негативної точки зору»[8].

Свідчення перетворили *L0pht* на першу групу хакерів — рок-зірок, а Мадж був її лідером. Але навіть маючи захист уряду, він та інші в *L0pht*, особливо наймолодші та «чисті» члени, як-от Кріс Вісопал і Крістіан Ріо, були зацікавлені не тільки в поліпшенні стану безпеки, а й у зароблянні собі на життя в процесі. Вони знали, що *L0pht* не може бавитися ідеями чи жбурляти вербальні ручні гранати в уряди чи гігантські компанії.

Для цього був «поганий коп», *cDc*. Обидві групи були розлючені тим, що Microsoft відсторонилася від *Back Orifice*, ігноруючи проблеми безпеки. Компанія висловила дві тези: що *Back Orifice* не є проблемою і що користувачі завжди можуть просто перейти на *Windows NT* чи пізніші версії. Єдиним способом боротьби було створення нової версії *Back Orifice*, яка буде здатна подолати нову операційну систему. Це продемонструвало б, що головні програми *Microsoft* залишилися фундаментально проблемними, тому що не надавали користувачам надійний спосіб дізнатися, що в їхніх комп'ютерах варте довіри. Крістіан був найкращим кандидатом для написання сиквелу *Back Orifice*. Хоча тоді його роботу оплачував *L0pht*, члени групи не могли оприлюднювати те, що вирішили назвати *Back Orifice 2000*, бо це надто сильно прив'язало б *L0pht* до *cDc*, а отже, до *Def Con*, чудернацького одягу та читання репу разом з атмосферою наркотиків і злочинності. «*Back Orifice 2000* не міг асоціюватися з *L0pht*, тому що вже тхнув ним»,— пояснив Мадж. Програма мала залишатися відокремленою від *L0pht*, щоб не налаштувати проти себе інших Річардів Кларків,

які були його потенційними клієнтами та партнерами. У липні 1999 року *cDc* презентує *Back Orifice 2000* на *Def Con* з ще більшою театральністю, ніж торік.

Хоча *Windows NT* розробили набагато ретельніше за *Windows 98*, головна проблема залишалася. Комп'ютер віддавав забагато контролю зовнішнім програмам, які не мали цифрового підпису або не були якось підтверджені як автентичні *Microsoft* чи іншими постачальниками. Внаслідок цього хакеру було легко запустити зловмисну програму на комп'ютері з *Windows* і приховати її присутність. *cDc* хотіла попередити всіх, що ситуація з безпекою Microsoft надто заплутана і що користувачі можуть запускати щось небезпечне, не знаючи про це. Вона хотіла, щоб компанія вимагала від споживачів підтверджувати джерело й стан зовнішнього софту, аби вони могли вирішити, чому довіряти. «Наше прагнення — не дати *Microsoft* прочухана, а навчити користувача»,— написав Крістіан іншим членам групи. *Microsoft* сіла в калюжу та «має відповідати за те, що надала користувачеві стільки влади».

Програма Крістіана була значно кращою за твір Джоша. Поряд із поліпшенням коду *cDc* хотіла розв'язати суперечку між постачальниками програм *Microsoft* і деякими хакерами, що Back Orifice небезпечна і може містити бекдор для *cDc*. Цього разу група хотіла оприлюднити код, зробити його відкритим. Це довело б, що *cDc* не тримає ніякого козиря в рукаві. Також це підвищило б ставки, спрощуючи хакерам модифікацію програми та знижуючи ефективність антивірусів, які шукають ідентичні версії об'єктів, раніше позначених як шкідливі. Офіс ФБР в Атланті попередив Пентагон[9] й інші потенційні мішені, що нова версія буде «набагато

більш руйнівною та важко ліквідовуваною» і що всі зацікавлені особи повинні «активно переглядати й контролювати» свої заходи безпеки. Кримінально-розслідувальна служба Міністерства оборони[10] проаналізувала *Back Orifice 2000*, щоб допомогти військовим розробити контрзаходи, але далі не пішла. Буде більше хакінгу. Але це справить ще більший тиск на Microsoft, вимагаючи виправляння програм.

Як і раніше, *cDc* відмовилася інтегрувати додаткову програму, яка скористалася б вадою софту, щоб доставити й встановити інструмент. На думку *cDc*, відсутність такого експлойту обмежувала моральну провину групи. Її члени розповсюджували інструмент для зламування сейфу, але не ключі від сховища, у якому стояв сейф. Існував також ризик юридичної відповідальності. На той момент суди постановили, що код є мовою, тому майже ніяке регулювання не могло завадити його написанню та розповсюдженню. Але найсерйозніші програми використовували шифрування для комунікації. У випадку *Back Orifice 2000* шифрування перешкоджало б перехоплюванню й розшифруванню даних, які переміщувалися від зараженого комп'ютера до комп'ютера хакера. Адміністрація Клінтона продовжувала придушувати експорт надійної криптографії попри заперечення мультинаціональних технологічних компаній. Уряд прирівнював серйозне шифрування до зброї, хоч і призначеної для захисту, та зробив його предметом експортного контролю. Як і відбувається дотепер, Вашингтон хотів зберегти можливість зламувати коди, використовувані в інших місцях. Якщо якісні шифрувальні продукти потраплять в інші країни, це

завдання ускладниться. Тому Дядько Сем використовував цілу низку постанов, щоб зупинити такий експорт чи завадити йому.

Крістіан не хотів неприємностей з урядом США. Щоб оглянути програму та гарантувати, що пов'язаних з експортом проблем не виникне, члени групи найняли юристку[11]. Вона порадила їм докласти більше зусиль, щоб не дати програмі потрапити у ворожі руки, принаймні до вирішення деяких відкладених судових справ з аналогічних питань. Також вона порекомендувала перевіряти, чи розміщуються *IP*-адреси тих, хто завантажує програму, в США, і брати з місцевих обіцянку не передавати програму за кордон. Ті, хто мешкав за межами США, отримували версію з меншим шифруванням. «Перше правило активіста — не попадатися,— писав Кевін.— Час, проведений у федеральній тюрмі,— поганий час».

У новому експерименті cDc вирішила назвати *Back Orifice 2000* інструментом для віддаленого адміністрування. По суті це висунуло б аргумент, що софт є найновішим інструментом для таємних електронних зламів, але також належить до найкращих інструментів, колись створених для корпоративних працівників для віддаленого нагляду за офісними комп'ютерами та встановлення нових програм. Тоді як *Symantec* і *Compaq* стягували за свої інструменти віддаленого доступу понад 100 доларів, *cDc* запропонувала б аналогічні чи кращі можливості безкоштовно, з кодом, з яким міг ознайомитися користувач. Якщо група обкрутить таке діло, вона кепкуватиме не тільки з *Microsoft*, а й з усталених компаній сек'юріті-галузі, які, на думку *cDc*, наживалися

на ажіотажі навколо акцій інтернет-компаній, у той самий час продаючи посередні продукти.

З наближенням дати запуску верхівка галузі показала своє справжнє обличчя. Компанія з Атланти, *Internet Security Systems*, яка першою продала свої акції громадськості 1998 року, засудила небезпеки *Back Orifice 2000*, щоб розкрутити власний бізнес. Але за лаштунками вона лестила cDc і просила надати попередню копію програми. У такий спосіб вона могла ще до релізу заявити, що здатна заблокувати її. Посередник з *ISS* навіть пропонував готівку[12], що було жахливим способом почати переговори з групою волонтерів, які були переконані, що знайшли етичне обґрунтування своїх дій. Потім Мадж говорив, що *«ISS* була багато в чому геть низькопробною»[13]. *cDc* оприлюднила пропозицію та надіслала відповідь, яку потім передала пресі: «Ми з радістю дамо вам цю програму, якщо та тільки якщо ви натомість подаруєте нам мільйон доларів і монстр-трак»[14]. Деякі співробітники *ISS* працювали в офісі у вихідні, коли проводилася *Def Con*, і відправили своїх дітей у зал, щоб отримати диск і завантажити його за першої нагоди.

Оскільки *cDc* хотіла максимального ефекту, їй була потрібна максимальна увага преси. Щоб це сталося, їй треба мати «ауру зла», розмірковував Кевін, у той самий спосіб, як панк- чи метал-група напрошується на осуд. «Преса, яка в темі, має нас любити, а старомодна й нудна — ненавидіти за цю роботу. Це вічний суспільний конфлікт, на якому можна зіграти,— написав він групі.— День, коли [євангеліст] Пет Робертсон скаже

про *cDc* щось позитивне, буде днем нашого кінця. Саме через конфлікт і драму цікаво та варто про це писати».

Внутрішні звернення теж допомогли. Коли група відпускала жарти, які розуміли тільки інші хакери, це надавало їй престижу та водночас справляло враження на сторонніх людей, які усвідомлювали, що *cDc* знаходила розуміння у справжніх хакерів більше, ніж у людей в костюмах. Але Кевін попередив групу не задирати носа, нагадуючи, що *cDc* починала з висміювання Legion of Doom та інших самовпевнених кодерів. Ідея полягала в тому, щоб розважитися та принести користь. Якраз перед *Def Con* він написав: «Якщо ми надто захопимося власним хайпом, це буде та сама жалюгідна ідіотська штука, якою захоплюються нікчемні зірки рок-музики та кіно, коли вони “не можуть впоратися з тиском” і розвивають руйнівну наркозалежність чи стають мудаками, тому що не розуміють своєї ролі у системі».

[x x]

Коли настав великий день, презентація почалася зі звучання електронної музики й голосів фермера та його дочки: він наказував їй відвести корову назад до хліва, а дівчина відмовлялася. На екрані в затемненому залі пульсували вогники, Кевін понад п’ять хвилин читав реп і ходив сценою. Це був перший повний рок-н-рольний хакерський реліз, прикрашений висвічуванням символу групи точковими прожекторами. «*cDc* любить вас! — викрикнув Кевін і знову підбурив натовп: — Мертва!» — «Корова!». Навіть після того, як у залі спалахнуло світло, він продовжив виступати, «зціляючи вірою». Нарешті

виснажившись, він попросив Сема Ентоні відрекомендувати дев'ятнадцятьох членів *cDc*, які зібралися на сцені,— на той момент у набагато більшій кількості водночас, ніж десь ще.

«Це Deth Veggie, ви всі його знаєте,— почав Сем.— Майбутнє програмування, містер Dildog». Він назвав їх усіх, закінчивши несподіваним поверненням співзасновника Білла Брауна, який був одягнений у старомодний костюм. Далі Сем сказав, що має додати дві зміни до свого минулорічного заклику до хакінгу. «Обери мету», а не займайся хакінгом навмання. І не попадайся. Крістіан зробив відверту презентацію головного продукту і деяких доповнень, підкреслюючи, що код цілком можна пристосувати до індивідуальних потреб. Натовп кілька разів переривав його аплодисментами та криками захвату, коли він пояснив функції, як-от здатність потрапляти в інші комп'ютери, підключені до мішені. Коли він і Джош закінчили відповідати на запитання, світло раптово знову згасло. Білл зірвав з себе верхню частину костюму та продемонстрував стикіні на грудях. Мадж ударив по гітарі та жбурнув її у старий комп'ютер.

Крістіан заздалегідь записав на *CD*-диски копії *Back Orifice 2000*[15] на комп'ютері Лімор Фрід з *Ninja Strike Force*. Він зустрічався з нею. На жаль, її пристрій був заражений вірусом *Chernobyl*, який розповсюдився на диски для преси і ті, що група привезла до Лас-Вегасу, щоб кинути їх у натовп відвідувачів, серед яких були працівники-шпигуни з *ISS*. Щойно хакери на *Def Con* завантажили його в мережу, хтось виявив вірус і здійняв галас. *cDc* визнала помилку й попросила вибачення. На

щастя, версія, доступна для завантаження з вебсайту *cDc*, була чистою.

Крістіан був дуже молодий, і він приєднався до *cDc* настільки швидко, що не мав зв'язків зі злочинцями, як інші члени групи. Коли його спитали, чи скористаються зловмисні хакери його творінням у злочинних цілях, Крістіан відповів, що так не вважає. У ретроспективі це була неправдоподібно наївна думка. Хоча він аж ніяк не був злочинцем, він сказав, що і не є праведником, радше «тим, хто ставить запитання. Я не повною мірою "білий капелюх", тому що намагався не захистити світ, а підвищити обізнаність».

Газета рідного міста Кевіна бачила тільки «чорні капелюхи», і Swamp Rat був абсолютно щасливий. «Ми воліємо називати це справжнім іменем — організованою злочинністю та тероризмом,— оголосив *Lubbock Avalanche-Journal* у редакційній статті, що засуджувала *Back Orifice 2000*.— *Back Orifice 2000* — це зброя. Вона не призначена ні для чого, крім атак і винищення власності людини чи корпорації. Ми вважаємо, настав час для енергійної кампанії проти організованого хакінгу. На нашу думку, це ганебно — надати зброю на кшалт *Back Orifice 2000* у публічному релізі, не боячись притягнення до відповідальності». Як підсумував Кевін для своїх друзів, газетярі «майже назвали нас безбожними комуністами та загрозою американському способу життя й невинності їхніх дочок. Це було кльово»[16].

Сек'юріті-компанії не вдавалися до таких висловлювань, але класифікували *Back Orifice 2000* як вірус. Фінська F-Secure зауважила, що хакери, найпевніше,

скористаються програмою, особливо через те, що вона може працювати непомітно й уникати видалення. Вона продовжувала змінювати свій ідентифікатор процесу та створювала новий замість знищеного. Найвідоміший експерт з криптографії того часу, Брюс Шнаєр, схвалив її як професіонал[17]. Він написав, що ця програма корисна для системних адміністраторів. Також він визнав, що вона сподобається правопорушникам, адже *Back Orifice 2000* є «одним із найкрутіших інструментів у світі». Шнаєр відкрито посилався на філософську гру *cDc* і проголосив її переможцем. «Оскільки її поширює не респектабельна компанія, їй не можна довіряти. Оскільки її написали хакери, це зло. Оскільки її використання в злочинних цілях обговорюють активніше, використання заради користі ігнорують. Це неправильно»,— написав він у своєму блозі. Він сказав, що у Windows 95 і *98* майже немає захисту і що користувачеві довелося б внести більш як триста коригувань до стандартних налаштувань *Windows NT*, щоб убезпечити її.

Microsoft створила небезпеку, а «Back Orifice інформувала користувачів комп'ютерів про неї. Можливо, світ був би в більшій безпеці, якби загрозу не продемонстрували настільки наочно, але я не впевнений,— писав Шнаєр.— Microsoft реагує на загрози безпеці, тільки якщо їх демонструють. Роз'ясніть проблему в науковій статті, і *Microsoft* заперечить її; випустіть хакерський інструмент типу *Back Orifice*, і компанія раптом сприйме вразливість серйозно». Деяка найбільш захоплена підтримка надійшла від високих осіб з організацій-підрядників уряду й Міністерства оборони. Один експерт з *Lockheed Martin*

написав фахівцям з безпеки[18], що галас навколо Back Orifice підштовхнув його дослідити поширеність троянських програм і що він був у шоці, коли виявив в обігу понад десять. Він сказав, що новий гамір навколо *Back Orifice 2000* — це шокова терапія, якої потребують адміністратори мережі. «Якщо ваш захист недостатньо сильний, щоб зупинити скриптомалюків зі загальнодоступними інструментами, вам нічого сподіватися захистити свою мережу від войовничих професіоналів,— написав він.— Прокиньтеся, люди, буде набагато, набагато гірше».

На публіці *Microsoft* знову відмахувалася від проблем навіть після того, як хакери розмістили відеозаписи, на яких вони захоплювали чужі комп'ютери. Але за зачиненими дверима відбувалася паніка. Один керівник попросив спеціаліста з безпеки, Роба «Вайті» Бека, друга Керрі Кемпбелл, принести відеозапис презентації на Def Con. Керрі хотіла допомогти *Microsoft*[19]. Тому вона прийшла в кампус, зустрілася з керівником, а потім ахнула від здивування, коли він вставив принесений нею компакт-диск у свій офісний комп'ютер. «Стривайте,— сказала вона, перш ніж він встиг натиснути кнопку "запустити".— У вас є комп'ютер з пісочницею?» Вона мала на увазі механізм, що перешкоджав потраплянню шкідливої програми в інші комп'ютери. Чоловік витріщився на неї. «Ви не збираєтеся вставити той диск у комп'ютер, приєднаний до мережі, еге ж?» — «Звісно», — відповів він. «Точно? Хіба у вас немає окремого обладнання для цього?» Ще один спантеличений погляд. «Чи правильно я вас зрозуміла? Перед вами сидить представниця всесвітньо відомої хакерської групи, яка щойно випустила інструмент, чия мета —

завдати поразки безпеці *Microsoft*, ви взагалі її не знаєте, і ви вставляєте записаний вдома *CD*-диск, що вона дала вам, прямо у свій комп'ютер? Будь ласка, скажіть мені, що у вас є хоча б антивірус». Ні, він його не мав.

Увесь цей галас ще не повністю достукався до *Microsoft*. Але він нарешті дійшов до її клієнтів, особливо банків, які тиснули на компанію, вимагаючи істотних змін, або ж вони всі перейдуть на *Linux*. Після *Back Orifice 2000* *Microsoft* почала популяризувати електронні підписи, які встановлювали, звідки надходить програма. Крім того, цілісність файлу стала важливою справою, казав Бек, завдяки софту, який перевіряв, чи змінювали програму. Бюджети на безпеку зросли по всій галузі, адже компанії витрачали більше коштів на ретельніші дослідження та купували фаєрволи та системи виявлення вторгнень.

Запуск *Back Orifice* два роки поспіль закріпив статус *cDc* у культурі безпеки, коли інтернет-бум був на піку. У форматі, що пізніше запозичить *Reddit* для своїх чатів, провідний в обговоренні технічних тем сайт *Slashdot*[20] тією осінню влаштував, щоб члени *cDc* під своїми ніками відповіли на запитання читачів. Поряд з купою жартів і вдаваною грубістю вони поділилися переконаннями та цілями, з якими погодилося багато обізнаних читачів. Вони особливо хотіли, щоб компанії-розробники приділяли більше уваги, вкладали більше зусиль і грошей у захист і приватність користувача, навіть якщо не зараховували себе до сек'юріті-бізнесу. «Краще зробити питання безпеки невіддільною частиною процесу розробки, ніж думати про це потім»,— наполягав Сем. Крістіан додавав: «Зашифровуйте все. Відмовтеся від *HTTP* і всюди перейдіть на *HTTPS*».

Приблизно дев’ятнадцять років по тому браузер *Google Chrome* нарешті почне попереджати користувачів, які заходили на *HTTP*-сайти, що вони «не захищені».

Оскільки в усіх членів групи була основна робота, вони обертали на жарт пропозиції розповсюдити значно розширений набір програмного забезпечення, але насправді вони мали більше амбіцій, ніж дозволяли собі визнати. Вони вже розпочинали шлях, запропонований членом, який спонукав використати їхню славу заради якнайбільшого блага. Це був Oxblood Ruffin.

Розділ 7.
OXBLOOD RUFFIN

Лейрд Браун був у повному сенсі цього слова чужинцем, якого прийняли до «Культу мертвої корови», але він найбільше вплине на його шлях. Він народився в Канаді та був скромним технічним спеціалістом, який приєднався до групи в період, коли *cDc* привертала деякі найкращі розуми у сфері безпеки. Лейрд привніс дві речі: поліпшений стиль маркетингу в дусі Кевіна Вілера та відчуття нагальності етичних проблем. Кевін Вілер і Білл Браун завжди наполягали, що головне в *cDc* — не технології, а зв'язок і комунікації. Ретельніше досліджуючи технологічні теми, група дедалі більше розчаровувалася роботою компаній і державних службовців. Великі компанії ігнорували проблеми, якщо їх не показували настільки яскраво, що споживачі погрожували піти, а це було рідкісне явище для монополіста на кшталт Microsoft. Сек'юріті-галузь не виправляла помилки, тому що головні проблеми полягали не в софті: річ була в бізнес-моделях, корпоративній владі та юридичних обмеженнях. Й уряд був сліпим, неповоротливим чи підкупленим, особливо поза військовою сферою. *cDc* бачила все це і, маючи нещодавно отриманий зірковий статус, була готова підняти дискусію на новий рівень.

Високий, балакучий, але розсудливий, Лейрд познайомився з хакерським світом до релізів *Back Orifice*. Він прочитав особисту розповідь Джона

Лестера[1] про його вибрики на *HoHoCon* 1994 року та скопіював його стиль. Він використав мову *cDc* та поступово переконав її членів сформувати певну масштабну позицію. Оскільки він розумів, де група зараз і куди вона прямує, у нього була відповідь на її невідчепне відчуття розчарування. Він почав з раптового, легковажного, чудернацького, улесливого електронного листа Люку Бенфі на його адресу в *L0pht* у вересні 1995 року. «Cher legume, писав він, я знаю про твої труднощі... так багато запитів на твої ресурси... На жаль, це частина тягаря величі. Саме тому мені так тяжко просити про твоє наставництво». Використовуючи латину, французьку та власну версію повної самоіронії хакерської мови, Лейрд пояснив, що два дні читав архівовані текстові файли *cDc*, і йому дуже неприємно завдавати клопоту, але він хоче знати, чи є щось ще «у темі», що міг би порадити Люк. Протягом наступного року приходили інші епізодичні листи, зазвичай одному чи кільком членам *cDc*, які пересилали їх усім іншим. Лейрд сказав, що працює на неприбуткову технічну консалтингову групу[2] з багатьма контрактами з канадським урядом.

Лейрд набув чуття етики[3], зневажав владу та вмів справити враження задовго до коледжу. Він народився 1950 року в родині зварника та вчительки в передмісті Торонто, Гамільтоні, і номінально був протестантом. Але він відвідував католицьку школу для хлопчиків і вподобав моральні настрої навколо, як-от підтримку руху за громадянські права в США та супротивників В'єтнамської війни, багато з яких утекли в Канаду, щоб уникнути військового призову. «Це був визначальний

момент. Усе це, особливо заперечення громадянських прав, було для мене злом»,— казав Лейрд.

З раннього дитинства він грав на скрипці та виступав у різних жанрах за гроші, вивчаючи музику у Віндзорському університеті, поки навчання не позбавило це заняття веселощів. Після роботи працівником автомобільного заводу, кухарем і фотографом Лейрд переїхав до Нью-Йорку. Там він редагував внутрішні інформаційні вісники Організації Об'єднаних Націй і, допомагаючи колишньому працівнику Держдепартаменту з розвідувальними зв'язками, склав багатотомний збірник про внутрішню роботу ООН. Він «прочитав мільйон документів і дізнався, хто є хто», розвиваючи глибокі знання ідеалів і справ організації. Далі він надавав консультації західно-африканським і південно-американським країнам, пояснюючи, як працює ООН. Він залишався на цій - роботі, поки лівійська місія не запропонувала йому вигідну посаду делегата. Погодитися було смішно, але пропозиція призвела до роздумів, які закінчилися тим, що Лейрд покинув місто й повернувся в Торонто.

Протягом десяти років роботи в ООН Лейрда переслідували думки про скрутне становище китайських дисидентів. Ринкова лібералізація у 1980-ті посприяла зародженню китайського студентського руху за свободу слова та демократію, і Комуністична партія не знала, як на це реагувати. Після того як 1989 року на площі Тяньаньмень зібрався більш як мільйон протестувальників, прем'єр Лі Пен оголосив військовий стан і ввів війська, які вбили понад сотню осіб. Лібералів позбавили лідерських позицій у Комуністичній партії, і обсяг дозволених для обговорення тем сильно

скоротився. Однак Лейрд став активістом тільки після свого приєднання до *cDc* 1996 року.

Як і належить тому, хто роками працював серед красномовних ораторів в ООН, Лейрд зберігав поважний тон, навіть коли став частиною групи. Але поступово він умовив *cDc* змінитися, мати основоположну точку зору та ретельно вибрану ціль. *cDc* була знаменитою, але не відстоювала жодних важливих питань, крім комп'ютерної безпеки. І він вважав, що варіантом розширення бачення є політика китайського уряду. Це був дуже особистий аргумент, адже Лейрд подорожував Азією та був добре знайомий з людьми, які боролися за громадянські права в Китаї. Також він сказав, що в період роботи в ООН познайомився з китайськими дипломатами, які натякнули про свою невдоволеність подіями на батьківщині. Від самого початку Лейрд розповів іншим про чоловіка, якого зустрів у Торонто,— китайського вигнанця, котрий допомагав іншим виїхати після різанини на площі Тяньаньмень. Поступово надійшли подробиці історії. Його друга захищали члени гангстерського угрупування, які таємно перевозили людей з інших причин. У нього була мережа помічників. І він зацікавився технологіями, які можна використати для допомоги дисидентам, що було якраз до вподоби *cDc*.

За внутрішніми правилами *cDc*, будь-хто мав можливість висловити думку щодо кандидата в члени групи, але останнє слово було за Кевіном. Крім того, хтось мав знати його особисто. Влітку 1996 року Люк відвідав Лейрда в Торонто, і невдовзі його прийняли до *cDc*. Він обрав собі нік Oxblood Ruffin, поєднавши посилання на темно-червоні черевики *Doc Martens*, популярні на

британській панк-сцені, та на Девіда Раффіна — головного вокаліста гурту *Temptations* у піснях *My Girl* та *Ain't Too Proud to Beg*.

У жовтні Люк повернувся в Торонто в товаристві Джона Лестера та Сема Ентоні. Лейрд задокументував цю подію[4] в класичному стилі *cDc*, написавши решті групи смішного електронного листа, схожого на текстовий файл. Він заявив, що вони щойно провели першу річну «Вон-Тон-Кон» у ресторані в Чайнатауні. Він описав ресторан як улюблене місце зустрічей «Гонконгівських блондинок», «об'єднання китайських комп'ютерників і демократичних активістів», які, за його словами, не могли приєднатися до них того дня з причин безпеки. Кілька місяців по тому Лейрд розповів дивну історію «Гонгонгівських блондинок». Він пояснив в електронному листі, що вигадав групу як жарт, але його не названий бос у неприбутковій консалтинговій фірмі був «зачарований» вигадкою, «цією потужною міфічною силою у мережі», яка може спричинити появу імітаторів і спантеличити китайський уряд. Лейрд сказав, що познайомив свого керівника з вигнаними дисидентами в Торонто і що «Блондинки» стали реальністю.

Китайський уряд став ідеальним каталізатором, що підштовхнув *cDc* до політики. Він ненавидів вільний потік інформації, головну цінність cDc і хакерського руху. До того ж Китай протистояв уряду США, де працювали деякі члени *cDc* та їхні друзі й родичі. І Китай мав справи з тими самими компаніями, які так ненавиділа *cDc*, головне місце серед яких посідала *Microsoft*.

Лейрд був майстерним маркетером, і ця справа посилила його мотивацію. Хоча його таємнича поява й туманна біографія спантеличила групу, у словах Лейрда була людяність, як казав Міша Кубека, і це було великим кроком уперед для гіків. Попри все він знайде спосіб розповісти переконливу історію, яка зачепить медіа, практиків сфери безпеки та, мабуть, найпопулярніших технічних спеціалістів. «Дякувати Богові, що в нас були підказки Лейрда,— пригадувала Керрі Кемпбелл.— Він сказав: “Зараз у вас є трохи слави, то що ви хочете робити? Бігати навколо неї як ідіоти чи щось вдіяти?”» Лейрд перетворювався на нового мудрого дорослого — роль, яку відігравав Кріс Такер.

[x x]

Так само як Такеру, Лейрду було від чого відштовхнутися. Основою його переконань була політизація, найдраматичніше висловлена 1996 року лібертаріанським республіканцем Джоном Перрі Барлоу, засновником *Electronic Frontier Foundation*. На вечірці у дні Світового економічного форуму в Давосі, Швейцарія, Барлоу прочитав, що ексцентрична спроба ввести інтернет-цензуру щойно стала частиною американського законодавства про телекомунікації.

Ексцентричною відповіддю Барлоу стала «Декларація незалежності кіберпростору»[5]. Написана в дусі Томаса Джефферсона, вона починалася з натяку на Карла Маркса: «Уряди Індустріального світу, ви — втомлені гіганти з плоті й сталі, а мій рідний край — Кіберпростір, новий дім Розуму. Від імені майбутнього прошу вас,

у кого все в минулому, дати нам спокій. Ви зайві серед нас. Ви не маєте верховної влади там, де ми збираємося». Бойовий заклик у шістнадцятому параграфі незабаром опиниться на десятках тисяч вебсайтів. «Ми створюємо світ, до якого можуть увійти всі, без привілеїв чи упереджень, породжених расою, економічною владою, військовою силою чи місцем народження. Ми створюємо світ, у якому будь-хто та будь-де може висловити свої переконання, хоч які вони своєрідні, не побоюючись примусу до мовчання чи конформізму».

«У Китаї, Німеччині, Франції, Росії, Сингапурі, Італії та Сполучених Штатах Америки ви намагаєтеся протистояти вірусу свободи, створюючи вартові пости на кордонах Кіберпростору. Можливо, на деякий час вони його стримають, але це не спрацює у світі, який невдовзі буде охоплений цифровими медіа. Ми створимо цивілізацію Розуму в Кіберпросторі. Хай вона буде людянішою та справедливішою, ніж світ, раніше створений вашими урядами». Це було ідеалістично та доволі наївно для технологічної культури, яка вже винагороджувала експлуатацію людської поведінки, що ґрунтувалася на кліках.

Двадцять років по тому Барлоу сказав, що наївність була свідомою[6]: «Я знав, що поява мережі обов'язково принесе однаково дуже позитивне й дуже негативне. Якщо можливо, щоб усі дізнавалися все, що їм цікаво, також можливо, що хто завгодно, будь-де, винайде повністю готовий тоталітаризм, у якому можна клацнути перемикачем і побачити всі ваші наміри». Барлоу хотів «установити культурні очікування», щоб посилити сторону справедливості для майбутніх битв. «Я хотів,

щоб люди усвідомили та відчули, що ми входимо в золоту еру, і вона означає свободу, а також стрімкий розвиток і поширення знань. І якщо пощастить, ми розберемося, як давати раду жахливій стороні процесу».

Попри всі свої навмисні недоліки та надлишок пристрасті, промова Барлоу відгукнулась натовпу технічних спеціалістів, шукачів справедливості та споживачів, які відчайдушно бажали, щоб уряд зробив щось інше, крім руйнації найвеличнішого винаходу в їхньому житті. Найпалкішими прихильниками були програмісти, люди, які щодня створювали технології для себе та інших. Усі вони за визначенням завжди працювали над чимось новим, що мало бути кращим, ніж раніше. Всередині цієї групи найбільшими ентузіастами були хакери, нонконформісти та дослідники, які розбирали та розбирали речі і які з найвищою імовірністю порушували у процесі закони на кшталт Закону про телекомунікації, Закону про комп'ютерне шахрайство та зловживання й Закону про авторське право в цифрову епоху.

Зважаючи на схильність хакерів працювати ізольовано та відкидати соціальні норми, важко робити узагальнення щодо їхніх переконань. Дуже багато майстрів робили все можливе, щоб ігнорувати величезні частини зовнішнього світу, особливо ті, що мали стосунок до політики, а деякі майже не звертали уваги на хакерів, які працювали в суміжних сферах, як-от інше апаратне забезпечення, операційні системи чи застосунки. Але справедливо говорити, що більшість тих, хто звертав увагу на політичний світ,— а їхня кількість значно зросла, коли наполовину уявний

незалежний кіберпростір Барлоу зіткнувся з реальністю уряду,— була на його боці.

Коли декларація Барлоу вкупі з лайкою Лейрда на адресу Китаю викликала резонанс у *cDc*, Міша винайшов термін хактивізм, сполучення слів хакінг та активізм, концепцію, яка десятиліттями матиме величезне значення в пошуку хакерами своєї ролі у суспільстві. «Це слово описує спільну справу “Гонконгівських блондинок” і *cDc*»,— написав Міша групі.

[x x]

Наступний рік відзначився серпневим відродженням хакерської конференції, заснованої в Нью-Йорку три роки тому журналом *«2600»*. Вона мала назву *Hackers on Planet Earth* («Хакери на планеті Земля»), або *HOPE*. Назва, яку 1997 року змінили на *Beyond HOPE*, була показовою для конференції, що зосередиться на ідеалізмі сильніше, ніж це зробила *Def Con*. Її відвідали дві тисячі осіб, удвічі більше за збіговисько 1994 року. У членів *cDc* було багато виступів, зокрема у суботу була панель *L0pht* з Маджем, а в неділю у ній взяли участь вісім членів *cDc*. Це взагалі була перша хакерська конференція, яку відвідав Лейрд, і на той момент йому вдалося закріпитись у *cDc* і мати на подив сильну лідерську роль у групі.

Люк був ведучим півгодинної панелі та відрекомендував Кріса Такера, «хакера-лауреата» Маджа, Сема Ентоні, «міністра закордонних справ» Лейрда, Керрі та Джона Лестера під їхніми ніками. Хоча панель було присвячено оновленню інформації про діяльність групи, Люк

роз'яснив, що найважливіша подія — «стратегічний альянс» з китайською продемократичною групою «Гонконгівські блондинки», до складу якої входять технічні спеціалісти та активісти. Потім настав публічний дебют Лейрда. Зі своїм охайним виглядом і короткою стрижкою він був єдиним у панелі, кому, здавалося, було б зручно в костюмі, хоча він був убраний у жовту спортивну сорочку.

Лейрд розповів, що працював в ООН, познайомився з китайськими дисидентами, які перебували за кордоном 1989 року, та підтримував з ними зв'язок навіть після того, як різанина на Тяньаньмень висмикнула демократичний рух з поля зору. Він пояснив, що назва «Блондинок» посилається на жаргонне слово, що позначає золото як наріжний камінь свободи, й описав дещо з того, яким є життя за репресивного режиму. Здавалося, він ставить собі за заслугу те, що запропонував «Блондинкам» використати мережу для координування протестів: «Кілька років тому я спитав одного зі своїх контактів у Принстоні: "А ви користуєтеся мережею для правозахисної діяльності?" Він був вражений і сказав, що це, мабуть, гарна ідея. Ми знаємо, що він установлює зв'язок з кількома своїми колегами й партнерами, що спеціалізуються на комп'ютерних науках і дуже співчувають боротьбі за демократію». Діяльність «Гонконгівських блондинок» формально почалась у вересні 1996 року. «Хакерська спільнота міжнародна,— заявив він у своїй шести-хвилинній промові.— Ми всі в одній спільноті».

Кріс Nightstalker Такер закликав хакерів у США бути більш політично активними та консультувати законотворців, а Сем сказав, що ті, хто добре знається

на технологіях, можуть відігравати велику роль принаймні у привертанні уваги до важкого становища китайців й інших: «З тих, хто розуміє цю технологію, ми найсильніші в розповсюдженні інформації. І коли інформація на волі, вона допомагає». Далі група відповіла на запитання про «Блондинок», безпеку, текстові файли та проєкт операційної системи з відкритим кодом, очолений її партнером. На думку керівника конференції та засновника журналу *«2600»* Еріка Корлі, у cDc був ідеальний бадьорий активізм, якого він хотів. «Вони розважилися та передали важливе повідомлення,— сказав Корлі.— *cDc* була унікальною».

Виступ у Нью-Йорку надав гостям конференції нагоду зустрітися з місцевими членами cDc і одне з одним. До тих вихідних Лейрд особисто знав дуже мало інших членів групи; вони були просто друзями за листуванням та партнерами. Кріс Такер ніколи не зустрічав Сема чи Керрі. Особливо радісним було возз'єднання Керрі та іншого давнього члена *cDc*, Psychedelic Warlord. Він поїхав на схід країни, щоб навчатись у коледжі, та два роки поспіль подорожував разом з членами панк-гурту на літніх канікулах. Дістався до Сіетлу, вони оселились у Керрі.

Тепер Psychedelic Warlord жив у Нью-Йорку та працював на інтернет-провайдера. Він покінчив з хакінгом і не відвідував формальні заходи. Натомість у п'ятницю він зустрівся з членами групи у Пак-Білдинг, де проводилася конференція, та пішов з ними на вечірку. Керрі — коротке біляве волосся, чорна помада — познайомила його з Джоном, Семом, подругою групи Лімор Фрід й іншими, хто приєднався до cDc після нього. Вони пригадали старі часи. Psychedelic Warlord поцікавився,

чи працює ще електронна дошка *cDc*, *Demon Roach Underground*. Хтось набрав номер модему Кевіна та передав телефон Warlord, щоб він почув звук спроби підключення — доказ, що дошка досі існує.

[x x]

В останній день конференції Oxblood Ruffin був у центрі уваги лише кілька хвилин. Більшість слухачів цікавив хакінг, а не китайська політика. Популярна преса ще не захопилася питаннями безпеки, а *cDc* ще не зажила слави, що надійде завдяки Back Orifice. Тому медіа майже не виявили інтересу до заходу. Один молодий репортер, Ерік Гессельдаль, зацікавився темою і відтоді надокучав Oxblood Ruffin запитаннями. Пів року по тому він написав коротку статтю про «Блондинок» у журналі *Wired*[7], згадуючи, що, як заявив йому Oxbood Ruffin, вони вивели з ладу китайський супутник. Пізніше Гессельдаль говорив: «Зважаючи на божевільну історію взаємовпливу хакерів, антиістеблішменту й типів контркультури на Заході у 1970-ті, це не був стрибок віри, хоча, я вважаю, “надія” — точніше слово, що схожі події відбувались у Китаї».

У той час як більшість активних членів *cDc* була у захваті від роботи Джоша Бухбіндера над *Back Orifice*, Лейрд продовжив спілкуватися з Гессельдалем, який наполягав на знайомстві з будь-яким членом дисидентської групи. Лейрд відмовив, але сказав, що може передати запитання від імені репортера. Це перетворилося на повноцінний текстовий файл у формі інтерв’ю між Лейрдом під ніком Oxblood Ruffin і дисидентом, якого він назвав Блонді Вонг.

Лейрд написав, що розмова відбулась у барі[8] *Ted's Collision & Body Repair* в Торонто. Переважно йшлося про створену Блонді підпільну мережу технологічно обізнаних бунтівників у Китаї, яка минулоріч збільшилася на двадцять членів, багато в чому завдяки порадам хакерських груп, серед них і «Культу мертвої корови». «Коли я зрозумів, якого впливу "Культ мертвої корови" набув у хакерському світі та як усе влаштовано, зміг узяти з цього найкраще та використати для нашої боротьби»,— розповів Блонді. Вони обговорювали телесеріал «Сайнфелд», Брюса Лі, моду та проблему соціального відчуження у старших класах. Але жартівлива розмова затягнула легковажних читачів, щоб увести їх на темну територію: вбивство батька Блонді Червоною Гвардією Мао та студентів-протестувальників на Тяньаньмень. Блонді сказав, що жорстокі репресії змусили його залишитися за кордоном і звідти допомагати своїм співвітчизникам. Він закликав читачів до самоосвіти, попросив вести торгові відносини залежно від поліпшень у становищі прав людини та викривати чи навіть зламувати американські компанії, які співпрацюють з Китаєм. «Якщо люди хочуть брати в цьому участь, мають застосувати свої навички»,— сказав Блонді.

Лейрд передав попередню версію запису інтерв'ю Гессельдалю як ексклюзивний матеріал, знаючи, що це зробить статтю привабливішою. Гессельдаль знову подав свій матеріал у *Wired*, але отримав відмову й врешті-решт домовився з його онлайн-відгалуженням — Wired News. Звідти історія набула неймовірного поширення. Попри інтернет-бум, висвітлення технологічних тем було для більшості

журналістів у новинку, і майже ніхто не розумівся на комп'ютерній безпеці. Але це не стосувалося *Wired News*. Її репортери знали про технології, безпеку та «Культ мертвої корови». Тому коли репортери з популярних видань прочитали статтю *Wired News* про «Гонконгівських блондинок», вони припустили, що журнал перевірив свої джерела та знає, про що - говорить.

Перша реакція членів *cDc* на текстовий файл Лейрда була неоднозначною, але більшість була вражена. Вони повірили історії, тому що її подробиці збігалися з тим, що він розповів їм раніше. Але Кевін і редактор текстових файлів Міша, чию репутацію було поставлено на кін, відчули щось підозріле. Переглядаючи текст перед публікацією, Кевін написав: «Інтерв'ю з Блонді Вонгом чудове. Наскільки воно справжнє?» Лейрд відповів: «На три чверті справжнє, решта — теревені». Міша, якому належало відредагувати файл, був різкішим у своєму листі до Лейрда. «Здебільшого він [Блонді] не розуміє деякі з твоїх комічних зворотів мовлення і висловлюється дуже формально, обережно, а потім зненацька говорить щось типу "Той хлопець — ідіот. Хочу сказати, якщо мені потрібна порада від голови партії щодо орального сексу з молодою дівчиною, я сама увага". У мене запитання: це інтерв'ю справжнє? Чи ти написав за обидві сторони?»

Але попри всі свої сумніви Міша був загнаний у кут. Лейрд уже передав файл Wired News, який використав його для публікування власної статті. «Як лідер хакерської групи "Гонконгівські блондинки"[9] Вонг мав чим підкріпити свої загрози,— писав Гессельдаль.— «Гонконгівські блондинки» заявляють, що виявили

істотні діри в безпеці комп'ютерних мереж китайського уряду, особливо систем, пов'язаних зі супутниковими комунікаціями». Було б страшенно дивно, якби *cDc* не оприлюднила свою сенсаційну новину. До того ж Міша вважав, що стаття може підвищити обізнаність, і в минулому він неодноразово брав участь у жартах над медіа. Він вишліфував інтерв'ю Лейрда та розмістив його на сайті *cDc*.

Після появи статті у *Wired News* на зв'язок вийшла Наомі Кляйн. Успішна канадська журналістка особливо цікавилася Китаєм. Клінтон прагнув нормалізувати відносини[10] й применшити значення прав людини й щойно здійснив перший президентський візит у країну після подій на Тяньаньмень. Лейрд написав групі: «Вона вважає нас праведною політизованою машиною хакінгу, яка працює заради миру в усьому світі чи чогось такого... Хай там що, вона дуже нам допоможе». Він мав рацію. Докладний огляд Кляйн[11] у *Toronto Star* повідомляв, що «"Блондинки" — це хакерське крило китайського продемократичного руху, розкидане по всьому світу й вимушене працювати з підпілля після подій на Тяньаньмень. 7 липня, за лічені дні після повернення Білла Клінтона з Китаю, керівник "Блондинок" під псевдонімом Блонді Вонг зустрівся з хакером Oxblood Ruffin, і вони вийшли на світло з новим рівнем політичного хакінгу». Повідомлення Кляйн підхопили багато інших видань. Вона напише декілька книжок, як-от *No Logo: Taking Aim at the Brand Bullies*, у якій теж процитує Блонді Вонга.

Здавалося, історія прийшла з майбутнього. Вона кочувала з сайту на сайт ще молодої мережі,

неймовірна розповідь про майстерних, таємничих хакерів, які допомагають героїчним борцям за права людини в тоталітарному світі. Хоча ніхто, крім Лейрда, не заявив, що був у контакті з Блонді — якого різні версії описували як астрофізика та торгівця валютою — або має якесь інше підтвердження його існування, вийшли нові статті, появі яких посприяла наївність репортерів і той факт, що перед тим *cDc* затвердилась у національних медіа як елітний клуб гуру хакінгу.

cDc була у повному захваті та зробила «Блондинок» етичним обґрунтуванням своєї роботи. Виступаючи на *Def Con* у день презентації Back Orifice та рік по тому — *Back Orifice 2000*, Кевін згадав «Блондинок» як головний приклад того, за що бореться група. Коли Microsoft припинила відкидати програму *Back Orifice* як іграшку та почала називати її небезпечною й критикувати *cDc* за її випуск, Люк випустив пресреліз, у якому пов'язував компанію з Китаєм і натякав, що хактивісти використовують *Back Orifice* для атак на бізнеси, що сплуталися з репресивним режимом.

Чи був публічний реліз Back Orifice аморальним[12]? У Microsoft були б тільки раді, якби споживачі повірили, що ми погані хлопці та що вони — як постачальники цифрового решета — ніяк за це не відповідають. Але питання моралі частіше відносні, ніж абсолютні. Тому, щоб спростити ситуацію, ми спрямуємо нашу культуру та дії проти них, і нехай громадськість вирішує, хто з нас має кращий вигляд у чорному. Ми хочемо спитати Microsoft, чи, точніше, Білла Ґейтса, чому 1996 року він стояв пліч-о-пліч з китайським головою Комуністичної партії, яка засудила будь-яке обговорення прав людини в Китаї на річному засіданні

Комісії ООН з прав людини в Женеві? Чи спиралося рішення підлизатися до найбільшої тоталітарної держави на деяку високу моральну позицію, чи було просто зручніше наступити на людську порядність і заробити більше грошей?

А тепер повернімося до Back Orifice. Чи було б аморально використати цей інструмент для негідних цілей стосовно мереж з Windows? Чи було б аморально, якби Back Orifice потрапила в Китай і скаламутила найбільший цільовий ринок Microsoft? Чи варто хактивістам використати Back Orifice як форму протесту проти мультинаціональних корпорацій, які поділяють точку зору Microsoft «гроші понад гідність»? Життя коротке, і всіх нас судитимуть за нашими вчинками. Тому вдіяли ми правильно чи ні, вирішувати історії та людській совісті. Але якщо боги захочуть прокляти нас за те, що ми принесли вогонь з гори, ми сядемо поруч із Прометеєм і матимемо справу з наслідками. Зрештою, КУЛЬТ МЕРТВОЇ КОРОВИ не вважає, що світу судилося бути поганим місцем.

Група ретельно працювала над медійною стратегією, сполучаючи репортерів з історіями та членами, яких цитували найчастіше. Лейрд наполягав, щоб вони вживали слово хактивізм незалежно від того, про що йдеться. «Якщо десять різних журналістів подадуть матеріал з тим самим словом, воно [хактивізм] дуже швидко ввійде у загальний лексикон,— написав він у поштовій розсилці в липні 1998 року.— Переходьте до їхньої теми лише після того, як скажете те, що хочете, потім торкніться їхнього запитання, якщо воно варте відповіді, чи повністю проігноруйте...». Стратегія

спрацювала набагато краще, ніж він міг собі уявити. У січні 1999 року поважна авторка з Китаю написала тематичну передову статтю[13] у Los Angeles Times про різні способи використання мережі демократичними активістами в Китаї. Вона назвала cDc і «Блондинок» групами хактивістів, які борються з проєктом «Великий китайський файрвол» і процитувала слова Oxblood Ruffin та гіпотетичні заяви Блонді Вонга.

[x x]

Не вся преса була одержима сагою про «Гонконгівських блондинок». У *Back Orifice* була чітка історія, за участю великої кількості експертів, з публічними демонстраціями та попередженнями великих компаній про небезпеку. «Гонконгівські блондинки» не мали підтверджень. Маючи лише слова Лейрда, найвідповідальніші видання не друкували нічого. Атакований проханнями журналістів улаштувати зустріч з Блонді Вонгом для написання власного матеріалу, Лейрд сказав, що той зник. У грудні 1998 року, якраз перед виходом статті у *Los Angeles Times*, він написав ще одну розповідь про їхні відносини. У текстовому файлі *cDc* № 361 він повідомив, що три роки тому випадково зустрів Вонга на вечірці[14], що вони за кілька годин спільно розробили організаційну структуру «Блондинок» і що Вонг нещодавно переїхав до Індії, здебільшого щоб працювати з південно-азійськими програмістами.

Далі Лейрд змінив тему, наводячи незаперечні докази порушень прав у Китаї та посилено розхвалюючи софт з відкритим кодом як той, що несе більше потенціалу

поліпшення життя, ніж західні уряди чи компанії. Також він назвав імена справжніх китайських активістів і сказав, що хактивісти можуть у різні способи допомогти їм. Вони можуть привезти *Back Orifice* до Китаю для використання проти корумпованих партійних службовців і допомогти у привертанні уваги. У своєрідному прогнозі він сказав, що хактивізм могутній і полягає переважно в розповсюдженні знань у новому типі конфлікту, «інформаційній війні, у якій інтернет-меми змагаються за частку людської уваги та рейтинги замінюють кількість слухачів».

Хакери й активісти взяли історію «Блондинок» до уваги, і деякі нанесли шкоду китайським урядовим вебсайтам. Одна група американських хакерів, *Legions of the Underground*, у грудні 1999 року звернулася до своїх союзників із закликом зруйнувати комп'ютерні мережі в Китаї та Іраку. За лічені дні *cDc* розмістила заяву-відповідь[15] спільно з *L0pht*, *Phrack* і німецькою хакерською спільнотою *Chaos Computer Club*. «Хоча ми, можливо, погоджуємося з *Legions of the Underground*, що злодіяння в Китаї та Іраку повинні зупинитися, ми не згодні з методами, за які виступає група,— говорилось у заяві.— Не можна справедливо сподіватися поліпшити вільний доступ нації до інформації руйнуванням її мереж... Якщо хакери заявляють про себе як про зброю, хакінг загалом розглядатиметься як акт війни». *Legions of the Underground*, члени якої не мали внутрішньої згоди[16] щодо цього, сприйняла попередження серйозно та вирішила відкликати атаку.

cDc спробувала переспрямувати енергію на захист. Лейрд працював з кількома іншими політично активними

членами групи над створенням підрозділу *cDc* під назвою *Hacktivismo*. Він плекав проєкти з обходу цензури й безпечних комунікацій, хоча жоден з них, здавалося, не досяг критичної маси. Тим часом провідні технологічні таланти *cDc* більше зосереджувалися на своїй основній роботі. Зокрема Мадж і Крістіан Ріо повели *L0pht* у приголомшливо новому напрямку. Вони та решта групи організували її придбання комерційною компанією та взяли венчурні гроші, щоб вийти на повністю професійний рівень. Релізи новин і софту *cDc* уповільнилися, і на літніх хакерських зборах 2000 року була вистава й стримані повідомлення, але мало свіжих інструментів, новин чи натхнення.

Деякі хакери нарікали, що Лейрд зруйнував *cDc*, політизувавши її, і дехто порушував серйозні питання щодо «Блондинок». Понад десятиліття по тому Лейрд пригадав цю історію[17] в дописі в *Medium*, кажучи, що ніколи не зустрічався з кимось, крім Блонді, та вигадав деякі частини історії, щоб захистити його. Він продовжує наполягати, що принаймні Блонді існував. Але журналіст Гессельдаль поступово усвідомив, що його пошили в дурні. Двадцять років по тому він сказав таке: «Завдяки цим історіям у наукових та інтелектуальних колах відбулися деякі цікаві й конструктивні дискусії про те, як хакери й активісти можуть допомагати одне одному. Якщо ті обговорення в якийсь спосіб спричинили позитивні зміни у світі, це прекрасно. Але мене це не виправдовує».

Навесні 2001 року на розповідь Лейрда про Блонді Вонга натрапив один британець, який переїхав до Індії. Грег Волтон був трохи хіпі, коли залишив одноманітну роботу у Великій Британії заради Північної Індії, де

знайшов спосіб відволіктися. Із розквітом мережі у наступні кілька років Волтон подумав, що міг би допомогти консультаціями з прав людини та розробкою вебсайтів для тибетців у Дармсалі, фактичної столиці тибетського народу у вигнанні. Він сидів в офісі культурного закладу й читав під час перерви текстові файли, коли виявив оприлюднену три роки тому розповідь Лейрда про Блонді Вонга. Волтон не міг стриматися. Канадський обізнаний у технологіях активіст у змові з переслідуваними китайськими дисидентами. Тибетцям була потрібна така допомога. Щодня на них обвалювалися тонни фальшивих імейлів та електронних махінацій усіх типів з боку Китаю, який був рішуче налаштований дискредитувати Далай-ламу та завадити його лідерській ролі серед етнічних тибетців, які ще проживали на китайській території. Волтон написав Лейрду електронного листа з подякою за його роботу й запитанням, чи знає він когось, хто міг би допомогти з жалюгідним становищем інформаційної безпеки тибетців.

Лейрд спитав, чим займається Волтон, і пообіцяв поміркувати про допомогу. Однак спочатку він запросив Волтона приїхати того літа до Лас-Вегасу та приєднатися до панелі на *Def Con*, присвяченій потребі в кращій безпеці задля прав людини. *cDc* вирішила серйозніше взятися до ідеї хактивізму.

Волтон приїхав до Лас-Вегасу та провів багато годин у готелі *Hard Rock* через дорогу від місця проведення конференції, з Лейрдом і групою інших хакерів. cDc контролювала панель і запросила повного натхнення кандидата для головної дискусії — Патріка Болла, заступника проєкту з захисту прав в Американській

асоціації сприяння розвитку науки. Болл був першокласним програмістом й одним із перших, хто робив те, про що говорив Лейрд та інші члени *cDc*. Кинувши магістратуру 1991 року та переїхавши до Ель Сальвадору, Болл переміщувався від однієї проблемної країни до іншої, методично розробляючи програми, встановлюючи захисну криптографію та збираючи бази даних про деякі найжахливіші порушення прав людини у світі. 1998 року він виступив на конференції «Комп'ютери, свобода та приватність» в Остіні та дискутував про політику криптографії зі службовцем Міністерства юстиції, який хотів бекдорів і слабкого шифрування. Там він познайомився зі спонсором списку розсилки Cypherpunks і співзасновником *EFF* Джоном Гілмором і Філом Циммерманом, розробником шифрувальної програми *PGP*, який теж бився з федеральним урядом. «Я назавжди подружився з ними»,— казав Болл.

У Лас-Вегасі Болл та інші виступали в наметі, встановленому на даху готелю, тому що жодна зала не могла вмістити всіх присутніх. Це була найбільша аудиторія, перед якою він колись виступав,— мабуть, близько семисот осіб. Болл повідомив зачарованим слухачам, що тільки в Ель Сальвадорі його команда зафіксувала дев'ять тисяч розповідей свідків з описами тортур, викрадень і позасудових страт. Він зібрав дві бази даних,— зі злочинами проти сімнадцяти тисяч жертв та з кар'єрами тисяч військових,— а потім з'єднав їх і встановив, які службовці продовжували фігурувати у випадках найжахливіших порушень. Він виявив сотню найпримітніших — на руках чи під контролем кожного з цих людей налічувалося понад сто очевидних злочинів — і добувся їхнього звільнення. Технологічно

розвинена кампанія Болла продовжилася на Гаїті, у Гватемалі, Південній Африці та Сербії, де він виявив незаперечні докази геноциду, посприяв вигнанню з країни деяких з найбільших злочинців і змінив підручники історії.

Тепер Болл закликав присутніх теж допомогти — написанням листів до *Amnesty International* від імені політичних в'язнів, приєднанням до груп інтересів, які борються з обмеженнями на користування інтернетом, дослідженням безпеки або приділенням часу проєктам на зразок *Peekabooty*, розробленого *cDc* браузера, що захищає конфіденційність. Болл сказав, що «хактивізм — це шукання способів донести до держави правду». Лейрд і Волтон приєдналися до Болла в обговоренні *Hacktivismo*, підрозділу *cDc* з новою програмною заявою щодо прав людини. Схожа за своєю формою на резолюцію ООН і датована 4 липня 2001 року «Декларація Hacktivismo»[18] цитувала Статтю 19 Загальної декларації прав людини, за якою кожна людина має право на свободу переконань і на вільне їхнє виявлення, і це право включає свободу одержувати інформацію. Декларація *Hacktivismo* виголошувала великими літерами: «Підтримувана державою цензура інтернету — серйозна форма організованого та систематичного насильства над громадянами з метою спричинити замішання та ксенофобію, і це варте догани порушення довіри». *Hacktivismo* пообіцяв застосувати технології для боротьби: «Ми вивчатимемо способи обійти підтримувану державою цензуру інтернету й використаємо технології, щоб кинути виклик порушенням права на інформацію».

Лейрд написав перший варіант тексту у квартирі Кевіна в Гарлемі та, поки обмірковував постійну назву, охрестив його «Гарлемською декларацією». Її було ретельно складено з допомогою Люка, Міши й інших. Лейрд порадився і з юристами, як-от членом *cDc* Ґленном Курцроком, який був прокурором на Лонг-Айленді, та Сінді Кон — вона працювала за контрактом н*а Electronic Frontier Foundation* і пізніше очолить її. Кон допомогла Лейрду поєднати моральний авторитет з легітимністю ООН, щоб охопити максимально можливу аудиторію, не провокуючи осудження урядів. Головною ідеєю було процитувати не лише Загальну декларацію прав людини, яка мала рекомендаційний характер, але й Міжнародний пакт про громадянські та політичні права, який був менш відомий, але мав силу договору. «Я написав “Гарлемську декларацію” не для того, щоб проповідувати новонаверненим,— заявив Лейрд, пояснюючи іншим деякі свої рішення.— Якби це було так, написав би щось типу “Лі Пен — недолюдок, який хоче зруйнувати інтернет”[19]».

У публічному дописі з відповідями на поширені запитання[20] Лейрд й інші головні члени *Hacktivismo* написали: «Головною метою було процитувати деякі визнані на міжнародному рівні документи, які прирівнюють рівний доступ до інформації до громадянських і політичних прав; однозначно заявити, що розважливий доступ до законно оприлюдненого матеріалу в інтернеті є базовим правом людини; що ми відчуваємо огиду до політичного лицемірства та корпоративної жадібності, яка створила цю ситуацію; і що ми виявляємо ініціативу й дещо робимо щодо цього».

Панель *Def Con* 2001 року була визначальним моментом для тих, хто стояв на сцені, та для багатьох слухачів. Якщо Лейрд раніше був епізодичним пропагандистом, провокатором-дилетантом, Болл був видатною фігурою, і він вразив хакерів на *Def Con* у саме серце. Наступного року він давав свідчення щодо військових злочинів на суді сербського диктатора Слободана Мілошевича в Гаазі. Мілошевич, який був сам собі за адвоката[21], хотів дискредитувати Болла й на перехресному допиті спитав: «Містере Болл, ви були в консультативній раді хактивістської групи міжнародних хакерів? Ви належите до керівництва групи, відомої як “Культ мертвої корови”?» Болл відповів, що він просто консультував членів *cDc* у їхніх «зусиллях допомогти молодим програмістам кинути незаконну діяльність і спрямувати свою енергію на продуктивну й законну діяльність», як-от захист прав людини.

Волтон був на зв’язку з Лейрдом і допоміг йому отримати роботу з організації в Дармсалі конференції з бездротових технологій, які здатні розширити доступ тибетців до інформації, водночас гарантуючи їхню безпеку. Лейрд переконав у своїй думці світил технологій, які привернули більше людей до конференції й надихнули інших допомогти тибетській спільноті. Волтон став набагато краще розуміти сутність загроз тибетцям, і його прагнення захистити тих, кому він служив, посилилося. Тим часом західна розвідка уважно спостерігала за тибетцями, адже кращий інформаційний захист означав, що китайці спробують витонченіші атаки. Щойно гра розкрутилася, розвідники зрозуміли: те, що китайці влаштовують тибетцям сьогодні, завтра очікуватиме великих військових підрядників США, як-от

Lockheed Martin. Волтон тримав агентів у курсі. «Якщо ті самі шкідливі програми зв'язуються з сервером команд й управління, який атакує комп'ютери військових підрядників і монастирів у Дармсалі, це доволі чітка вказівка, що за цим стоїть Китай,— сказав Волтон.— Тому я поділився інформацією з кількома національними розвідувальними агентствами. Лейрд теж мав гарні зв'язки з ними».

Насправді Лейрд мав більше зв'язків з розвідувальними колами, ніж усвідомлювала більшість членів *cDc*. До того як запросити Болла виступити на панелі *Def Con*, яка найбільше популяризувала ідею хактивізму, він обмірковував участь Джеймса Малвенона. Малвенон, військовий підрядник у *RAND*, був спеціалістом з Китаю і зосереджувався на допомозі розвідці США, а не пригнобленим китайським громадянам. Вони познайомилися після виходу статей про «Гонконгівських блондинок», коли Малвенон шукав докази використання мережі китайськими дисидентами. Але в ті дні китайські інтернет-акаунти досі були рідкісними. Малвенон подорожував материковою частиною Китаю й уважно вивчав хакерські групи. Він виявив: ті, що були хоч трохи політично обізнані, наприклад груп*а Honker Union*, часто діяли за вказівкою уряду.

Малвенон не виявив нічого схожого на те, про що писав Лейрд. Але ідея була такою привабливою, що люди в розвідці США почали відстоювати її як мету. «"Гонконгівські блондинки" були частиною історії, яка надихнула людей вірити в існування моральної місії»,— казав один офіцер розвідки, який познайомився з Лейрдом. За президента Барака Обами американський уряд розпочне власну програму, розповсюджуючи

інструменти для інтернет-з'єднання без цензури. Цю програму, неофіційно відому як «інтернет у коробці»[22], відстоював інноваційний радник Держдепу Алек Росс, який відмовився сказати, скількох країн вона досягла.

Тим часом Лейрд часто спілкувався з Малвеноном й особисто розповів йому про щонайменш один проєкт *cDc* з обходу цензури. Це був план спрямувати запити на вебсторінки через браузери інших користувачів, щоб створити плутанину, хто та які сторінки передивляється. Лейрд і Мадж були не єдиними членами *cDc*, близькими до розвідувальних служб. Адам О'Доннелл, відомий як Javaman, теж працював на проєкт ЦРУ[23] зі зворотного інжинірингу «Великого китайського файрволу» — системи, яку Китай використовує для контролю внутрішнього та зовнішнього інтернет-трафіку. Адам приєднався до *cDc* 2004 року. Після навчання в Центральній середній школі Філадельфії та коледжі він був стажувався в *Lucent Technologies*. Крім того, він відвідував заходи журналу *«2600»* в Нью-Йорку. Там йому допомогли зустрітися з хлопцями з *L0pht* у Бостоні. Пізніше, у Каліфорнії, він працював на антиспам-компанію *Cloudmark*, засновану членом хакерської групи *w00w00* Джорданом Ріттером, до того як 2009 року стати співзасновником сек'юріті-фірми *Immunet*.

Створені Адамом зворотні проксі-сервери дали людям у США змогу створити враження, наче вони перебувають у Китаї, тому вони змогли дізнатися, що саме блокує файрвол. Це також спростило обмін інформацією між тими американцями та людьми, які дійсно перебували в Китаї. Зрештою ЦРУ отримало кращу можливість спостерігати за дисидентським

трафіком чи зламувати китайські мішені, не здіймаючи тривогу.

Здавалося, допомогати людям у Китаї й отримувати деякий заробіток від уряду — це гідна справа, але іноді вона залишала Адама з неприємним відчуттям. Одного разу він мав забрати платіж у забігайлівці в Дюпон-Сьоркл, районі Вашингтону. Чоловіки, з якими він зустрівся, були небагатослівні, але дали йому паперовий пакет з 20000 доларів готівкою. Коли Адам спитав, чи потрібна їм розписка про одержання, вони лише розсміялися. «Не за щось менше як сто тисяч»,— сказав один із них.

Поки деякі члени *cDc* намагалися залучити уряд, щоб просувати свободу та безпеку в інтернеті, інші сподівалися робити добрі справи, скориставшись інтернет-бумом.

Розділ 8.
СТАВКИ РОСТУТЬ

Початок 2000 року відзначився абсолютним піком «бульбашки» доткомів. Хоча сек'юріті-компанії аж ніяк не були чинником божевілля на фондовому ринку чи жадібності до венчурного капіталу, вони отримували користь, працюючи на *AOL*, *Yahoo*, комп'ютерні фірми, підприємства електронної торгівлі та інших. Деякі компанії наймали жменьку талановитих тестувальників, які проникали в комп'ютери клієнтів з їхнього дозволу, а потім надавали рекомендації з закриття виявлених дірок. Гігантські консалтингові фірми, у яких працювали люди з різноманітними здібностями, були більш розповсюджені. Ще існували великі антивірусні компанії на кшталт *Symantec* і *McAfee*. Їхні продукти були кращі, ніж нічого, а їхні бізнес-моделі дозволяли гребти гроші лопатою. Компанії стягували зі споживачів і підприємств річну плату та блокували ті віруси, які могли. Якщо комп'ютер клієнта все одно інфікувався, компанії додавали до бази даних нову сигнатуру, щоб той самий вірус не потрапив до наступного користувача — якщо між зараженнями вірус трішки не змінювався, а саме так і відбувалося. На жаль, внесення дрібних змін до вірусу було тривіальною справою для хакерів, які націлювалися на конкретну жертву, і дуже швидко такі зміни стали автоматичною частиною масштабніших атак.

Компанії заробляли гарні гроші на захисті, але загалом були неспроможні убезпечити споживачів. Навпаки, у міру того як бізнеси поєднували різний софт, обладнання та мережі, стан безпеки тільки погіршувався, тому що кожна програма будь-якого розміру мала критичні вади, якими міг скористатися нападник. Підвищена складність допомагала хакерам. Але постачальникам софту бракувало стимулів, які спонукали звичайних виробників створювати безпечніші продукти. Компанії-розробники переконали суди, що закони про відповідальність за якість продукції до них не застосовуються. З формальної точки зору вони не продавали, а ліцензували свої продукти, та змушували користувачів відмовлятися від права на позов на момент інсталяції. Найбільші споживачі могли спробувати вимагати допомоги, вдаючись до угод про обслуговування чи аудиту коду. Але навіть якщо вони здобували право дослідити код на наявність дефектів, вони не мали права попередити споживачів про свої знахідки. Що більш важливо, у найголовніших продуктів було небагато гарних альтернатив, і всі вони мали слабкі місця. Безпека не була переважним критерієм вибору програм навіть для найбільших компаній. У найліпшому разі вони заохочували співробітників використовувати проєкти з відкритим кодом, як-от *Linux*.

Не бажаючи несподіванок з боку влади, команда *L0pht* дійшла висновку, що наступний найкращий спосіб підвищити безпеку світу — переконати найбільших виробників софту вчинити правильно, навіть якщо вони не повинні цього робити. Влаштований «Культом мертвої корови» публічний конфуз найуспішніше переконав *Microsoft* поставитися до питань безпеки серйозніше. Але *Microsoft* була лише однією компанією,

й осоромлення бізнесів не приносило *L0pht* грошей. Отримуючи невеликий дохід від продажу інструментів, як-от для зламування паролів, *L0pht* не міг масштабуватися. Тому Мадж та деякі інші замислилися, чи можуть вони якось отримати запрошення до компаній-розробників, щоб принаймні щось поліпшити. Крім того, вони могли б консультувати великі банки та інших споживачів, надаючи їм засоби для вимагання від постачальників кращого софту. Достатньо нового бізнесу — і можна найняти більше хакерів. Якщо *L0pht* зробить це правильно, зможе працювати і з продавцями, і з покупцями та захистити мільйони людей.

Мадж не був упевнений, що інші члени команди поділять його думку, але він не міг залишити все як є. Він, Крістіан Ріо та Кріс Вісопал писали більшість програм *L0pht*, які приносили гроші,— інструменти для сканування мереж, зламування паролів тощо. Але це означало, що їм доводилося працювати над поліпшенням тих програм, навіть якщо вони хотіли дослідити щось нове. Втомившись від цього тягаря, Мадж запропонував отримати зовнішні інвестиції від венчурної фірми, щоб усі могли робити те, що їм подобається. Знаючи, що це викличе роздратування в деяких пуристів, які бралися до хакінгу заради хакінгу, а не грошей, Вісопал заявив, що отримувати за це плату набагато краще. «Мабуть, зробити це було неможливо, та ми тішилися ілюзіями, що здатні вирішити це завдання»,— казав він. Для Маджа це було збільшення масштабу в дусі Кевіна Вілера — розповсюдження інформації про те, наскільки певні речі небезпечні та як їх поліпшити. «У той час ми були найкращим гаражним гуртом у світі. І єдині люди, яких ти знаєш, це жителі твого кварталу та, можливо, їхні друзі,— сказав він.— Отже, ти отримуєш гроші від

лейблу звукозаписної компанії. Це тягне за собою й інші речі, але ідея розповсюджується».

L0pht не міг поскаржитися на брак зовнішнього інтересу. Першим логічним претендентом була *Cambridge Technology Partners*. Це консалтингова сек'юріті-група з деякою репутацією; вона щойно виступила у телешоу 20/20 в частині, де кембриджський хакер Джобі Бенджамін та інші на камеру проникли у великий неназваний банк. Зустрівшись із *Cambridge Technology*, члени *L0pht* запропонували, щоб компанія найняла їх для тесту на проникнення. У такий спосіб, пояснив Мадж, керівництво знатиме, на що здатний L0pht. Погодившись, *Cambridge Technology* зробила фатальну помилку. Після підписання останнього офіційного дозволу Джо Гранд увійшов у голосову пошту керівників і спробував використати найочевидніші чотиризначні коди для прослуховування повідомлень: 1234, 1111, 4321. Вони вмить дізналися, що *Cambridge Technology* збирається запропонувати для придбання *L0pht*, якою буде найкраща пропозиція, якщо першу відхилять, і, найнеприємніше, що керівники думають про членів групи. Насправді їм були потрібні тільки Мадж, Крістіан і Вісопал. Вони були розлючені відкриттям, проте отримали право розважитися. *L0pht* повернувся до переговорів з дивними вимогами, наприклад будинку на колесах *Winnebago*, як зробили герої хакерського фільму «Пограбування замовляли?». Потім вони поклали на стіл свій звіт з тесту на проникнення. Вони не були настільки підступні, щоб додати до нього цитати з голосової пошти, але було ясно, що сталося. Більше вони нічого не чули від *Cambridge Technology Partners*.

Підхід *Battery Ventures*, усталеної венчурної фірми, спрацював краще. *Battery Ventures* щойно фінансувала новоспечений стартап під назвою *@stake*. *@stake* найняв давнього сусіда по квартирі Люка Бенфі, Дейва Ґолдсміта з *Cambridge Technology*, та Віндоу Снайдер. Вони погодилися на угоду в 10 мільйонів доларів, за якою *L0pht* увійшов до складу *@stake* після свого закриття в січні 2000 року. Приблизно в той час украй схвильовані працівники відділу зв'язків із громадськістю повідомили медіа справжні імена Маджа, Крістіана та Вісопала[1]. Вони спробували відкликати інформацію, але було запізно. І все ж таки світові не настав кінець. Спеціалістів прийняли на посади вищих керівників, даючи старій команді *L0pht* свободу продовжувати свої дослідження. Хакери були настільки у захваті від *L0pht*, що *@stake* перетягнула кількох найкращих працівників АНБ у приватний сектор, і нова компанія стала дивним союзом галузевого таланту й грошей.

Але культура нечепур-бунтарів у ланці звичайних співробітників зіткнулася з культурою тих, хто сидів у костюмах, складаючи плани продажу та контролюючи бюджет. Серед тих бунтарів було багато сильних особистостей із підозрілим минулим. Деякі співробітники пропустили зустріч із великим клієнтом, тому що не спали всю ніч, виготовляючи наркотики. Інші зустрічі слід було пропустити, але вийшло інакше: один ветеран L0pht кохався з повією[2] у своєму кабінеті, її зад випадково натиснув кнопку на телефоні та приєднав їх до конференц-дзвінка з гендиректором фірми-клієнта. А пізніше колишній працівник потрапив у тюрму за участь в одній з найбільших розкритих крадіжок номерів кредитних карток.

На поверхню спливли й інші специфічні питання. Чи продовжить *@stake* практику *L0pht* з випуску сповіщень про небезпечні баги? Чи робитиме це тільки стосовно компаній, на які не працює як консультант? Якщо це не викличе сум'яття в компанії, яка їм платить, то інших це може небезпечно наблизити до вимагань: «Найміть нас, і ми мовчатимемо про ваш продукт». Хоча *@stake* продовжила традицію координованого розкриття, яку започаткував *L0pht*, з її політикою не все було добре. Баг, виявлений у софті, який не був клієнтським,— чи виявлений у програмах клієнта в неробочий час,— можна було розкрити, але його також могли застосувати для розвитку бізнесу. Баги у клієнтських програмах, знайдені протягом ділових відносин, не розголошували.

@stake мала швидко розібратися зі своєю політикою розкриття, тому що для основної роботи їх найняв не хто інший, як *Microsoft*. Попри минулий антагонізм, команда *@stake* справила величезне позитивне враження на Microsoft. Немов оперативна група зірок-детективів, вони інтуїтивно відчували приховані в коді проблеми. Вони відстежували зв'язки від одного продукту до іншого та звертали увагу на закономірності. Кілька версій *Windows* були значно безпечнішими завдяки *@stake*, і 2002 року Білл Ґейтс випустив меморандум із заявою, що зараз безпека є головним пріоритетом компанії.

Невдовзі *Microsoft* найняла Снайдер та інших досвідчених працівників *@stake*. Снайдер залишиться на три роки. На початку в компанії не було окремої особи, відповідальної за безпеку наступних версій операційної системи. Снайдер зголосилася на цю посаду. Їй досі доводилося боротися за питання, що мали фінансові наслідки, як-от затримка релізу заради

усунення багів. Сперечаючись із менеджерами щодо переходу версії на «золотий» рівень для масового релізу, вона сказала, що *Microsoft* слід спочатку усунути дві вразливості середнього рівня, тому що хтось зовні виявить їх і використає, щоб створити щось небезпечніше. Її не підтримали, а за кілька днів виявилося, що вона має рацію[3]. Після цього інші менеджери припинили сперечатися з нею. Снайдер залучила багатьох найкращих зовнішніх консультантів з безпеки і відповідала за *Windows XP Service Pack 2*, який помітно покращив становище компанії. Крім того, вона допомогла познайомити ізольованих керівників із зовнішніми дослідниками, заснувавши конференцію *Blue Hat*, на якій хакери виступали перед працівниками *Microsoft*.

Працівники та ветерани *@stake* ввійшли на нову територію й в інші способи, як-от за допомогою публікації дослідження, яке мало непередбачені наслідки. Девід Лічфілд, шотландець, який стане найвідомішим у світі експертом з безпеки баз даних, пішов зі *@stake* і тестував безпеку *SQL* бази даних для німецького банку[4], коли зіткнувся з більшими, ніж зазвичай, труднощами у проникненні. Він спробував надсилати окремі різноманітні байти та виявив той, що обвалив систему. Це призвело до нових експериментів і невеликої програми, яка, можливо, була здатна захопити базу даних. Подальше копирсання виявило безпомилковий спосіб експлуатації аналогічного слабкого місця. Лічфілд сповістив *Microsoft* і спитав, чи можна йому виступити з цього питання на *Black Hat*, професійнішій версії *Def Con*, яка тепер відбувалася трохи раніше останньої. *Microsoft* не бачила в цьому

проблеми: на той момент вона вже підготує патч. Під час виступу Лічфілд продемонстрував приклад коду та порадив усім установити патч. Шістьма місяцями пізніше невідомий кодер випустив *SQL Slammer* — самовідтворюваного черв'яка, який 2003 року вивів з ладу чималий шматок інтернету. Лічфілд припустив, що патч був установлений лише на 10 відсотках комп'ютерів. Багато компаній уникнули б шкоди, якби він не оприлюднив код. Тому Лічфілд вирішив у майбутньому тільки описувати такі небезпечні дефекти та не публікувати код, якщо в нього не буде впевненості, що майже всі встановили патч.

Головний технічний директор *@stake* Ден Гір ще раз перевірив готовність компанії говорити правду. 2003 року він став співавтором статті, у якій стверджував, що монополія Microsoft — це погано для безпеки. Команда Гіра заявила, що панування *Microsoft* зробило пошук її слабких місць доцільним для хакерів, тому що вони отримали б золотий ключ, який наділив би їх можливістю ввійти майже куди завгодно. Це було правдою, але й водночас провокацією, і вона відбулася, якраз коли підтверджена судом монополія Microsoft нарешті захиталася під тиском оновленої *Apple*. *@stake* без церемоній звільнила Гіра.

Єдиною справжньою проблемою *@stake* була математика венчурного капіталу. У *Battery Ventures* знали, що більшість компаній, у які вони вклалися, спіткає невдача, тому зосереджувалися на тих, яких вважали здатними принести «100-кратні» доходи, абсолютний успіх. Але *@stake* заробляла гроші консультуванням, і компанія ніколи б не змогла створити такі доходи. Щоб задовольнити своїх інвесторів, *@stake*

довелося б вирости до рівня найбільших фірм з управлінського консалтингу. *@stake* шкандибав до свого продажу 2004 року компанії *Symantec*, яка поступово поглинула його.

[x x]

Історія @stake була дивним вимушеним союзом двох потужних і швидких на розвиток сил — венчурного капіталу та хакінгу. За короткий період свого існування *@stake* створила надзвичайно важливий прецедент у сфері безпеки: аутсайдери можуть стати працівниками великих компаній і зробити системи й продукти безпечнішими. Мабуть, важливіше те, що хакери зі *@stake* розосередилися та в найближчі кілька років заснували багато нових компаній і очолили підрозділи безпеки в *Microsoft*, *Apple*, *Google* та *Facebook*.

Але ті самі роки розкрили психологічну роз'єднаність, що супроводжувала фізичне розсіяння. На конференціях *Def Con* з 1998 до 2001 року *cDc* побачила пік розвитку переконань хакерів. Щороку кількість відвідувачів зростала, вони були молодші, надсміливі та за один крок від масового визнання, якщо не великих заробітків. Той короткий період був так само важливий для технологічної культури, як Літо любові у Сан-Франциско 1967 року для хіпі. Присвячена хактивізму панель Лейрда Брауна влітку 2001 року встановила високу планку для ентузіазму такого роду й ідеалістичних прагнень захистити людей навіть від їхнього уряду.

Але будь-яка етика молодіжного протесту стикається з проблемою, коли її послідовникам потрібно знайти

роботу й оплачувати рахунки. Та проблема загострилася 2001 року, після великого удару — вибуху «бульбашки» доткомів. Не всі могли працевлаштуватися у *@stake* чи в інших спеціалізованих компаніях. Але був другий, сильніший удар, який розкидав молодих хакерів у різних напрямках на багато років: терористичні атаки на Всесвітній торговий центр і Пентагон.

Умотивовані переважно грошима вже звертали менше уваги на етичні квести, як-от веселощі та ігри у спробах примусити *Microsoft* до чесності. За кілька місяців після терористичних атак 11 вересня перед тими, кого здебільшого мотивувала мета, теж з'явився сильний кандидат на їхню увагу: об'єднання проти найгіршого нападу на американську землю з часів Перл-Гарбору. Це було правдою для звичайних хакерів, які отримували завдання від військових чи розвідувальних агентств, і навіть для найкращих розумів *cDc*, як-от Мадж.

У Маджа була репутація, тому що він навчив урядових агентів і вони користувалися його інструментами. Лідер урядової «червоної команди» Метт Девост, який захищав *cDc* у звіті, наданому президентській комісії з захисту інфраструктури, використовував інструменти *L0pht* для проникнення в урядові мережі. Шпигуни обожнювали *Back Orifice* та *Back Orifice 2000*, адже якщо вони не залишали слідів, ніщо не довело б відповідальність уряду США.

За два роки до атак 11 вересня підрядник розвідслужби, якого я називатиму Родрігесом[6], був у Пекіні, коли військові НАТО в розвалюваній Югославії скинули п'ять американських бомб на китайське посольство в Белграді. Загинули троє. Вашингтон швидко попросив

вибачення за те, що назвав помилкою у націлюванні, але китайці гнівалися. У зверненні на національному телебаченні тодішній заступник голови КНР Ху Дзіньтао засудив бомбардування як «варварське» та злочинне. Десятки тисяч протестувальників вийшли на вулиці, кидаючи каміння та штурмуючи ворота американського посольства в Пекіні та консульств в інших містах.

США хотіли знати, що далі робитиме розлючений натовп, але працівники посольства були заблоковані у своїх будівлях. Родрігес, який працював у Китаї як приватна особа, мав свободу пересування. Він зв'язався з другом у відділі ЦРУ з Китаю та спитав, чим може допомогти. Аналітик попросив Родрігеса з'ясувати, що відбувається, а потім піти в інтернет-кафе й перевірити, чи можна відправити доповідь звідти. Опинившись в інтернет-кафе, Родрігес знову зателефонував із запитанням, як щось передати, не потрапивши в пастку китайських міжнародних комунікацій. Аналітик спитав адресу кафе та розсміявся, коли Родрігес точно сказав йому, де перебуває. «Жодних проблем, вам нічого не потрібно надсилати,— пояснив він.— Там на всіх комп'ютерах *Back Orifice*». Щоб показати Родрігесу потрібне місце, він віддалено відкрив *CD*-дисковод одного комп'ютера. Потім прочитав усе, що написав Родрігес, і роздрукував доповідь про події в Пекіні. Родрігес стер свій текст і вийшов, не залишивши жодних записів.

Мадж ще до подій 11 вересня спілкувався з Річардом Кларком та іншими в Раді національної безпеки. Він часто відстоював конфіденційність. Наприклад, уряд хотів додати до всіх мобільних телефонів функцію відстеження місцезнаходження як частину системи

911[7]. Мадж запевняв РНБ, що втручатися в особисте життя громадян немає потреби, що інформації від веж стільникового зв'язку достатньо для будь-якої серйозної ситуації.

Одного дня в лютому 2000 року, після сплеску мережевих атак на великі вебсайти, Річард Кларк привів Маджа в Білий дім на зустріч з президентом Біллом Клінтоном і гендиректорами кількох компаній. «Гадаю, то була перша в історії зустріч у президента щодо кіберінциденту»,— сказав Річард Кларк, який організував її, щоб пояснити Білому дому відповідальність і аргументацію щодо ретельнішого урядового нагляду. Відповівши на запитання Клінтона, що можна виправити, а що не можна, гості вийшли з кабінету. Гендиректори побачили репортерів, що чекали на них, і приготувалися відповідати своїми найбільш цитованими банальними фразами. Але представники преси з'юрмилися навколо Маджа, бо навіть ті, хто його не знав, припустили, що хлопець із зовнішністю гітариста гурту *Megadeth* — це хакер, який прийшов на зустріч із президентом не просто так. Як сказав Кларк: «Звісно, Мадж перетягнув усю увагу на себе».

Але щоб бути сприйнятим серйозно, він мав говорити правду. Одного разу його запросив до себе службовець РНБ і спитав, що він знає про терористів та інші загрози. Що йому було відомо про Усаму бен Ладена? Про групу, яка організувала заринову атаку в токійському метро? Про «Гонконгівських блондинок»? На останньому запитанні Мадж зблід.

— Що ви маєте на увазі? — перепитав він.

— Нам сказали, що це маленька підривна група в Китаї, яка допомагає дисидентам з шифрованими комунікаціями.

— Я чув про них.

— Що ви можете повідомити нам? — наполягав службовець.

Мадж зрозумів, що уряд не вклав багато ресурсів в абсурдні пошуки, тому що інформація, яку отримала б розвідка та інші джерела, виявилася б нічим і переконала досвідчених професіоналів, що це оманний маневр. Але він не хотів, щоб країна марнувала енергію, яку можна було витратити на допомогу людям, що дійсно її потребують. Він знизав плечима, подивився своєму співрозмовнику в очі та визнав:

— Ми їх вигадали.

Після атак 11 вересня Мадж перевантажив себе роботою. Президента Буша попереджали, що кібератака буде гіршою, ніж літаки, і він прислухався. Відтак Мадж почав досліджувати, на що може бути здатен хакер-терорист — «одинокий вовк». «Я дізнався, що є способи вивести з ладу великі зони найважливішої інфраструктури. Основа була наче збудована з піску. Це вибило мене з рівноваги»,— пригадував він. Погляд у безодню посилив його тривогу, схильність до надмірного ескапізму та посттравматичний розлад — наслідок розбійного нападу, що стався з ним до роботи в L0pht і залишив його з травмою мозку. Він увійшов у штопор і врешті-решт не витримав. «Зрештою, я трохи збожеволів»[8]. Він провів багато днів під психіатричним

наглядом. (Патологічний стан тривоги та емоційне вигорання на тлі майже невиконуваного завдання з високими ставками — захист мереж — ще не визнавали серйозною галузевою проблемою, це станеться десятиліттям пізніше.) На жаль, дещо з терапії Маджа ускладнило ситуацію. Як буває з меншістю пацієнтів, заспокійливі препарати, що він приймав, мали протилежний ефект. Зрештою він звільнив своїх лікарів, поекспериментував з різними ліками й терапією та відновив здоров'я. Але коли він повернувся у *@stake* після багатьох місяців відсутності, йому було складно й нецікаво повертати свою посаду. Вибух «бульбашки» доткомів призвів до звільнень первинних працівників *L0pht*, тоді як менеджери отримували величезні зарплати. Увага загострилася на негативі.

Поза *@stake* хакери почали зникати на шість місяців чи навіть більше. Повертаючись, вони стверджували, що не можуть розповісти, чим були зайняті. Серед тих, хто тимчасово чи постійно пішов працювати на розвідувальні служби або Пентагон, було чимало найкращих хакерів, включно з кількома нинішніми чи минулими членами *cDc* або багатьма їхніми друзями у *Ninja Strike Force*. Вони хотіли захистити свою країну чи покарати «Аль-Каїду» і в багатьох випадках працювали в цікавих проєктах. Але багато хто не пройшов би перевірку біографії, потрібну для отримання допуску до даних найвищого ступеня секретності. Щоб обійти цю проблему, вони працювали на підрядників або субпідрядників. Так чи інакше, значна частина їхньої роботи була пов'язана з Афганістаном та Іраком.

Деякі хакери відчували велике задоволенння від урядової служби. Робота на уряд у світлі терористичних атак надавала їм шанс знайти своє місце там, де це було неможливо раніше. Їх об'єднувала спільна справа. Але для багатьох з цієї групи етична прозорість на початку закінчилася усвідомленням, що етика розвалюється на шматки, коли уряди б'ються з урядами. Так сталося з членом *Ninja Strike Force*, якого я називатиму Стівенсом[9]. Коли пішла погана слава про «Аль-Каїду», Об'єднане командування спеціальними операціями США почало наймати більше таких американських хакерів, як Стівенс. Деякі бойовики встановили клавіатурних шпигунів[10] в іракських інтернет-кафе, завдяки чому їхні керівники могли бачити, коли об'єкт заходить в спостережувані імейл-акаунти. Далі загін фізично відстежував об'єкт, коли той виходив, і вбивав його.

Після 9/11 військові перевели Стівенса до іншої країни та доручили всю комп'ютерну роботу: від налаштування серверів до зламування телефонів підозрюваних у тероризмі. Хоча він був технічним спеціалістом, маленькі команди були добре згуртовані, а їхні члени за потреби замінювали одне одного. Іноді щось ішло не так, і рішення, ухвалені на місці подій, змушували його робити те, до чого він був не готовий, зокрема й психологічно. Роки по тому, досі борючись із травмою, він пригадував: «Ми робили з людьми погані речі».

Інші мали схожий досвід[11]. Давній доповідач на хакерських і розвідувальних зборах, колишній священник Річард Тім, виступив з промовою про тягар захисту таємниць і провину, від якої страждають ті, кого

примусили виконувати аморальні накази. Після його прохання надіслати свої історії деякі слухачі поділилися схожими розповідями. «Я розмірковую, як жорстко кар'єрний шлях привів мене від ідеалістичного анархіста до корпоративної підставної особи, амбітного підприємця, радника військових/розвідки/сил оборони/правоохоронних органів,— повідомила одна людина.— Багато кіберхлопців починали з чогось геть іншого, аж раптом вони в центрі військово-промислового комплексу роблять те, до чого ніколи не готувалися». У такій ситуації зберігати таємниці «може бути вкрай складніше».

Інша людина написала:

Якщо людина вступає до розвідувальної служби на початку своєї кар'єри, їй дають прості завдання, для початківців — без травмувальних учинків чи глибоких етичних міркувань, з невеликою кількістю рішень. Із розвитком кар'єри таких вчинків/рішень поступово стає більше, майже непримітно для багатьох людей. Людина може раптом «прокинутися» та усвідомити, що не готова до цього і що тепер зайшла дуже далеко. Якщо це так, повертатися надто пізно.

Коли ви у вирі подій, сказав Тім, «правила, за якими люди нібито живуть, припиняють існувати». Він сказав, що розвідслужби відхиляють кандидатури тих, хто отримує надто високі бали на тестах на моральні якості, тому що добросовісний викривач гірший за ворожого агента.

[x x]

Робота на підрядника була лише одним способом, у який хакери з кримінальною біографією та ризикованими зв'язками могли співпрацювати з федеральними органами. Навіть не вдаючись до такого варіанту, вони могли робити щось близьке до суто дослідження безпеки за гроші. Для проникнення в багато важливих і складних об'єктів розвідки уряд потребував таємного знання вад програмного забезпечення. Ті вади мали бути досить серйозними, щоб зовнішні хакери мали можливість отримати контроль над комп'ютером-мішенню. І їм була потрібна програма-експлойт, яка скористається слабким місцем об'єкта й установить шпигунський софт. Агентство національної безпеки та меншою мірою інші частини збройних сил і ЦРУ роками таємно створювали сховища таких вад і експлойтів. Але їх потрібно було постійно поповнювати. Експлойти могли розкрити після застосування. Навіть якщо їх не розкривали, було небезпечно використовувати той самий спосіб десь іще, тому що мішень або третя сторона могла зрозуміти, що атаки взаємопов'язані, та дійти висновків, хто за це відповідальний.

Щойно американський уряд активізував свою шпигунську діяльність після 9/11, у нього виникла потреба у виявленні нових вразливостей, які вможливлять електронні проникнення. Їх часто називали «вразливості нульового дня», тому що на момент розголошення у виробника софту і його клієнтів було нуль днів на виправляння дефекту. Вразливість десяти днів менш небезпечна, адже в компаній більше часу на розробку та поширення патчу і більше шансів, що клієнти ним скористаються. Підвищений попит на вразливості нульового дня підштовхнув ціни.

Після цього хакери з найрозвинутішими навичками виявлення багів, котрі було не під силу знайти іншим,— самотужки або за допомогою спеціальних інструментів, — тепер могли заробляти на життя винятково цим.
А далі вони мали зробити вибір. Вони могли продати свою знахідку урядовому підряднику та сподіватися, що вразливість використають для атаки на об'єкт, до якого вони відчувають особисту неприязнь. Вони могли продати підряднику й вирішити не перейматися тим, для чого використають предмет угоди. Або вони могли продати ту вразливість посереднику, який контролював її подальший шлях. Деякі посередники заявляли, що продають тільки західним урядам. Іноді так і було. Ті, хто взагалі нічого не говорив про своїх клієнтів, платили найбільше. Вперше найкращим хакерам було відносно просто обрати етичну позицію та взяти відповідну плату.

Ніхто не був зацікавлений в описі цього ринку. Роль уряду було засекречено. Підрядники теж були зобов'язані зберігати таємницю. Клієнти посередників не хотіли уваги до їхнього ланцюжка постачань. І більшість хакерів не хотіла оголошувати себе найманцями чи малювати на собі мішень для інших хакерів чи урядів, які, можливо, були зацікавлені хакнути їх і зібрати легкий врожай вразливостей нульового дня. Отже, розвивалася «сіра» торгівля, яку підживлювали чутки на *Def Con* і в інших місцях, і вона залишалася прихованою від громадськості протягом десяти років. Перші статті у провідних медіа про бізнес вразливостей нульового дня[12] з'явилися незадовго до того, як 2013 року Едвард Сноуден розкрив, що це була фундаментальна частина практики уряду США.

Коли атакувальні можливості зросли, захист зіткнувся з серйозними труднощами. Фірми на кшталт *@stake* намагалися захистити найбільші компанії та, що більш важливо, змусити найбільших виробників софту поліпшити їхні продукти. Але так само як уряд, кримінальний світ з ентузіазмом відкрив для себе хакінг. Невеликі поліпшення в безпеці вносили до чорного списку адреси, що надсилали найбільше спаму. Це підштовхнуло спамерів найняти творців вірусів, щоб захопити тисячі неінфікованих комп'ютерів, які можна буде використати для обходу блокувань. І коли вони отримали мережі, відомі як ботнети, вони захотіли побачити, що ще з ними можна зробити. З 2003 року організовані злочинці, переважно в Росії та Україні[13], були відповідальні за більшість серйозних проблем з комп'ютерами в Америці. Оператори ботнетів використовували захоплені комп'ютери для запуску мережевих атак, які робили вебсайти недоступними, та вимагали за їхнє припинення грошей через *Western Union*. До того ж вони збирали банківські дані користувачів, щоб спустошувати їхні рахунки. А коли в них закінчувалися ідеї, вони здавали свої ботнети в оренду стороннім людям, які могли спробувати інші трюки. Поза тим міжнародне шпигунство набирало обертів. Іноді службовцям у їхніх пошуках допомагали союзники з кримінального світу.

Вихідці зі *@stake* поповнили лави і нападників, і захисників. Мадж вийшов зі свого некерованого штопору та пішов працювати в маленькій сек'юріті-компанії, потім на шість років повернувся у *BBN* як технічний директор проєктів для розвідслужб. Його колега у *@stake* і ветеран АНБ Дейв Айтель заснував *Immunity Inc*., продаючи інструменти, використовувані

урядами й корпораціями для тестування та шпигування. Він продавав вразливості нульового дня та зізнався в цьому пресі, а це зрідка робили в ті дні з етичних причин і через страх подальших запитань — хто клієнти та що вони роблять з інформацією. Айтель стверджував, що ті самі вразливості будуть виявлені іншими, тому немає підстав повідомляти цю інформацію постачальникам і дозволяти їм безкоштовно скористатися результатами його праці. З точки зору захисника, «щойно ви визнаєте факт існування багів[14], про які ви не знаєте, справа не в моменті часу, коли хтось розкриє інформацію про вразливість, а у ваших допоміжних засобах захисту»,— сказав Айтель, рекомендуючи інструменти виявлення проникнень, оновлені операційні системи та обмежувальні налаштування, які перешкоджають небажаній діяльності.

Лондонський вихідець зі *@stake* оселився в Таїланді, взяв собі нік Grugq і став найвідомішим у світі брокером вразливостей нульового дня. Роб Бек, який був співробітником *@stake* між посадами в *Microsoft*, переїхав до Фініксу та приєднався до Вела Сміта, знаменитого члена групи *Ninja Strike Force*, у спеціалізованій фірмі, яка працювала і з урядовими агентствами, і з компаніями. Вони ретельно обмірковували, до яких завдань беруться і для кого. «Ми пірати, а не найманці,— заявив Бек.— У піратів є кодекс». Вони відмовлялися від протизаконної роботи[15] й тієї, що мала б негативні наслідки для споживача. Один із основних керівників *@stake*, Кріс Дербі, 2006 року став гендиректором *In-Q-Tel*, венчурної фірми у Кремнієвій долині за підтримки ЦРУ, і Ден Гір приєднався до неї як головний спеціаліст

з інформаційної безпеки навіть без процедури допуску до засекречених даних. Пізніше Дербі очолив Endgame, військового підрядника, що продавав уряду вразливості нульового дня на мільйони доларів до того, як 2011 року вийти з бізнесу після викриття хакерами.

Крістіан Ріо та Кріс Вісопал заснували компанію *Veracode*, яка аналізувала програми на наявність дефектів, використовуючи автоматизовану систему, задуману Крістіаном для спрощення повсякденної роботи. Після *Microsoft* Віндоу Снайдер пішла працювати в *Apple*. У програмах Apple було менше дірок, ніж у *Microsoft*, але її споживачі були вразливіші, адже, як правило, мали більше грошей. Снайдер шукала в кримінальній екосистемі слабкі місця, де могла б завадити шахрайству. Однією з її інновацій була вимога про сертифікат розробника, який коштував 100 доларів, для інсталяції чогось на *iPhone*. Це була невелика сума, але достатня, щоб постачання шкідливих програм у старий спосіб стало для злочинців економічно невигідним.

Снайдер пішла далі та заявила, що злочинці менше націлюватимуться на користувачів *Apple*, якщо компанія зберігатиме менше їхніх даних. Але більший обсяг даних сприяв бездоганному користувацькому досвіду, головній темі *Apple*, і керівники тиснули на Снайдер, вимагаючи доказів, що це питання непокоїть споживачів. «Стало легше, коли люди почали з запалом обговорювати Сноудена,— сказала вона.— Коли вони дійсно розуміють ситуацію, їм не байдуже». Значною мірою завдяки Снайдер *Apple* запровадила нові методи, які, на велике розчарування ФБР, зробили айфони неприступними для поліції та для самої Apple. Вона

стала першою великою технологічною компанією, яка оголосила, що має вважати себе потенційним ворогом власних споживачів. Це був прорив у моделюванні загроз. Пізніше Снайдер очолила підрозділ безпеки в *Intel*.

Девід Лічфілд відкрито бився з компанією *Oracle* через її роздуті заяви про безпеку. Він підіймався кар'єрними сходами в підрозділах безпеки *Google* та *Apple*. Кеті Муссуріс зі *@stake*, союзниця *cDc*, деякий час залишилася працювати в Symantec, а далі перейшла в *Microsoft*. Вона переконала компанію приєднатися до інших постачальників софту в сплаті винагород хакерам, які виявляли серйозні вади та відповідально повідомляли про них. Пізніше Кеті пішла у вільне плавання й започаткувала програми координованого розкриття в багатьох інших організаціях, включно з Міністерством оборони. Крім того, вона невтомно працювала над тим, щоб інструменти для тестових проникнень припинили бути предметом угод про контроль над озброєннями.

Особиста етика стала темою палких дебатів, і вони вилилися навіть у хакінг усередині самого хакерського середовища. Деякі висококваліфіковані хакери, які знаходили вразливості нульового дня та приховували їх, засудили рух за активніше розкриття. Під лозунгом *Antisec* («антибезпека») найбільші ентузіасти цієї групи зробили мішенню своїх атак компанії, групи електронної пошти та окремих осіб, які оприлюднювали експлойти. На початку вони стверджували, що розкриття експлойтів озброює позбавлених таланту скриптомалюків — таких, що, можливо, були відповідальні за *SQL Slammer*. Але деякі просто не хотіли додаткової конкуренції. Естафету

підхопив хакер Стівен Ватт і група, що називала себе Phrack High Council, яка зробила *Antisec* рухом на межі злочинного. Пізніше Ватт відсидів тюремне ув'язнення за передачу сніфера, який перехоплював усі дані, що проходили мережею, Альберту Гонзалезу — одному з найзнаменитіших американських злочинних хакерів. 2008 року Ватт похвалився початком проєкту «Погром»[16], який, серед іншого, планував хакінг проти знаменитих «білих капелюхів». «Ми всі дуже повеселилися»,— сказав Ватт. Згодом місію *Antisec* підхопить нове покоління хактивістів.

[x x]

Тед Джуліан, який починав керівником маркетингового відділу в *@stake* до його злиття з *L0pht*, і Дуг Сон, хакер старої школи з групи *w00w00*, заснували компанію *Arbor Networks*. Вона стала серйозною силою в боротьбі з мережевими атаками та захисті комерційних і урядових клієнтів від самовідтворюваних черв'яків. Пізніше Сон стане засновником *Duo Security* та поширить двофакторну аутентифікацію в гігантських, як-от *Google*, і середніх компаніях.

Сон познайомився з файлами *cDc* та її членами онлайн до того, як особисто шаленіти від релізу *Back Orifice*. 1999 року він оприлюднив *dsniff*, інструмент перехоплення паролів та іншого мережевого трафіку. Поки в Arbor обмірковували додаткову роботу на уряд, Сон потроху розробив новий інструмент, який перехоплював більше даних. Він планував показати його керівникам *Microsoft* на першій започаткованій Віндоу Снайдер конференції *Blue Hat* 2004 року. Сон відвідав

конференцію та розповів про свій поліпшений сніфер, який аналізував контакти миттєвих повідомлень і документи й повністю записував голоси *IP*-дзінків, як-от у *Skype*. Для демонстрації він склав досьє на працівників *Microsoft*. Потім він вирішив, що небезпека від такого інструмента переважує вигоду від хапання за руку інсайдерів, що крадуть дані. Він переконав інших керівників *Arbor* скасувати плани з укладання контрактів і закрити його проєкт.

Один із молодих талантів *@stake* працював з офісу в Сан-Франциско. Алекс Стеймос приєднався невдовзі після закінчення Каліфорнійського університету в Берклі через захоплення Маджем та іншими засновниками. Коли *Symantec* поглинула *@stake*, він вирішив відкрити нову компанію разом з чотирма друзями. *@stake* довів, що можливо керувати бізнесом, який справляє величезний позитивний вплив на безпеку звичайних людей. Але він мав два недоліки, які Стеймос сподівався усунути в новій компанії. Першим було отримання венчурних грошей, що поставило перед стартапом нереалістичні фінансові цілі. Відмовившись від зовнішніх інвестицій, Стеймос і його партнери, серед них Джоель Валленстром і Джессі Бернс зі *@stake*, вклали 2000 доларів кожен і власними силами заснували нову консалтингову фірму, *iSec Partners*[17]. Вона не наймала багато керівників та агентів з продажу, а працювала як юридична фірма, у якій кожен партнер веде власні стосунки з клієнтами.

Бізнес-модель *iSec* спробувала розв’язати й іншу проблему *@stake*, яку Стеймос описував як «брак моральної основи». Він дбав, щоб ані йому, ані його партнерам не доводилося робити щось, що викликало б

дискомфорт: для будь-якого великого рішення була потрібна згода всіх п’яти.

2004 року *iSec* почала консультувати *Microsoft* після зникнення зі сцени *@stake* і допомогла істотно поліпшити безпеку в *Windows 7*. Чотири роки по тому її запросили допомогти з величезним проєктом для *Google*: мобільною операційною системою *Android*. *Android* розробляли настільки таємно, що навіть відмінні сек’юріті-спеціалісти самої Google не були в курсі. *iSec* отримала запрошення лише за сім місяців до запуску. Партнери в iSec виявили в екосистемі Android величезний ризик. *Google* як слабкіший гравець проти айфонів Apple планувала випустити софт безкоштовно та дозволити виробникам мобільних телефонів модифікувати його, як вони вважають потрібним. Але в *iSec* усвідомили, що в *Google* немає можливості забезпечити, щоб патчі дійсно потрапили до споживачів. *iSec* написала доповідь про небезпеку й надіслала її Енді Рубіну, відповідальному за *Android*. «Він проігнорував його»,— сказав Стеймос, хоча Рубін пізніше говорив, що не пригадує попередження. Більш як десятиліття по тому це досі найнебезпечніша вада *Android*.

Стеймос був невдоволений, що його покликали з запізненням, і почав думати, що робота власними силами — правильний шлях. Урешті-решт він улаштувався головним спеціалістом з інформаційної безпеки в *Yahoo*. Валленстром став гендиректором розробника системи безпечного обміну повідомленнями *Wickr*; Джессі Бернс залишався в *iSec* до її придбання *NCC Group* 2010 року, а 2018-го очолив підрозділ «хмарної» безпеки в *Google*. Тим часом 2005 року Дейв

Ґолдсміт заснував конкурента *iSec* на Східному узбережжі, компанію *Matasano Security*, яка залучила ще більше вихідців зі *@stake* до поліпшення безпеки для великих постачальників софту й споживачів. Пізніше він став вищим керівником у *NCC*.

Початок міленіуму був дивним і сповненим ідейних незгод періодом для сек'юріті-галузі. «Це був час визначитися з моральними переконаннями. Люди усвідомили свою владу»,— казав Дуг Сон. Сотні цілеспрямованих технічних експертів зі слабкими соціальними навичками, не кажучи вже про етичне виховання, раптом отримали повну свободу дій. Груп і галузевих зірок як потенційних рольових моделей було мало, а відкритої дискусії про правильну й неправильну поведінку — майже ніякої. Більшість працівників @stake залишилися на боці захисту й після тривалих обговорень розробили різні особисті кодекси етики в малих і великих компаніях. Хоча в наступні роки вони відіграли величезну роль у поліпшенні безпеки, можливо, найважливіша робота, на яку надихнула *cDc*, не була пов'язана з діяльністю корпорацій чи уряду.

Розділ 9.
TOR І *CITIZEN LAB*

На *Def Con* 2001 року, коли панель «Культу мертвої корови» зосередилася на хактивізмі й розхвалювала *Hacktivismo*, група також анонсувала те, що стане її першим інструментом обходу державної цензури. Ідея була складною та називалася *Peekabooty*. Користувачі у вільних країнах могли встановити програму й відігравати роль посередників для людей за національними файрволами в Китаї чи десь ще — тих, хто не мав можливості напряму зайти на заборонені релігійні, новинні чи інші вебсайти. Вони зв'язувалися з волонтерами, які встановили *Peekabooty*, мали повний доступ і могли автоматично спрямувати бажаний контент за допомогою *SSL*-протоколу, використовуваного на сайтах, вебадреса яких починається з *«https»*. Органи влади не змогли б зчитати трафік і не отримали б сповіщення, тому що це виглядало б як звичайна зашифрована ділова транзакція.

Хоча *BBC* повідомила, що проєкт з відкритим кодом запустять на *Def Con*, він не був готовий для релізу. Лейрд Браун сподівався, що завчасний розголос привабить більше волонтерів, яким він зможе доручити різні аспекти завдання. Провідним програмістом проєкту на повний робочий день був Пол Барановські, розробник і співробітник Лейрда в торонтівському стартапі *OpenCola*. Але його дратувало, що Лейрд не може

знайти інших програмістів, і він разом зі своїм другом Джої ле Вілла пішов з *Hacktivismo*, забравши з собою код. Вони оприлюднили його окремо на конференції в Сан-Франциско у лютому 2002 року. На думку Барановські, «у *Hacktivismo* добре вміють придумувати нові проєкти»[1], та не доводити їх до кінця. Але їхні зусилля теж не досягли критичної маси. «Найціннішим внеском *Peekabooty* було розуміння “Агов, ця штука можлива. Ось ідея, розвиваймо її”,— казав де Вілла.— Істинною цінністю був доказ життєздатності концепції».

2004 року Лейрд розповів про систему *Six/Four*, посилання на 4 червня 1989 року — бійню на площі Тяньаньмень. Написана новим членом *cDc* Кемалем Акманом, талановитим німецьким хакером з ніком Mixter, система *Six/Four* була ще однією спробою створити безпечну мережу проксі-серверів. «Я подумав, що напакостити тоталітарним урядам — це класно,— казав Кемаль.— cDc на повну використовувала свою славу, щоб зробити щось позитивне». Кемаль провів понад рік, налагоджуючи *Six/Four* до стану, коли її можна буде передати іншим. Але в групі електронної пошти *Hacktivismo* досі було приблизно двадцять активних членів і, можливо, дві сотні наглядачів. Як і спроба Барановські, *Six/Four* зазнала поразки. Однак самі публічні спроби *Hacktivismo* надати безкоштовні безпечні інструменти сотням мільйонів людей, що живуть в умовах суворих урядових обмежень, надихнули інших програмістів, які завершили цю роботу. Виявилося, їм не потрібно винаходити новий інструмент — лише переробити старий.

У середині 1990-х трьом чоловікам у Науково-дослідницькій лабораторії ВМС США спала на думку

ідея перекидання трафіку від одного сервера до іншого, а потім до третього, щоб обидва краї залишалися прихованими для шпигунів посередині. Перший вузол знав би тільки первинного відправника та, після відкриття першого шару повідомлення, куди відправити решту контенту. Другий вузол знав би тільки, що контент має перейти до третього вузла, а третій вузол знав би тільки кінцевий контент. Нікому не був відомий і контент, і відправник. Оскільки це багатокрокове розшарування нагадувало цибулину, проєкт став відомий як *The Onion Router*, пізніше скорочений як *Tor*. 1997 року Агентство передових оборонних дослідницьких проєктів США (*DARPA*) надало нове фінансування, ухопившись за цю ідею як спосіб захистити військових США та інших таємних службовців від викриття під час їхніх онлайн-розслідувань.

Утім, для уряду ця система мала фатальний недолік: будь-хто, з ким зв'язувалися через Tor, знав, що у двері стукає федеральний агент. Але один із первинної трійки, математик Пол Сіверсон, і нові співробітники Роджер Дінгледайн і Нік Метьюсон знайшли спосіб зробити інструмент достатньо привабливим, щоб люди поза урядом теж його використовували, ефективно ховаючи агентів у натовпі. Вони завершили створення прототипу у вересні 2002 року, за сім місяців після виходу коду *Peekabooty*, і наступного року зробили публічний реліз версії Tor.

Peekabooty та *Six/Four* істотно вплинули на *Tor*. «Найсильніше *Peekabooty* вплинув тим, що спонукав нас додержати слово, чіткими технічними умовами для *Tor* та уявленням, чого він намагається досягти»,— заявив Дінгледайн. Крім того, додав він, *Peekabooty* був на роки

попереду Tor у протистоянні цензурі, а не тільки в збереженні анонімності. 2004 року, бажаючи отримати фінансування з зовнішнього та неурядового джерела, проєкт Tor виграв грант від *Electronic Frontier Foundation*, чиї юристи вже брали участь у діяльності *cDc* та *Hacktivismo*. Підтримка *EFF*, своєю чергою, допомогла *Tor* отримати гроші від *Human Rights Watch*, *Google* та інших частин федерального уряду. Серед іншого, рання конкуренція з боку Hacktivismo продемонструвала потенційним інвесторам, що на послуги анонімності існує реальний попит і що незалежні від уряду активісти хочуть його задовольнити. «Ми вважали їх ключовою частиною нашої клієнтури та своїми однодумцями,— сказала про *cDc* тодішня юридична директорка та майбутня виконавча директорка *EFF* Сінді Кон.— Ці хлопці намагалися підтримати застосування технологій, іноді дуже передових, щоб розширити можливості користувачів і посприяти соціальним і політичним змінам. Ми теж у це вірили».

Дружнє змагання продовжилося на благо користувачів. 2006 року *Hacktivismo* й техаський член *Ninja Strike Force* Стів Топлец випустили найпопулярніший з розроблених групою інструмент анонімності. Це була ще одна спроба створити захищений браузер, і він називався *Xerobank*, або *xB*. Він був призначений для роботи з Tor, який на той момент передбачав зв’язки між комп’ютерами, використання електронної пошти й інші сервіси, але не легку навігацію мережею. Цей браузер був модифікованою версією браузера *Firefox*, який міг працювати з *USB*-накопичувача. Це означало, що користувач міг використати його з комп’ютера в громадському місці та не залишити слідів. Публічно працюючи над безпечним браузером, *Hacktivismo* знову

підштовхнув проєкт *Tor*. Tor випустив свій власний браузер, зробивши його набагато зручнішим. На 2006 рік більше людей покладалися на *Tor*, щоб обійти цензуру, а не зберегти анонімність, і Китай став третім за обсягом ринком з приблизно десятьма тисячами щоденних користувачів.

2006 року Лейрд організував конференцію з бездротових технологій у Дармсалі, базі тибетського уряду у вигнанні. Це допомогло зробити її місцем роботи розробників-ідеалістів. Лейрд переїхав до міста 2009 року та провів там три роки, безоплатно допомагаючи громаді. Він працював над безпекою в офісі Далай-лами та допоміг підготувати місцевих спеціалістів. Потім він ще два роки мешкав у Бангалорі, працюючи в неприбутковій організації.

Hacktivismo надихнув сотні чи тисячі людей і груп. У багатьох були історії, схожі на досвід Натана Фрейтаса. Нью-йоркський комп'ютерник Фрейтас уперше почув про переслідування тибетців на концертах рок-групи *Beastie Boys*. Наприкінці 1990-х через знайомого по роботі він познайомився з крихітною тибетською групою в районі Пекельної кухні{8}. Вона мала лише один модем і потребувала допомоги в налагодженні офісної мережі. Натан зробив це та звернув увагу, що майже на кожному комп'ютері є віруси. Він усвідомив, що тибетців постійно атакує китайський уряд.

2004 року Фрейтасу довелося зробити вибір. Кілька років тому *Palm*, піонер виробництва смартфонів, придбав маленький стартап, співзасновником якого він був. Тепер *Palm* хотів підвищити його та перевести до

Кремнієвої долини. Але якби він прийняв підвищення, то на активізм не залишилося б часу. Фрейтас бачив, на що здатні в *cDc*. «Вони були смішними, цікавими й ефективними»,— казав він. Вони довели, що маленькі групи можуть «вплинути на державну чи навіть глобальну корпоративну політику. Саме завдяки *cDc* я сказав собі: “Можливо, я здатен чогось досягти в цьому напрямі”».

Фрейтас залишив *Palm* і витратив гроші від продажу стартапу, щоб стати хактивістом на повний робочий день. Він на місяць поїхав до Китаю, щоб дізнатися, як блокують короткохвильове радіо та як його захистити. Відтак він допоміг заснувати *Tibet Action Institute* разом з лідеркою руху «Студенти за вільний Тибет» Ледон Тетонг, надаючи технічну допомогу та поради з безпеки емігрантам по всьому світу. У період підготовки до Олімпійських ігор у Пекіні 2008 року Фрейтас створив для загальнодоступного вебсайту супутникову відеотрансляцію, щоб показувати протести в таборі на горі Еверест. Підвищена увага до активізму призвела до витонченіших китайських атак, що тільки зміцнило його рішучість. Тільки 2008 року він забезпечив сімдесят осіб, переважно у материковій частині країни, криптофонами, одноразовими передплаченими мобільними телефонами та нетбуками на суму 3000 доларів. 2008 року Фрейтас приїхав у Дармсалу, щоб навчати тибетців і зустрітися з Лейрдом. «Він мав подібний до чернечого статус, але це був високий білий канадець», — пригадував Фрейтас. Лейрд навчав його та допоміг скласти список ідей, як досягти більшого за допомогою меншого, і познайомив зі своїм світом контактів. Коли *Google* запустила платформу *Android*, Фрейтас почав використовувати її, щоб зробити безпечний телефон за

менші гроші. Зрештою йому вдалося створити мобільну версію *Tor*. Відтоді його програму завантажили 17 мільйонів разів, і зараз вона очолює список усіх мобільних пропозицій *Tor*.

[x x]

Лейрд також став натхненником організації, яку багато незалежних експертів з безпеки вважатимуть найкращою моделлю дослідження та розкриття урядового використання інтернету для репресій,— *Citizen Lab* у Школі глобальних відносин імені Мунка при Торонтському університеті. Початок поклав студент цього університету Нарт Вільнев ще 2001 року. Він прочитав текстові файли *cDc*, стежив за нею, коли група запустила *Hacktivismo*, і невдовзі приєднався до списку поштової розсилки. Надихнувшись, він створив скромний вебсайт, що відстежує хактивістську діяльність, і провів інтерв'ю з Лейрдом для написання власного текстового файлу. «Коли я починав, мені подобався архетип міфічного хакера, який здатен на все»,— пригадував Вільнев. Не маючи досвіду в технологічній сфері, він цікавився традиційною політикою і протестами. На початку підривна тактика, як-от спотворення вебсайтів і мережеві атаки, мала для нього сенс. Але тексти Лейрда перетягнули його до «конструктивнішої точки зору», казав він, зокрема щодо обходу цензури. Тим часом люди в Китаї скаржилися, що їм недоступна деяка частина мережі, але не було даних про те, що саме заборонено. Вільнев запропонував спосіб протестувати блокування вебсайтів і написав на цю тему письмову роботу для професора Рона Дейберта. Дейберт заохотив його розробити таку

програму та прийняв до неприбуткової організації *OpenNet Initiative*, яка відстежувала цензуру по всьому світу. Потім Вільнев познайомив Дейберта з Лейрдом.

Двоє чоловіків довго обговорювали технологічні, соціальні, політичні та комерційні проблеми підтримання в інтернеті такої свободи, яку проголошував Джон Перрі Барлоу. Вони говорили про потребу отримати й оприлюднити об'єктивну, докладну інформацію про те, що відбувається всередині роутерів і комутаторів на неприязних територіях. Вони погодилися, що модель фінансування для такого проєкту має бути бездоганною, щоб його не можна було обвинуватити в сидінні в кишені розвідувального агентства чи уряду. Потрібна здатність донести інформацію до дослідників, преси та громадськості, щоб вчинити політичний тиск на причетні уряди й компанії, багато з яких базувалися на Заході та надавали інструменти цензури й шпигування.

«Жодних сумнівів, дещо з наших перших обговорень хактивізму було важливо для мене з точки зору створення Citizen Lab,— казав Дейберт.— Мене, як і Лейрда, надихав хакінг у первинному сенсі цього слова, поєднаний з політичною позицією чи етикою. Я подумав, це дуже привабливо. Гадаю, у нас однаковий світогляд і філософія стосовно того, що прийнятно, а що ні»[2].

Лейрд стверджував, що основні дослідження мали приналежність до університету, тому що знання були для нього важливіші за прибуток чи політику. Так само як проєкт Tor у практичній сфері, університет міг брати трохи державних грошей і все одно залишатися чистим. І він міг запрошувати спеціалістів з інших дисциплін — програмістів, сек'юріті-експертів і навіть політологів.

Його амбіції приголомшливо зростуть, адже багато коледжів досі не пропонували курси з безпеки.

Навесні 2001 року, після отримання схвалення від Торонтського університету й початкового гранту від Фонду Форда, Дейберт розпочав роботу *Citizen Lab*. Вільнев став його першим співробітником. Скромна офіційна місія: досліджувати кіберпростір «у контексті міжнародної безпеки»[3]. Але використовувані інструменти варіювалися від технічної розвідки до польових досліджень і політичної теорії. Атаки 11 вересня майже миттєво підвищили ставки. Оскільки розвідслужби США жорстко критикувалися за брак інформованості, нагляд мав неминуче посилитись і на Заході, і на Сході. І це був тільки початок. Геополітика інтернету розповсюджувалася навсібіч, перетворюючись на одну з найважливіших і найскладніших проблем, з якою зіткнеться світ. Знайти відповіді буде важко. Але ні в кого іншого не було кращих можливостей, щоб спробувати.

Спочатку лабораторія ретельно дослідила вебфільтри в арабському світі, їхніх постачальників і сторінки, до яких обмежували доступ. Під час тієї тривалої роботи виявилося, що Сирія використовує програму фірми Blue Coat із Кремнієвої долини[4], щоб шпигувати за власними громадянами, потенційно порушуючи санкції США. Лабораторія також узялася за дослідження легального продажу експлойтів[5] та інших інструментів для того, що галузь називала «законним перехопленням», простежуючи численні випадки, коли постачальники говорили, що продають тільки урядам, які поважають права людини. Попри такі заяви, дослідники часто

виявляли, що репресивні режими використовують продукти компаній на кшталт Gamma Group, що базувалася в Сполученому Королівстві та Німеччині, та італійської фірми *Hacking Team* проти правозахисників, журналістів і політиків з партій меншості. Значно пізніше на основі відкриттів *Citizen Lab* газета *New York Times* надрукувала разючу серію статей[6] про використання шпигунського софту Pegasus ізраїльської компанії NSO Group проти мексиканських журналістів, політиків та інших осіб, зокрема службовців, які розслідували масові зникнення людей, і навіть активістів руху проти ожиріння. Президент Мексики наказав провести розслідування, яке, за висновками ФБР, було фікцією.

Незалежна академічна структура лабораторії щоразу надавала їй можливість писати про те, про що не могли писати інші. Наглядова рада університету мала схвалювати методи дослідження на етичних і юридичних підставах. Проте очільник головної канадської розвідслужби у відставці одного разу уїдливо зауважив, що, на думку деяких людей, Дейберта слід заарештувати. Оскільки більше країн починали шпигувати одна за одною в мережі, використовуючи компанії як засоби для досягнення цілей чи співучасників, розплутування всього цього клубка могло мати неприємні політичні та комерційні наслідки для будь-яких приватних дослідників. Ті самі великі компанії, які успішно досліджували та пояснювали зловмисний софт, використовуваний організованою злочинністю, не були такими відвертими, коли усвідомлювали, що винними були уряди, що контролювали великі ринки збуту їхніх програмних засобів системи безпеки. Уряди теж мовчали, тому що розвідувальні агентства завдяки

бюрократії зберігали панування в кібернападі та кіберзахисті, і такі агентства не хотіли розкривати те, що знають.

Деякі спеціалізовані фірми, як-от *Mandiant* і *CrowdStrike*, розкривали більше інформації у приватних доповідях клієнтам. Іноді вони робили публічні заяви, у яких пов'язували зараження вірусами в певних галузях з координованими кампаніями, що проводяться підвладними уряду хакерськими групами. Але вони стикалися з обвинуваченнями в упередженості[7], тому що їхні системи виявлення було розгорнуто тільки в деяких країнах, вони працювали на уряд США за контрактом чи мали ринкові причини розголосити те, що роблять. *Kaspersky Lab*, що базувалася в Москві, подібним способом стала найкращою у світі в дослідженні фінансованих США кампаній кібершпигунства, починаючи зі *Stuxnet*, новаторської зброї, яка вивела з ладу іранські ядерні центрифуги до свого розкриття 2010 року, коли всі дізналися про нову еру кібервійни. Але *Kaspersky Lab* мало що могла сказати про російські шкідливі програми. *Citizen Lab* могла називати речі як є. І вона розширила сферу своєї діяльності, співпрацюючи з дослідниками інших організацій, наприклад з *Google*, яким було б складно публікувати результати під іменем свого головного роботодавця. Лабораторія також співпрацювала з дослідниками в *Amnesty International* та *Electronic Frontier Foundation*.

[x x]

З роками робота лабораторії стала тільки ефективнішою та більш важливою. За одним із найбільших проєктів Вільнев мав з'ясувати, що за шпигунство відбувається в Тибеті. Як видно з усього, принаймні деяке шпигування було, адже активістів раз у раз не пускали до Китаю, іноді заарештовували та показували їм записи їхніх електронних чатів з людьми всередині Китаю. Вони ризикували своїми життями. Лейрд познайомив команду з Ґреґом Волтоном, який досі був у Дармсалі та за канадського фінансування працював над ініціативами з захисту прав. У Волтона були хороші відносини з тибетцями, і 2008 року Дейберт найняв його місцевим дослідником. Дейберт уперше дізнався про спеціалізоване шкідливе програмне забезпечення. Пізніше Волтон умовив Далай-ламу передати комп'ютери керівників для дослідження. Нападники зрешетили захист тих комп'ютерів. Виявилося, передчуття Волтона принесло великі результати. Мережевий трафік від багатьох комп'ютерів містив той самий рядок з двадцяти двох символів. Вільнев пошукав його й одразу опинився в комп'ютері в материковому Китаї, на порталі, що перелічував сотні комп'ютерів, у які проникла та сама група. Серед жертв був поштовий сервер *Associated Press* у Гонконгу, незасекречений комп'ютер у штаб-квартирі НАТО і посольства Індії, Пакистану, Німеччини й Тайланду.

Команда Дейберта назвала шпигунську мережу *GhostNet*[8]. *Citizen Lab* розкрила її 2009 року, потрапивши на перші шпальти газет у всьому світі. Дейберт завчасно запросив *New York Times*, частково заради максимального ефекту, частково як страхування на випадок, якщо канадський уряд спробує замовчати

те, що знайшла *Citizen Lab*. Перша така доповідь неурядової організації та одна з перших узагалі, які пов'язували конкретне комп'ютерне шпигунство зі світовою державою, стаття про GhostNet не обвинувачувала Китай прямо. Але та країна, безсумнівно, стояла за прикладом того, що стане відомо як розвинена стала загроза, або цілеспрямований суперник у кіберпросторі. Проникнення контролювалися чотирма серверами, зокрема одним на острові Хайнань, базі Третього технічного відділу Народно-визвольної армії Китаю.

Команда гарячково працювала, розмотуючи всі зв'язки та документуючи, як вони функціонують. Водночас вона зазнала труднощів із новими питаннями розкриття інформації. Якби виявилося, що Китай шпигує за окремою ідентифікованою людиною, вони б вважали, що зобов'язані попередити жертву, хоча чіткого етичного правила не було. Що, як серед жертв опинився б їхній власний уряд? А як щодо інших урядів? Кому що повідомляти та коли? Замість іти напряму до канадської розвідки та наражатись на ризик примусу до співпраці, Дейберт із люб'язності пішов до канадської групи реагування на порушення комп'ютерної безпеки. Крім того, *Citizen Lab* спитала Міністерство закордонних справ Канади, чи може воно надіслати сповіщення іншим країнам. На відповідь від міністерства довелося чекати місяцями, і воно відмовилося допомогти.

Натан Фрейтас, хактивіст і спеціаліст з *Tor*, який допомагав тибетцям, зіткнувся зі схожою проблемою. Коли доповіді пролили світло на китайське шпигування, більше людей захотіло отримати копії вірусів, що атакували мережі тибетців. «Ніхто раніше не бачив

такого зловмисного програмного забезпечення, з яким ми зіткнулися,— розповідав Фрейтас.— Дослідники приходили до нас із запитанням, чи можна їм отримати зразок». Деякі з них були вченими, які шукали матеріал для докторської дисертації, деякі — працівниками приватних компаній, хтось — державними службовцями. Очевидно, що серед них були розвідувальні агенти або підрядники. Фрейтас усвідомлював: «Не можна обманювати себе. Це глобальна кібервійна». Замість спробувати розібратися, хто на кого працює та чи доречно надавати перевагу емісарам однієї країни над іншими, Фрейтас тільки розвів руками. Він вирішив ділитися зразками лише з *Citizen Lab*, у якої була своя етика. Але в спільноті, яку піддавали стільком атакам, з присутністю різних помічників із Заходу, деяка інформація все одно потрапила до могутніх західних розвідслужб, які боролися з Китаєм. Хактивізм надавав тим агентам привід бути серед активістів.

Попри обережне етичне балансування Дейберта, фігури розвідки все одно були причетні до роботи *Citizen Lab*. Лабораторія отримала аналітичну допомогу від Рафаля Рогозінські, консультанта з лабораторних досліджень, який обіймав кілька посад водночас. Рогозінські був гендиректором *Psiphon Inc.*, мережі проксі-серверів для обходу цензури, яка відділилася від *Citizen Lab*. Також він працював на військових і як технічний радник ООН з комунікаційних проєктів у колишніх радянських країнах. Хоча й називав себе незалежним підрядником, він визнавав свої розвідувальні зв’язки, і його симпатії не викликали сумнівів. Лейрд і Вільнев називали його «спецслужбістом», за словами Рогозінські, помилково.

Лейрд теж заперечує, що він шпигун, і ніколи не зізнавася в цьому в *cDc*. Але його дивне знайомство з групою, ігри з історією «Гонконгівських блондинок» і пізніша міжнародна діяльність змусили декількох членів *cDc* замислитися, навіть не знаючи про відносини з розвідслужбами. Двоє його контактних осіб у розвідці сказали мені, що Лейрд був досить близький до спільноти, яка, можливо, справедливо чи ні вважала його «таємним агентом». Цього достатньо, щоб змінити історію хактивізму.

Розвідувальні агентства інтенсивно поглинали інформацію про *GhostNet*. Рогозінські і Вільнев разом проводили брифінги для АНБ, а Рогозінські отримував інформацію напряму від Ґреґа Волтона. Певною мірою західні розвідувальні служби були в захваті від роботи *Citizen Lab*. Вона викрила геополітичного суперника та справляла позитивніше враження, тому що не мала прихованого мотиву. Крім того, вона використовувала законні, але агресивні інструменти, як-от сканери портів, для яких знадобилося б багато етапів схвалення, якби деякі уряди використовували їх напряму. Але Дейберт помітив ворожість і з боку канадських органів влади, яку неможливо було пояснити тільки професійною заздрістю чи зневагою до організацій-вискочок. За кілька років, ретельно вивчаючи злиті Едвардом Сноуденом документи, Дейберт вирішив, що зрозумів причину, і Рогозінські з ним погодився: канадці знали про китайську шпигунську мережу та користувалися нею, збираючи власні розвіддані, поки про неї не розповіла *Citizen Lab*.

За рік після доповіді про *GhostNet* компанія *Google* заявила, що китайці зламали і її теж і що через це вона

залишає країну. Тепер усі усвідомили, що живуть в умовах неоголошеної кібервійни. У *Google* всюди були найкращі спеціалісти з захисту. Після того як *Google* усвідомила, що китайці полюють на акаунти правозахисників і сам код Google, вона запросила найкращі зовнішні таланти, які тільки могла знайти. Серед них був Дейв Айтель та інші ветерани АНБ і навіть само АНБ. Громадськість була стурбована, але взагалі не усвідомлювала, наскільки ефективною була китайська кампанія, тому що ні в кого не було мотиву це визнати. За словами Маджа, китайці проникли в сховища вихідного коду багатьох великих компаній і вписали дещо схоже на помилки програмування. Насправді існували бекдори, які надавали китайським шпигунам змогу зламувати пристрої споживачів великих технологічних компаній, коли їм заманеться. У такій боротьбі *Google* та багато інших зі зрозумілих причин вважали, що АНБ — хороші хлопці. Але все було не так просто. За кілька років, коли відбудеться публічний дебют викривача АНБ Едварда Сноудена, *Google* та багато інших американських технологічних компаній, не кажучи вже про решту світу, побачать в агентстві свого заклятого ворога.

Розділ 10.
ДЖЕЙК

Після того як браузер *Xerobank* від *Hacktivismo* підштовхнув проєкт Tor розширити свою місію 2006 року, сервіс став дійсно корисним для великої кількості людей. Tor почав активно розповсюджуватись у країнах на кшталт Китаю та Іраку, де після нагляду міг швидко слідувати тюремний строк. *Psiphon*, *Freegate* та інші сервіси могли надати читачам доступ до заборонених частин мережі, але тільки поліпшений *Tor* міг приховати, хто їх читає. Це не випадковість, що того року фінансування урядом США проєкту *Tor* значно збільшилося. Як і з іншими проєктами вільної комунікації, що активніше їх використовували в регіонах, де керують політики, опозиційні американським інтересам і репресивні щодо власного місцевого населення, то більшим був ентузіазм США стосовно інструментів, які сприяють свободі слова.

Але попри відкритість вихідного коду *Tor*, його походження з лабораторії ВМС і продовжуване федеральне фінансування викликали підозри, чи містить він бекдори для шпигунів США або інші зловживання. Як покажуть документи Едварда Сноудена за кілька років, їх не було. *Tor* зірвав плани розвідувальних агентств США, які були нездатні надійно його зламати. Підтримка з боку *Electronic Frontier Foundation* і патріотично налаштованих криптографів, включно з кількома в групі електронної пошти

Cypherpunks, допомогла переконати багатьох людей, що вони можуть довіряти *Tor*. Але більшість із них належала до попереднього покоління, довговолосих математиків, які почувалися набагато комфортніше в університетській бібліотеці чи офісних парках Кремнієвої долини, ніж на зустрічах з молодими активістами.

Очевидна відповідь на проблему Tor у відносинах з громадськістю надійшла в особі Джейкоба Еплбаума, відомого як Джейк і @IOerror у Твіттері — посилання на несправність у взаємодії «ввід/вивід». Джейк був молодим і привабливим, харизматичним публічним спікером і частим доповідачем на серйозних конференціях з безпеки. І він мав надзвичайно захопливу особисту історію[1]. Багато хакерів рано почали використовувати комп'ютери, щоб утекти від важкого дитинства, але випадок Джейка був жахливим. Його матір страждала на шизофренію та виховувала його, поки не втратила батьківські права. Джейка передали тітці, яка залишила його в інтернаті. Коли йому було десять, пішов жити до батька, але той підсів на героїн. Батько й син жили в автобусах і лігвах наркоманів, й одного разу Джейк знайшов свого тата при смерті від передозування. Повернувшись до інтернатів, Джейк кинув старшу школу та сам навчився програмувати, працюючи на *Greenpeace* та *Rainforest Action Network*. На *Def Con* Джейк познайомився з лідерами проєкту Tor Роджером Дінгледайном і Ніком Метьюсоном і став волонтером. Він приєднався до штату проєкту 2008 року та швидко перетворився на його найвідомішого представника. Він також був одним із найактивніших мандрівників у мережі *Tor* —

подорожував і навчав місцевих жителів, як ним користуватися.

Хай би де була увага, здавалося, Джейк теж там був, навіть як співавтор наукової статті про те, що можна відновити незашифровані паролі завдяки заморожуванню чипів оперативної пам'яті. «Це дуже круто»,— написав Люк Бенфі, коли 2008 року успішно висунув кандидатуру Джейка у члени «Культу мертвої корови». «Жодних сумнівів, він ентузіаст»,— додав Люк, хоча й «трохи дивний». Більшість головних членів *cDc* були тоді достатньо вражені, щоб підтримати пропозицію, і Джейк увійшов до групи за фінального схвалення Кевіна Вілера. Навіть тим, хто не був знайомий з ним, здавалося, що вони його знають, адже його історію розповіли різні видання — присвячені безпеці, технологіям і навіть деякі провідні. Існувала додаткова причина його прийняття. Лави групи рідшали, і новобранців з молодшими послідовниками слід було цінувати, якщо *cDc*, якій уже було понад двадцять років, хотіла залишатися життєздатною організацією.

До *Hacktivismo* приєднався Кемаль Акман (відомий як Mixter) та інші за запрошенням Лейрда Брауна, а також старі друзі, наприклад Патрік Lord Digital Крупа. Деякі нові дослідники безпеки, як-от Адам О'Доннелл, теж піднялися на борт. Але більше членів просили видалити їх зі списку розсилки. Серед них були деякі технологічні ентузіасти, зайняті керуванням власними компаніями, та менш захоплені технологіями ветерани, як-от Керрі Кемпбелл. 2006 року вона написала сумного листа й попросила видалити її з розсилки, частково обвинувачуючи себе за те, що не познайомилася з новими членами та віддалилася від групи.

Боюся, мій інтерес до хакерського світу давно згас. Нові люди не знайомі зі мною. Я була 16-річною дівчиною, коли Psychedelic Warlord побачив мої божевільні, жахливо написані, повні підліткової туги дописи на своїй дошці та запросив приєднатися до cDc. Це була честь для мене. Я з радістю приєдналася та продовжила писати паскудні, жахливі підліткові т-файли. Я обожнювала спільноту дотепних людей (і їхніх подруг), з якими цікаво поспілкуватися й обговорити ідеї. Прийняття мене як жінки було вкрай рідкісним явищем у хакерському світі, і я це цінувала. Я ніколи не вдавала з себе хакера, адже не майстерна в цій сфері (хоча легко навчилася соціальній інженерії).

Чомусь я чисто випадково опинилася єдиною дівчиною у найвідомішій у світі хакерській групі, і хоча тоді це було дуже цікаво, зараз мій вік наближається до 40. У мене не залишилося енергії для cDc чи поштової розсилки. Та в мене є енергія для чудових друзів, яких я здобула на цьому шляху тривалістю, о господи, десь 21 рік. Будь ласка, іноді пишіть мені.

Оскільки Керрі була головною, хто підтримував згуртованість групи, і віддалилася майже настільки, як Кевін, він був схвильований її вибуттям і почав непокоїтися, що слідом за нею підуть інші. Він довго гуляв Центральним парком, а потім написав їм листа з проханням залишитися. «Хакерський світ не є тим, чим я захоплений, це радше база вербування кмітливих сучих синів — і радісно скажімо “чорт забирай!”, що так є,— написав Кевін.— Сподіваюся, колись серед нас буде штучний інтелект і ми намагатимемося зрозуміти практичний сенс геополітики та філантропії. Завжди

є що сказати, до чого привернути увагу, щось цікаве, приголомшливе та захопливе. Універсальна, непохитна, вічна частина цього — передача інформації, комунікація. Завжди. Я хочу, щоб ви залишилися».

[x x]

Але плем'я потребувало нової крові. Якщо Джейк був таким хорошим, як здавалося, він міг додати не тільки нової енергії, але й потенційно нових членів. Невдовзі з'явилися деякі підтвердження, що він — вдала ставка. Його появи в пресі вражали, зокрема досьє в *Rolling Stone* 2010 року, у якому його назвали «ексцентричною версією Марка Цукерберга» та провідним поширювачем «Євангелія анонімності».

Усередині cDc Джейк поводився інакше, люто сперечаючись із колегами, іноді зі зневагою до старших. Ця риса посилилася, коли він устряв у дещо більше, ніж *Tor*,— *WikiLeaks*. Хакери-активісти запустили сайт 2006 року і вперше привернули велику увагу 2010-го, коли розмістили відеозапис під назвою «Супутнє вбивство» з кадрами обстрілу з американських гелікоптерів в Іраку. Загинуло не менше дванадцяти осіб, включно з двома журналістами Reuters. Відео спростувало заяви США, що обстріл був частиною бойових дій.

Тим самим засновником *WikiLeaks*, який вистояв після років внутрішнього розбрату та незгод, був австралієць Джуліан Ассанж, дитинство його було майже таким жахливим, як і Джейкове. Він і його мати ховалися від переслідувань небезпечної секти. Навіть більший

хвалько, ніж Джейк[3], Ассанж був агресивно налаштованим, опозиційним щодо істеблішменту й іноді зловмисним хакером у рідній Австралії. У 1990-ті під іменем proff він фігурував у деяких з найпопулярніших каналів ретрансльованого інтернет-чату, присвячених безпеці та хакінгу, як-от *#hack*. Він був амбітним і небезпечним хакером, який пізніше приписував собі проникнення в комп'ютери австралійського уряду й Пентагону. У членів *cDc* не дуже приємні спогади про нього, адже вони вважали його самозакоханою людиною, яка переховувалася замість брати участь у дискусіях. А коли він говорив, це часто була критика або прохання надати код, який він міг використати для проникнень.

У 1996 і 1997 роках Ассанж регулярно отримував розсилку *Cypherpunks*, порівнюючи нотатки інших про новини криптографії та поточний конфлікт зі службовцями багатьох урядів, які прагнули обмежити її. Ассанж рекламував власний список розсилки щодо «юридичних аспектів комп'ютерних злочинів». Він починався з маніфесту, який декларував, що комп'ютерні злочини надмірно переслідують і що вторгнення не слід вважати злочинними діями, якщо вони не заподіяли шкоди. У якийсь момент він зробив допис про комерційну спам-операцію та спитав: «Хто хоче першим обвалити цей сайт?» Однак Ассанж і Мадж поважали один одного та зустрілися за вечерею на зборах *Chaos Computer Club* 2000 року в Німеччині.

cDc дуже захоплювалася ранньою *WikiLeaks*, і цілком обґрунтовано. Сайт публікував широке розмаїття документів і, як було видно з усього, спеціалізувався на неправомірних діях урядів. Отримавши 2010 року

десятки тисяч дипломатичних телеграм Держдепартаменту США від тодішнього рядового Бредлі Меннінга (тепер Челсі Меннінг), він співпрацював з медіапартнерами, які ретельно проаналізували важливі історії, водночас не друкуючи інформацію, здатну призвести до смертей тих, хто співпрацював з американськими службовцями за кордоном. «У мене деякі проблеми з цією організацією, але вона мені радше подобається, принаймні поки що»,— написав того року Лейрд у листі до членів *cDc*.

Ассанж мав виступити на конференції *HOPE* в Нью-Йорку в липні 2010 року. Але Пентагон позначив WikiLeaks як загрозу, й Ассанж боявся арешту. Замість нього несподівано приїхав Джейк. Він палко розповів історію сайту-викривача, на його думку, така сміливість продовжує традицію висвітлення Вотергейту й В'єтнамської війни у *Washington Post* і *New York Times*, а також згадав про недавню нерішучість медіа, зокрема про відтермінування Times у викритті несанкціонованого прослуховування АНБ. «Якщо медіа не дають говорити, ми відмовляємося мовчати»,— заявив Джейк. Він додав, що нічого не скаже про хакера Адріана Ламо, який видав Меннінга органам влади після того, як стурбований рядовий поділився з ним, що це він передав документи Держдепартаменту. Потім Джейк розстібнув свою сорочку і показав футболку під нею з написом «Припиніть доносити». Наприкінці його виступу зал раптом занурився в темряву. Коли світло ввімкнулося, присутні побачили, як начебто Джейка проводжають у безпечне місце. Насправді це був двійник, якого залучили, щоб Джейка не заарештували чи не заподіяли йому шкоди або просто щоб переконати аудиторію

в можливості обох варіантів подій. Справжній Джейк вийшов через чорний хід.

Після цього американські митники й прикордонники часто зупиняли Джейка в аеропортах і допитували без пред'явлення обвинувачень. Він на весь голос скаржився на публіці та своїм колегам у *cDc*, і на початку 2011 року сказав їм, що «уряд США позначив мене так само, як нацисти примусили євреїв носити жовту зірку. Втім, у мене немає можливості позбавитися своїх міток. Тепер вони назавжди в паспортній системі». Як людина, яка жила в інтернеті та ставила йому на заслугу своє спасіння в дитинстві, Джейк мав би знати про «закон Ґодвіна». Названий на честь свого автора та першого штатного юриста *EFF* Майка Ґодвіна, цей вислів стверджує: «У міру розростання дискусії в мережі ймовірність порівняння, що згадує нацизм або Гітлера, наближується до одиниці». Ґодвін був засмучений падінням якості онлайн-обговорень і браком серйозності до теми Голокосту.

Ветеранів *cDc* цей хід не вразив. «Чуваче, ти це серйозно? — написав Люк.— Тобі щойно вдалося втілити в життя закон Ґодвіна. Джейку, гадаю, тобі потрібне деяке розуміння, що хто каші наварив, той мусить і з'їсти». Прокурор Ґленн Курцрок був точніший у цитуванні правил, які регулюють роботу Прикордонно-митної служби США. «Не схоже, щоб працівники Прикордонно-митної служби робили щось неправильне. Вони мають повне право обшукувати та затримувати вас, включно для перевірки вмісту будь-яких електронних пристроїв». Джейк також часто сперечався з іншими щодо Ассанжа, у якого, за висловом Лейрда, такий самий демократичний стиль менеджменту, як

у правителя Саудівської Аравії. «Ось вам і хактивістська солідарність»,— скаржився Джейк. Люк і Кемаль обійняли позицію посередині: Ассанж — засранець, але він, здається, робить гарні речі.

Загалом оприлюднені *WikiLeaks* телеграми Держдепартаменту показували, як службовці США виконують свою роботу. Не було великої зловісної змови. Але різноманітні історії досі бентежили американський уряд і псували дипломатичні відносини. Документи містили відверті оцінки лідерів іноземних держав, включно з їхніми брудними альянсами та схильністю до корупції. Пристрасть до антисекретності на WikiLeaks нагнітала галасливі дебати всередині *cDc*. Ґленн та інші вважали Ассанжа необачним, зауважуючи, що судова система й інші частини уряду мали дуже вагомі причини зберігати конфіденційність деяких фактів. Обговорюючи гіпотетичну ситуацію потрапляння кодів запуску ракет не в ті руки, Джейк заявив: «Можливо, вам не слід володіти ракетами, якщо ви не можете зберегти в таємниці свої коди?» Він сказав багато провокаційних речей, оголосивши, що прослуховування «цілком фіктивні» та що більшість ордерів на обшук недоречна. Одна із найнесподіваніших заяв надійшла у відповідь на запитання, хто має вирішувати, які секрети розголошувати. Джейк сказав, що на це має право не *WikiLeaks* як видавець, а її джерела, хай ким вони є. «Це сувора реальність, але критика WikiLeaks навряд чи має сенс,— написав він.— Справа преси — інформувати».

[x x]

Члени Конгресу засудили *WikiLeaks*, а федеральне кримінальне розслідування тиснуло на *PayPal*, *Visa* й інші організації, які допомагали людям робити пожертвування вебсайту. Активістська онлайн-група, відома як «Анонімус», улаштувала координовані мережеві атаки на *PayPal* і *Visa*, по суті, підхопивши естафету хактивізму. Історію «Анонімусу»[4] набагато повніше викладено в книжках антропологині Ґабріелли Колман і журналістки Пармі Олсон, і вона складна й захоплива. Крім того, вона трішки завдячує частиною своєї культури *cDc*. Один із хороших друзів і колишніх вебхостерів *cDc*, Том Делл, написав програми для MindVox Патріка Крупи, а потім керував *Rotten.com*, сайтом-передвісником *4chan*. Користувачами *4chan* були переважно хлопчики-підлітки, які обговорювали зображення, і дописи на сайті автоматично позначалися Anonymous. Але якщо під загрозою опинялися головні цінності інтернету, як-от свобода слова, на сайті виникали спалахи політичної активності. Коли Церква Саєнтології спробувала покласти край розголошенню її секретів, користувачі *4chan* організували протести онлайн і в реальному світі, і їхні учасники відділилися як рух «Анонімус». Подальшими об’єктами атак стали організації, що відстоюють авторське право, як-от Американська асоціація кінокомпаній. Об’єднати величезні натовпи в ретрансльованому інтернет-чаті в щось продуктивне було дуже складно від самого початку. Організатори переходили в таємні менші канали, щоб розібратися з пріоритетами, а потім поверталися до більших зібрань, аби поширити інформацію.

Хто завгодно міг оголосити себе членом «Анонімусу», і будь-який член міг закликати до операції, найчастіше — мережевої атаки. Інші члени самі вирішували, брати участь чи ні. У разі мережевих атак членів заохочували завантажити інструмент для участі. Але хоча це надавало їм відчуття важливої ролі з низьким ризиком, вони помилялися. Деяких заарештували, тому що той інструмент не приховував їхні *IP*-адреси. І джерелом більшої частини атак були ботнети, мережі захоплених комп'ютерів під контролем невеликої підгрупи членів «Анонімусу». Звичайні члени допомагали з прикриттям і спричиненням сум'яття — та й усе.

Коли «Анонімус» об'єднався з *WikiLeaks* і вдарив мережевими атаками по платіжних сайтах, думки членів cDc щодо етики подій розділилися, і вони вирішили не робити нічого як колектив. Лейрд, який роками виступав з промовами про етику хактивізму, взяв на себе основний тягар щодо цієї теми. Він виступав проти мережевих атак як цензури, стверджуючи, що засіб проти неприємних промов — ще більше промов. Коли репортери просили його про коментарі щодо «Анонімусу», він стояв на своєму. Люк, з іншого боку, вважав, що залежно від мотивів і мішеней деякі мережеві атаки — це обґрунтована громадянська непокора. Він сказав, що напад лише тимчасово вивів з ладу *PayPal* і *Visa*, тоді як вони зміцнили свій захист. Але недовге викидання їх в офлайн привернуло увагу медіа та підвищило обізнаність з порушених питань. Люк вважав, що коли увага натовпу зосереджується на кількох речах, які здатні змінити політику, це сприяє гідному компромісу.

Десятки членів «Анонімусу» дійсно мали хакерські навички, що стало очевидно після того, як 2011 року я написав коротку статтю в *Financial Times*[5] про дослідника Аарона Барра. Він сказав, що виступить на конференції з розповіддю про людей, які, як він вважає, керують групою. Висококваліфіковані ватажки «Анонімусу» поспілкувалися в приватному каналі та після виходу моєї статті члени того каналу зламали файли Барра та двох афілійованих компаній, *HBGary Federal* і *HBGary*, щоб упевнитися, що він не має на них компромату. Вони оприлюднили електронні листи від компаній, які показали, що слова Барра були далекі він істини та що він брав участь у деяких сумнівних справах, наприклад хотів дискредитувати WikiLeaks наданням сфабрикованої інформації.

Першокласні хакери проголосили себе світові як *Lulz Security*, почали твітити в акаунті *@LulzSec* і влаштували шалену виставу, зламуючи таблоїди Руперта Мердока, щоб розміщувати дописи про його смерть, і навіть приймаючи запити від підписників. *LulzSec* вела активний і кумедний канал у Твіттері, який наповнював такий собі Topiary, пізніше ідентифікований як 18-річний житель Шетландських островів Джейк Девіс.
В анонімному інтерв'ю незадовго до свого арешту Девіс пояснив, чому, на його думку, *LulzSec* мала стільки прихильників: «Те, що ми робили, відрізнялося[6] від інших хакерських груп. У нас був активний акаунт у Твіттері (який контролював я), милі котики у дефейс-повідомленнях і грайливий, мультяшний характер наших операцій. Ми знали, коли почати, коли зупинитися, і найголовніше, більшість із нас знала, як розважитись».

Пізніше Девіс сказав[7], що його надихнули британський сатирик Кріс Морріс та комік Ноель Філдінг і що його пустотливість мала серйозний зміст: він хотів, щоб люди замислилися, чому проблеми безпеки настільки поширені, замість приписувати всі її порушення нестримним геніям. «Це було поєднання навмисної абсурдності та безтурботної дитячості, призначене змінити напрям розмови: “Ці люди роблять це, немов у гру грають. Можливо, нам справді слід почати думати про безпеку, якщо ці бовдури здатні влаштувати стільки безладу”».

Ці витівки та публічні коментарі нагадували презентації *Back Orifice*. Девіс відточив свої письмові навички, складаючи тексти для сатиричного хакерського сайту *Encyclopedia Dramatica*, який за стилем нагадував старі текстові файли *cDc*. У житті Девіс був тихим і сором’язливим, зовсім як засновник *cDc* Кевін Вілер поза сценою. Але серйозні протиправні акти повели *Lulz Security* іншим шляхом, і їй так чи інакше бракувало стабільності «Культу мертвої корови». Її члени не були знайомі одне з одним у фізичному світі, тому не могли впевнено вирішувати, кому довіряти. В «Анонімусі» ця проблема ускладнилася тисячократно. Втім, «Анонімус» і *LulzSec* започаткували нову еру викрадання й публікування матеріалів, як проголошувалося, задля суспільного блага.

Мотивом багатьох трюків *LulzSec* була водночас політика та розваги. Під кінець Девіс, спантеличений, як і *cDc*, тим, що робити з публічною увагою далі, заявив, що *LulzSec* відновить *Antisec*, стару кампанію проти професіоналів — «білих капелюхів». Цього разу *LulzSec* об’єднається з іншими членами «Анонімусу» та

переслідуватиме служби безпеки, банки та інші осередки влади. Джуліан Ассанж уважно стежив за подіями[8], у певний момент попросивши групу про допомогу в проникненні в ісландські служби електронної пошти, які могли показати, що уряд несправедливо ставиться до *WikiLeaks*. Після того як прихильник *LulzSec* Джеремі Гаммонд зламав електронну пошту розвідувально-аналітичної фірми *Stratfor*, *WikiLeaks* оприлюднила мільйони її листів до клієнтів. Зрештою органи влади схопили майже всю команду *LulzSec*. Технологічний ватажок Гектор Монсегюр, відомий під ніком Sabu, змінив позицію та допоміг запроторити в тюрму Девіса й інших. Після того як Монсегюр почав працювати під прикриттям на ФБР в обмін на значно пом'якшений вирок, він заохочував хакерів підривати більше мішеней і неодноразово звертався до Ассанжа та Джейка. Це наводить на думку, що стосовно обох провадили розслідування.

ФБР була не єдиною організацією, яка просочилася в «Анонімус». Звичайні злочинці використали груповий протест проти політики *Sony Corporation*, щоб увійти й викрасти номери кредитних карток. У Росії теж була істотна кількість представників в «Анонімусі»[9]. У ретроспективі цікаво, що деякі члени «Анонімусу» пізніше підуть працювати на Москву. Одна з них, Касандра Фейрбенкс, перейшла від участі в демонстраціях «Анонімусу» в реальному світі до відвідування та висвітлення протестів *Black Lives Matter* та активного підтримування Берні Сандерса на праймериз 2016 року. Маючи понад сто тисяч підписників у Твіттері, вона отримала роботу в російському інформаційному агентстві *Sputnik* і почала

голосно підтримувати Трампа на виборах 2016 року й після них. Якраз перед листопадовим голосуванням вона з'явилася на ютуб-каналі теоретика змов Алекса Джонса, кажучи, що «дуже ймовірно», що *gmail*-акаунт Джона Подести, голови передвиборчої кампанії Гілларі Клінтон, містив закодовані посилання на педофілію.

Монсегюру подобалося розповідати про свою політичну роботу. Він сказав журналістам, що дуже давно займався хакінгом заради вищої мети, протестуючи проти бомбардування ВМС США Пуерто-Рико, де мешкала його родина. Також він заявив, що 2001 року порушив роботу китайських вебсайтів, як робили інші прихильники *Hacktivismo*. Монсегюр повідомив, що приєднався до «Анонімусу», коли рух боровся з *PayPal* і *Visa*, та перемістився від галасливого основного ретрансльованого інтернет-чату до елітніших каналів планування, серед яких був і той, що став *LulzSec*. Найразючіша історія: у межах операції «Анонімусу» «Туніс», у період Арабської весни, він особисто вивів з ладу вебсторінку прем'єр-міністра країни, який схвалив масове зламування комп'ютерів громадян. Але підтвердити цей та інші відносно благородні вчинки виявилося неможливо. Авторка Олсон описала туніський епізод як роботу Монсегюра, посилаючись на нього як на єдине джерело. Професорка Габріелла Колман отримала архів записів чату й повідомила, що Монсегюр не очолював команду, яка порушила роботу вебсторінки прем'єр-міністра. У будь-якому разі навіть кілька з решти прихильників Монсегюра погодилися б, що він затятий брехун. Його прозаїчніші злочини, як-от крадіжки автозапчастин і номерів кредитних карток, узагалі не були таємницею.

Ще один центральний член *LulzSec*, 16-річний Мустафа tflow Аль-Бассам, іракський біженець у Лондоні, зробив дещо сміливіше, ніж спотворення вебсайту. З допомогою місцевого тунісця, який отримав фішингові електронні листи від уряду, Аль-Бассам проник у сервер, що надсилав листи, та змінив шкідливу програму так, що вона припинила функціонувати.

Як і в ситуації з Монсегюром, у розважливості Ассанжа невдовзі сумніватимуться. Розшукуваний для допиту у шведському розслідуванні сексуальних домагань, 2012 року Ассанж програв апеляцію щодо рішення про екстрадицію, втік до посольства Еквадору в Лондоні та залишився там. Після того як Ассанж вилаяв шведських обвинувачів зі своєї схованки, дехто з *cDc*, хто не висловлював своєї думки, перейшов в опозицію. Але поки наростав той фурор і *WikiLeaks* сильніше зосереджувалася на розкритті американських секретів, Джейк тримався свого курсу. Та відданість зробила його рок-зіркою інформаційної безпеки для тих, хто залишився прихильником Ассанжа. Однак він спричинив нову напруженість у *cDc*.

У приватному листі членам *cDc* Лейрд написав, що стурбований відходом інших стійких прихильників *WikiLeaks*, ситих донесхочу владними манерами й хизуванням Ассанжа. Це означало, що група покладалася на людину, яка виявляла себе щоразу менш надійною. «Я чув, що в Ассанжа були проблеми з жінками задовго до розголошення цієї шведської історії,— написав Лейрд.— Чи утихомириться Ассанж, поки хмара навколо зґвалтування не розсіється? Аякже! Йому завжди мало уваги преси. Тому якщо його засудять за певний злочин сексуального характеру, це,

на мою думку, повністю зруйнує *WikiLeaks»*. Джейк кинувся захищати Ассанжа як візіонера, відкидаючи скарги жінок як «шукання слави».

[x x]

Ослаблена репутація *WikiLeaks*[10] була причиною, чому 2013 року Едвард Сноуден не звернувся до неї зі своїми документами, хоча Ассанж пізніше доручить колезі переправити його з Гонконгу до Москви. Надихнувшись Декларацією незалежності кіберпростору Джона Перрі Барлоу, Сноуден носив на роботі в АНБ светр із логотипом *Electronic Frontier Foundation*. Коли він визнав потрібним попередити світ про те, що робить його агентство, він спочатку анонімно звернувся до нового відгалуження *EFF* під назвою Freedom of the Press Foundation, яке заснували на підтримку *WikiLeaks* Джон Барлоу, викривач «Документів Пентагону» Деніел Еллсберг, Ксені Жардін із журналу Boing Boing і кілька працівників *EFF*. Один із них порадив Сноудену зв'язатися з директоркою *Freedom of the Press Foundation* Лаурою Пойтрас, яка знімала фільм про *WikiLeaks*, і колишнім колумністом вебсайту *Salon* Ґленном Ґрінвальдом у британській The Guardian. The Guardian оприлюднила багато з найважливіших одкровень зі скарбниці Сноудена, але ці двоє також співпрацювали з іншими виданнями, як-от *Washington Post* і *New York Times*.

Пізніше Джейк передав інші матеріали для *Der Spiegel*[11] у Німеччині, ідучи ще далі в розкритті конкретних можливостей США. Хоча було заведено вважати, що документи, згадувані в повідомленнях, надійшли від

Сноудена, інформація з них не цитувалася в *Guardian*, *New York Times* чи *Washington Post*, хоч ці видання й мали доступ до основних архівів Сноудена. Це натякає на декілька можливостей: у *Der Spiegel*, можливо, був інший стандарт публікування, матеріал міг надійти від іншого, досі невідомого джерела, або його могли отримати навіть через російські хаки, які потім злили інформацію у *Der Spiegel*.

Сноуден показав, як активно уряд США співпрацював з американськими технологічними компаніями та використовував їх, поглинаючи записи внутрішніх телефонних дзвінків, просіюючи електронні листи в пошуках конкретного контенту та досліджуючи комунікації в інших країнах, не захищених конституційною забороною на необґрунтовані обшуки й затримання. У *Google*, наприклад, не усвідомлювали, що АНБ проникало в її мережі за кордоном, і швидко почали зашифровувати внутрішні трансфери користувацьких даних. В інших повідомленнях ішлося, що АНБ продовжує шкодити продуктам з гарантування безпеки[12], сплачуючи за вбудування в них бекдорів чи просуваючи стандарти, які можна обійти, як-от генератор псевдовипадкових чисел *Dual_EC_DRBG*. Конгрес не ухвалив великих реформ, і гнів в інших країнах прискорив балканізацію інтернету та введення націоналістських політик, які негативно позначилися на американських провайдерах. Водночас розкриття інформації інтенсифікувало роботу над безпечнішими альтернативами.

Однією з найперспективніших був *Signal*, розроблений командою видатного анархіста й колишнього волоцюги Моксі Марлінспайка та випущений 2014 року. Викриття

Сноудена достатньо повпливали, щоб протокол наскрізного шифрування в *Signal* став широко розповсюдженим навіть без відома більшості його користувачів. Засновниками *WhatsApp*, надзвичайно популярного застосунку для обміну текстовими повідомленнями на смартфонах, були Ян Кум і Браян Ектон. На початку 2014 року вони продали свою компанію «Фейсбуку» за 19 мільярдів доларів і зберегли деяку незалежність в управлінні нею. Кум був членом давньої хакерської групи w00w00, до якої належав Адам О'Доннелл із *cDc* і Дуг Сон, один із друзів *cDc*. Сон наполегливо радив Куму звернутися до Марлінспайка[13], і Кум погодився, коли Ектон запропонував, щоб WhatsApp використав технологію Signal з відкритим кодом, захищаючи мільярд осіб від масового спостереження. 2018 року Ектон пожертвує 50 мільйонів доларів на створення фонду для подальшого поширення *Signal* і стане його головою, згадуючи нагоду[14] «зробити важливий внесок у життя суспільства створенням стабільної технології, яка поважає користувачів і не хоче перетворення персональних даних на товар». Пізніше він сказав, що його мотивувало «збільшення обсягу запитів від правоохоронних органів і бажання зробити ті запити марними». Кум залишився у «Фейсбуку», де був одним із лише трьох керівників, які також працювали в правлінні компанії. Хоча він продовжив керувати *WhatsApp*, «Фейсбук» почав вимагати більше, ніж очікувалося, даних про користувачів застосунку, збільшуючи дохід від реклами, водночас піддаючи користувачів більшому корпоративному й урядовому контролю. У середині 2018 року Ян Кум піде з «Фейсбук».

[x x]

2012 року Джейк переїхав до Німеччини та витратив більше часу на популяризацію *Tor*, ніж на написання його коду. Він додавав своє ім'я до статей з досліджень інших питань безпеки, які привертали велику увагу, але пізніше деякі співавтори поскаржилися, що він попросив вписати його, щоб використати свою славу для просування роботи.

Джейк на різні лади виявляв свою нестриманість: хвалився минулою роботою на БДСМ-порносайт і пропонував секс на першому побаченні, навіть у професійному середовищі. Він вихвалявся великою кількістю коханок[15] і був у стосунках з Лаурою Пойтрас, яка пізніше визнала, що він жахливо поводився з її подругою та Ксені Жардін із Boing Boing. Джейк розповідав, як прокинувся в ліжку з Ассанжем і двома жінками, і відвідував приватні секс-вечірки (частіші в хакерській культурі, ніж десь іще). Він відкидав норми середовища навіть там. Як розповідав його давній приятель Енді Айзексон: «Чудові таланти Джейка мають ті самі чинники, що і його провал. Він дуже розумний і впертий». Головний урок, сказав він, полягає в тому, що «аб'юзери можуть використовувати слабко керовані організації як мисливські угіддя».

Жертви розповіли, що як першокласний соціальний інженер Джейк експлуатував свою роль провідника до видатного статусу, що змусило багатьох дійти висновку: їх витиснуть, якщо вони відмовлять. Він переслідував більше молодих жінок у спільноті *Tor*, де навесні 2015 року скарги призвели до його звільнення з посади

на десять днів. Це не стримало його. На щастя, того року давня керівниця *EFF* Шарі Стіл обійняла посаду генеральної директорки Tor і започаткувала відповідальніше лідерство.

Для деяких вона прийшла запізно[16], як-от для молодої інженерки Челсі Комло, яка зацікавилася безпекою після промови Джейка про Сноудена у своїй компанії. У грудні 2015 року Комло прибула в Гамбург на Всесвітній конгрес хакерів і після заходу поїхала відпочити з іншими до Берліну. Вночі 1 січня у квартирі Джейка вона знепритомніла, а коли отямилася, Джейк кохався з нею без її згоди. Пізніше вона відкинула його неодноразові вимоги сексу перед іншими та з іншими, але сталося і те й те. Вдома вона довірилася людям, які були знайомі з іншими жертвами, та зв'язалася з ними. Прихід Шарі Стіл у *Tor* надав їм надію, що зміни можливі. Щоб захистити себе та попередити інших, вони поговорили зі Стіл і створили вебсайт, на якому під псевдонімами розповіли свої історії про насильство та примус. «Для мене дуже важливо, щоб з новими людьми, які приходять у спільноту, не сталося те саме, що зі мною»,— говорила Комло.

2 червня 2016 року Джейк звільнився, але *Tor* не пояснив причину у своєму оголошенні. Тільки після запуску анонімного вебсайту наступного дня, у суботу, Стіл визнала, що за виходом Джейка стоять конкретні обвинувачення в сексуальному насильстві та розслідування. Протягом півтора року деякі жертви назвали себе, серед них Челсі Комло та Лі Ганівелл, канадська інженерка безпеки для великих технологічних компаній. Ганівелл розповіла, що десять років тому, коли вони були в нерегулярних стосунках за взаємною

згодою, Джейк проігнорував стоп-слово і повівся як ґвалтівник. «Стосунки з ним були постійним потоком принижень,— написала Ганівелл на своєму сайті.— Він ображав мене на очах в інших і ділився подробицями нашого інтимного життя з друзями, які часто були його колегами»[17].

Джейк відбивався, частково з допомогою медійних знайомств, які сумнівалися в деяких розповідях. Він заперечував найгірші обвинувачення, погрожував жінкам позовами й натякав, що причини атак на нього криються в його роботі, пов'язаної зі свободою слова та безпечними технологіями. Однак з'являлися нові повідомлення, і сукупність доказів проти нього зростала. *«Tor* дав цьому раду так, як ви хотіли б і сподівалися»,— сказала Челсі Комло. Вона отримала запрошення на конференцію Tor наступного року, почала писати код для проєкту. Згодом її призначили основним співробітником. Вона сказала, що це особливо надихає через домінування чоловіків у галузі й тому, що жінок з більшою ймовірністю переслідують. «Безпека та приватність — дуже важлива сфера для жінок, адже в ній відбувається багато міркувань з етичних тем, і ви працюєте тут, тому що хочете захистити людей. Це має бути щось, що знаходить розуміння не тільки в гетеросексуальних білих чоловіків».

Проєкт *Tor* замінив увесь склад правління. Навіть наставник Джейка Роджер Дінгледайн і Нік Метьюсон відійшли, хоча залишилися провідними працівниками. Люди, які брали участь у процесі, сказали, що за минулого ладу лідерства не було, а керівники постійно відкидали те, що їм розповідали про Джейка. Один співробітник сказав: «Тебе характеризують речі, які ти

вважаєш припустимими та неприпустимими»[18]. Серед нових директорів були Сінді Кон з *EFF*, експерти з криптографії Брюс Шнаєр і Метт Блейз та Габріелла Колман, антропологиня, яка простежила історію «Анонімусу». За кілька днів *Freedom of the Press Foundation*, де Джейк був членом правління, понизив його до неоплачуваного консультанта. *Noisebridge*, величезний хакерський простір у Сан-Франциско, співзасновником якого був Джейк, повідомив, що він може не повертатися.

Серед перших захисників Джейка були деякі оператори вузлів *Tor*, співзасновник *EFF* Джон Гілмор і Деніел Дж. Бернштейн, криптограф з антиурядовими настроями, який кілька років тому допоміг послабити правила експорту. Більшість застерігала від похапливих суджень без судового процесу. Нинішній професор у Нідерландах і видатна фігура у поширенні не підтримуваного АНБ шифрування Бернштейн залишив Джейка своїм аспірантом.

Новини були особливо болісними для *cDc*, яка з допомогою інших хакерів сформувала репутацію Джейка. Його поведінка зробила наголос на чоловічому домінуванні в галузі безпеки загалом та в хакерському соціальному світі зокрема. Що найгірше, Джейк втілив темну сторону формули *cDc* — медійно грамотну, зневажливу до меж особистість, яка здатна підвищити громадську обізнаність, але водночас тішить своє ненаситне его.

Спільні цінності попри різні погляди та галузі знань зробили *cDc* особливою, і цю особливість було зруйновано. «Ті з нас, хто колись був знайомий

з Джуліаном, завжди знали, що він якийсь паскуда. Здебільшого через це особисто я завжди з підозрою ставився до *WikiLeaks*,— сказав Пол Леонард.— Усі пояснення коріняться в суті *cDc*, ба більше, у причині, чому Джейк Еплбаум вдарив нас настільки боляче. Йдеться про міру, до якої *cDc* функціонувала як сімейна ланка».

[x x]

cDc могла б нічого не сказати. Вона була не настільки відомою, як десятиліття тому, і багато статей про Джейка не згадали б його зв'язок з нею. На честь групи, її географічно віддалені члени поквапилися вжити заходів до того, як з'явився сайт анонімних жертв чи проєкт *Tor* склав своє оголошення про звільнення Джейка в одному реченні. Джейк досі був у списку розсилки *cDc*, тому обговорення мали відбутися десь в іншому місці, у менших ланцюжках листів. Люк повідомив Кевіну та Лейрду про перші обвинувачення у Твіттері. Крістіан Ріо написав Міші Кубеці. Їхнє занепокоєння супроводжувалося обережністю.

«Це погані новини, але перш ніж ми вживатимемо якихось внутрішніх заходів, я хотів би побачити більше свідчень, крім лише декількох від випадкових осіб у Твіттері»,— написав Люк. Міша висловився відверто: «Чорт забирай. Що там таке з людьми *WikiLeaks* і зґвалтуваннями?» Після того як Крістіан знайшов вебсайт анонімних обвинувачів і відправив посилання, вранці суботи Лейрд обміркував події, кажучи, що знав, що жінки намагаються зібрати проти Джейка свідчення про зґвалтування, та що він чув деякі огидні розповіді

про сексуальні «завоювання». «Він може бути цілковитою наволоччю,— написав Лейрд.— Я сам стикнувся з цим, коли приймав його в Індії. Він викинув там декілька дурних фортелів». Люк додав до обговорення Адама О'Доннела, і вони запропонували розібратися з роллю Джейка в скандалі.

У неділю почали надходити нові повідомлення, і друг групи Нік Ферр відкрито написав про те, як йому погрожували Джейк і його прихильники. Це сталося після того, як Ферр погодився на вимогу Джейка скасувати на Всесвітньому конгресі хакерів п'ятихвилинний виступ людини, яка заявляла, що Джейк — інформатор американської розвідки. Ферр відмовився передати Джейку своє листування з потенційним спікером. «Щовечора я повертався до свого готельного номера і бачив на подушці друковану записку: "Не примушуй нас до крайніх заходів. Віддай усе"». Ферр сказав, що поговорив з людьми, яким він начебто міг довіряти, але всі вони порадили йому знайти компроміс. «Не можна вести розмову з соціопатом,— написав Ферр.— Ще гірше, коли люди, яких ти вважаєш перевіреними друзями, стають на його бік»[19].

Цього було достатньо, щоб Лейрд захотів зробити публічну заяву, й Адам з ним погодився. Ще не отримавши відповідь Кевіна, Люк попросив Мішу видалити Джейка зі списку розсилки, щоб можна було надіслати рішення та заяву всій групі. Нарешті, пізно ввечері в неділю, Кевін вийшов на зв'язок і сказав, що хоче без шуму видалити всі сліди Джейка з сайтів *cDc*, зокрема й зі списку колишніх вихідців групи. «Мені дуже шкода за свою роль у прийнятті цього хлопця. Це була дурість,— написав він.— Я усвідомив, що в таких

ситуаціях особистість абсолютно важливіша за навички. Правдиві ці заяви чи ні, йому не місце серед нас». Група переконала Кевіна, що їй потрібне публічне дистанціювання. Вони склали свою найсерйознішу за більш як десятиліття публічну заяву[20] та розмістили її на домашній сторінці *cDc* і відкритій тоді групі *cDc* у Фейсбуку, у якій ділилися інформацією багато членів і фанатів.

«Як і більшій частині хакерської спільноти, нам було неприємно почути заяви про сексуальне насильство, маніпуляції та знущання з боку одного з наших членів, Джейкоба Еплбаума, відомого також як IOerror»,— говорилося на початку тексту.

Нам також відомо, що проєкт Tor провадить внутрішнє розслідування, і заохочуємо виступити кожного, хто може дати свідчення у справі. Для когось це буде нелегко. Може бути осуд, приниження чи страх, що тобі не повірять. Ми відповідальні за створення середовища, у якому люди можуть не боятися виступити зі свідченнями. Ми завжди відстоювали свободу слова та самовираження, яка іноді робить потрібним право на анонімність. Це те, чого часто вимагають жертви насильства. Ми захищаємо їхнє право бути анонімними. Інші, як-от наш друг Нік Ферр, який вирішив відкрито розповісти про свої труднощі, заслуговують нашої поваги та підтримки. Кожен робитиме це на свій лад. Ми знаємо, що це може бути лячно, але ми заохочуємо жертв звернутися до відповідних місцевих органів влади. Ми розуміємо наші складні відносини з законом, але зараз час і місце для втручання держави. Якщо найсерйозніші

з цих заяв правдиві, слід розглянути їх у суді та вжити відповідних заходів.

«КУЛЬТ МЕРТВОЇ КОРОВИ» відомий багатьма справами, але жахливе поводження з людьми до них не належить. Якщо спільноти хочуть процвітати й зберегти свою актуальність, іноді потрібно робити чистку. Дізнавшись про анонімні обвинувачення в сексуальному насильстві та почувши розповіді від людей, яких ми знаємо та яким довіряємо, ми вирішили негайно виключити Джейка з групи.

В особистому дописі у Medium[21] Лейрд висловив надію, що усунення Джейка допоможе інформувати інших про системний сексизм у хакерському світі, загострений схильністю до порушення правил, недовірою судових установ до повідомлень про правопорушення та надмірним прагненням відповідати певним стереотипам: «Коли впливові люди переступають межу, у хакерському світі часто дивляться на це крізь пальці. Це має припинитися».

На здійснення цього побажання не довелося довго чекати. Коли восени 2017 року активізувався масштабний рух проти сексуального насильства і сексуальних домагань, відомий як #МеТоо, хакерська спільнота піднялася проти інших обвинувачених. Навіть Джона Дрейпера (відомого як Капітан Кранч), який часто відвідував хакерські конференції, нарешті вигнали за домагання до неповнолітніх хлопчиків і заборонили йому приходити на збори. Прессекретарка Дрейпера заперечила його поведінку.

Принаймні Джейк пішов із *cDc* до виборів 2016 року, коли його зв'язок з *WikiLeaks* був би непростимим для всіх у групі. *WikiLeaks* буде центральним, партизанським гравцем в обранні Трампа, який щедро хвалив її протягом своєї виборчої кампанії. *WikiLeaks* радісно оприлюднила електронні листи, вкрадені агентами російських спецслужб у Національного комітету Демократичної партії напередодні її з'їзду в момент, коли їх можна було розкрити з максимальним ефектом. За кілька годин після того, як кампанію Трампа сколихнула публікація відео, на якому він хвалиться хапанням жінок «за кицьку», WikiLeaks почала вивалювати викрадені електронні листи Джона Подести. Тим часом давно обіцяні витоки про Росію так і не матеріалізувалися. Й - Ассанж неодноразово намагався відкинути підозри в дезінформації, заперечуючи, що джерелом була Росія, та натякаючи, що це був співробітник Національного комітету Демократичної партії. Влітку 2018 року звинувачувальний висновок щодо причетності дванадцяти російських офіцерів розвідки посилатиметься на електронні листи між *WikiLeaks* і її справжнім джерелом[22], створеною росіянами особистістю під псевдонімом Guccifer 2.

Джейк та Ассанж були далеко не єдиними, хто драпірувався в знамена моралі та водночас переслідував інші цілі. Вони були лише найвидатнішими прикладами. Починаючи з 2016 року, багато начебто хактивізму буде дечим іншим, що ховається під його маскою.

Розділ 11.
МІКСТЕР, МЮНЧ І ФІНЕАС

Хоча Джейк Еплбаум і став прикладом негативного впливу «Культу мертвої корови», він був не єдиним. Едвард Сноуден зірвав завісу та показав симбіоз західних розвідувальних служб і великих технологічних компаній. Члени cDc влилися до обох сторін тих відносин, і обидві втратили моральний блиск. Але незабаром вихідці з *cDc* гратимуть з усіх сторін динамічної заплутаної боротьби між шпигунами в багатьох країнах, їхніми постачальниками технологій і ворогами тих постачальників — з моральних причин, як-от *Citizen Lab*, і з причин геополітичних. Крім того, будуть анонімні герої-месники, чиї мотиви важко зрозуміти. Здебільшого вони залишилися прихованими, захищені технологічною майстерністю найкращих хакерів або інструментами, наданими державою.

Першопричиною всього цього безладу була поглиблена інтеграція майже незахищеного інтернету в усі великі економіки протягом аморального зрушення технологічної галузі у 2000-ні. Коли це сталося, використання урядами слабких місць у системі безпеки на свою користь було неминучим. Можна не додавати, що вони проігнорували дослідження базового захисту, але вони це зробили. Отже, явище, яке в *cDc* назвали близькою катастрофою на межі тисячоліття,— неякісний софт, неосвічені покупці та незацікавлені державні службовці,— значно загострилося протягом наступних

десяти років. Замість діяти, можливо, за згодою, щоб поліпшити безпеку чинника економічного розвитку для всіх, уряди підтримували чорний ринок знань про конкретні вади програмного забезпечення та методи їхнього використання для шпигунства. Для деяких головними мішенями були правозахисники, журналісти та політики з партій меншості. Становище людей, яких хотів захистити Лейрд Браун і його однодумці, тепер було набагато гіршим, ніж десятиліття тому. «Коли я був молодим, у незахищеності інтернету було щось розважальне»[1],— поділився думкою винахідник *Signal* Моксі Марлінспайк. Він відкривав можливості для будь-кого, хто був достатньо винахідливим, щоб отримати користь попри свій статус аутсайдера. Тепер «незахищеність інтернету використовують люди, які мені неприємні, проти тих, хто мені подобається: уряд проти - громадян».

Звісно, багато з тих, хто зрештою постачав інструменти не тим людям, починав з добрих намірів, як-от ранній прихильник проєкту *Hacktivismo* Мартін Мюнч[2]. Коли німецький хакер Кемаль Акман під ніком Мікстер (Mixter) розробляв систему *Six/Four* для Лейрда, новий член cDc приєднався до мюнхенського стартапу *Ciphire Labs*, який прагнув розробити зашифровану поштову систему. Кемаль допоміг Лейрду працевлаштуватися там і шукав у компанії людей, які могли б стати волонтерами для *Hacktivismo*. Мюнч, яскравий і блискучий юнак, здавався Кемалю ідеальним кандидатом. Він додав його до списку розсилки Hacktivismo, у якому було приблизно двадцять стабільних учасників і вдесятеро більше пасивних читачів. Крім того, Кемаль познайомив

молодого чоловіка з іншими, кого він знав у берлінській спільноті, зосередженій навколо *Chaos Computer Club*.

«Мартін був ідеалістом,— пригадував Кемаль.— Я повністю довіряв йому». Але Мюнч «хотів бути рок-зіркою», і це теж вплинуло на його кар'єрний шлях. Він сказав Кемалю, що хоче допомогти поліції схопити найгірших з найгірших, виробників дитячої порнографії, і пішов з *Ciphire Labs*, щоб працювати над софтом, який, за його словами, міг би принести користь. Оскільки Кемаль найняв і навчив Мюнча та познайомив його з берлінськими хакерами, налаштованими захищати права людини, він почувався винним за те, що сталося далі. «Я привів Мартіна. Я частково відповідальний за його кар'єру,— казав він.— Особисто мені він здавався трохи дивним». Лейрд сказав, що досі вважає Мюнча другом, тим, хто втратив контроль над проєктом через боротьбу всередині заснованої ним компанії, а не через аморальний вибір.

Хай якою була причина, система Мюнча стала наступною точкою загоряння у ворожнечі через хакінг, безпеку та приватність. Так само як з *WikiLeaks*, суперечки вийдуть за професійні кола та залучать громадськість і медіа до обговорення балансу сили між урядами та звичайними громадянами. Хоча полювання Росії було таємним, вона фігурувала в істотній частині тих обговорень, можливо, у зв'язку з Мартіном Мюнчем і напевно у зв'язку з хакерськими інструментами, використовуваними АНБ. Не тільки *cDc* почала змішувати політичні мотиви та роботу над безпекою в історії з «Гонконгівськими блондинками»; два десятиліття збільшення геополітичного впливу на

справи хактивізму ускладнили розрізнення реальних дійових осіб і цілей багатьох публічних хаків.

Скромна програма Мюнча, перетворена на шпигунський софт, називалася *FinFisher*, або *FinSpy*. Кемаль вважає, що джерелом натхнення для проєкту була *Back Orifice 2000*, і Мюнч, можливо, використав щось з її відкритого коду. Але Крістіан Ріо націлювався тільки на комп'ютери з *Windows*. *FinFisher* Мюнча атакувала Windows і комп'ютери *Apple*, смартфони з платформою *Android* і *Apple*, інші пристрої та більшість операційних систем. Були й інші відмінності. *Back Orifice 2000* міг використати хто завгодно, але для інсталяції тим користувачам було потрібно знайти робочий експлойт чи довірливу жертву. Компанія *Gamma Group*, що продавала *FinFisher*, пропонувала трюки для інсталяції програми на пристроях. Мюнч очолив розробку продукту та офіс *Gamma Group* у Мюнхені. *Gamma Group* мала головні офіси у Великій Британії та афілійовані компанії в Сингапурі й інших країнах, які продавали начебто тільки державним установам з усталеною репутацією.

2008 року Кемаль дізнався про зв'язок Мюнча з *Gamma Group*. 2011 року активісти проникли на галузеві виставки, відомі як «Бал перехоплювачів», і залишили 60-сторінковий каталог *Gamma Group*[3]. «*FinFisher* — портфоліо найновіших інструментів електронного вторгнення на сучасному ринку»,— зазначалось у ньому. Портфоліо містило разючі шпигунські програми, призначені для смартфонів. Їх дуже важко виявити, можна застосовувати віддалено, і вони не тільки перехоплюють голосові дзвінки й електронні списки контактів, а й перетворюють телефони на постійні пристрої спостереження. Того ж року, протягом

Арабської весни, єгипетські повстанці виявили, що схожу пропозицію зробили Державній службі розслідувань інцидентів безпеки. У *Gamma Group* сказали, що угода не відбулася, що компанія дотримується законів про експорт і продає свої продукти тільки урядам, які використовують їх для боротьби зі злочинністю.

Але активісти підозрювали, що репресивні режими, щодо яких введено санкції, як-от Судан, використовують *FinFisher* проти законослухняних дисидентів. 2012 року *Bloomberg News* здобула потенційно заражені електронні листи, відправлені бахрейнським активістам, і передала їх *Citizen Lab*. Команда *Citizen Lab*, очолювана експертом з безпеки з *Google*, глибоко занурилася в дослідження. Вона встановила, що зараження мають стосунок до *Gamma Group*, як вони відбуваються та що дані від жертв мали надходити в телекомунікаційну компанію уряду Бахрейну. *Citizen Lab* виявила сервери *FinFisher* у десятках країн, як-от в ОАЕ, Ефіопії та В'єтнамі, де об'єктами атак були блогери. Серед технологічних трюків, застосовуваних компанією, було втручання в процеси оновлення програм і використання експлойтів у засобах *Adobe Flash*.

Два роки по тому хтось жахливо зламав *Gamma Group*. Хакер зареєстрував пародійний твіттер-акаунт @GammaGroupPR і розмістив посилання на викрадені файли з вихідним кодом, листами клієнтів та інший компромат, зокрема діаграму, яка показувала, що 2009 року країнами з найбільшою кількістю відвідувачів сторінок клієнтської підтримки були Нідерланди, Франція та Китай, а 2014-го — Китай і США. У працівників технологічної преси був вдалий день, дослідники-

активісти святкували подію, а неприбуткові організації подали в органи влади скарги, які заподіяли серйозну шкоду компанії.

2015 року @GammaGroupPR повернувся з оголошенням, що хакнув найвідомішого конкурента *Gamma Group*, італійську компанію *Hacking Team*. Як і в історії з *LulzSec* і *HBGary Federal*, хакери з задоволенням звернули публічну увагу на слабку захищеність компанії. Вони знову виклали вихідний код, списки клієнтів, які свідчили про очевидні порушення санкцій, і скандальні електронні листи. Інструменти *Hacking Team* використовували проти ефіопських журналістів й інших невинних людей, зокрема декількох у США. Той, хто контролював акаунт @GammaGroupPR, назвав себе Фінеасом Фішером і пізніше в інтерв'ю журналу Vice сказав, що атакував обидві компанії за грубе порушення прав людини. «Я прочитав звіти *Citizen Lab* про *FinFisher* і *Hacking Team* та подумав: "От срака повна!" І я їх хакнув,— пояснював він.— Сподіваюся, це принаймні трохи їх стримає та дасть віддихатися людям, які були атаковані їхніми програмами»[4]. У тому інтерв'ю, проведеному в електронному чаті в липні 2016 року, Фінеас послуговувався простою англійською та посилався на рух *Antisec*. Він охарактеризував себе «революціонер-анархіст» та оприлюднив посібники та маніфест, у якому заохочував інших зламувати своїх пригноблювачів.

У ще одному інтерв'ю за місяць до того[5] Фінеас зізнався у зламуванні профспілки каталонської поліції та оприлюдненні домашніх адрес понад п'яти тисяч офіцерів. Він назвав це «маленьким ударом по владі» та

заперечив, що він іспанець чи що говорить іспанською або каталонською. Попри це, саме географічне положення об'єкту атаки сприяло припущенням, що Фінеас — зацікавлений у політиці хакер з того регіону.

Трюки Фінеаса повели оригінальний рух *Antisec* і проникнення в *HBGary* саме в тому напрямку, у якому пішли б попередні хакери, які були готові порушити закон. Він використав свої знання про влаштування світу, щоб ускладнити використання технології для утисків. Після Фінеаса відбувся витік матеріалів, викрадених у *Cellebrite*, ізраїльської технологічно-криміналістичної компанії, яка проникає в телефони на запит правоохоронних органів, і у виробників *FlexiSpy*, софту, яким користуються батьки, щоб стежити за дітьми, та романтичні партнери, щоб шпигувати одне за одним. (Деякі публікації називали *Cellebrite* компанією, яка допомогла зламати *iPhone* терориста, що вбив державних службовців у Сан-Бернадіно, Каліфорнія, після відмови *Apple*.) Хакери віддали належне Фінеасу та оприлюднили оновлений посібник з безпеки та хакінгу для фанатів. «Якщо ви хакер, дійте у відповідь,— написали вони.— Якщо звичайна людина, бережіть себе. Дивіться, що відбувається і що говорять про те, як виявити *FlexiSpy* та захистити себе... Якщо ви постачальник шпигунських програм, ми прийдемо за вами[6]. Зупиніться, обміркуйте своє життя, знищте свою компанію та станьте кращою людиною. Або ж ви невдовзі нас побачите». Ґабріелла Колман, дослідниця історії «Анонімусу» та викладачка в Університеті Макгілла, назвала цю тенденцію зародженням «хакінгу в громадських інтересах»[7]. Цілком імовірно, що причиною принаймні деяких з понад півтора десятка

викриттів шпигунського софту були протести проти поведінки постачальників.

[x x]

Утім, варто поглянути на підбурювача Фінеаса ще раз у світлі вторгнення в Національний комітет Демократичної партії (НКД) та оприлюднення інструментів АНБ. Основні відомості про вторгнення в НКД і комп'ютери службовців Демократичної партії протягом виборів 2016 року чітко встановлені слідчими США, включно з тими, хто працював на спецпрокурора Роберта Мюллера. Одне проникнення в НКД відбулося невдовзі після публікації серії статей про «Панамські документи»[8], які показали, що друзі Путіна приховували за кордоном мільярди доларів. Путін обвинуватив Клінтон у витоці файлів юридичної фірми, що реєструвала офшори. З огляду на те, що розвідка США - дійсно обговорювала викриття корупції Путіна, він міг мати слушність, що це була операція ЦРУ. Хоча Ассанж намагався поставити під сумнів особистість того, хто передав WikiLeaks вкрадені електронні листи, російська розвідка очевидно була рушієм атак на НКД і пов'язаних із ними хаків. Guccifer 2, який злив деякі викрадені в АНБ дані та заявив, що є румуном, одного разу забув використати віртуальну приватну мережу та розкрив своє справжнє місцеположення — Головне розвідувальне управління Росії (ГРУ). Росія також організувала публікацію електронних листів й інших документів у *WikiLeaks*.

Зі вторгненням в АНБ ситуація не настільки чітка. У серпні 2016 року, за лічені тижні після припинення

хвастощів Фінеаса, хакерська група, що називала себе *Shadow Brokers*, почала оприлюднювати у Твіттері не тільки вразливості у Windows, маршрутизаторах Cisco й інших програмах, а й робочі експлойти — всі вони належали АНБ. Більша частина інформації надійшла наприкінці 2013 року, після втечі Едварда Сноудена з агентства. Це означає, що був ще один «кріт», або злам комп'ютерного устаткування агентства, або необережний працівник, комп'ютер якого зламали. *Shadow Brokers* діяли в тому самому дусі місяцями. Деякі з розкритих ними трюків згодом використали інші хакери, як-от, за припущеннями, північнокорейські розповсюджувачі програми-вимагача *WannaCry*, яка 2017 року заблокувала роботу багатьох установ по всьому світу. Зрештою, двох працівників АНБ звинуватили в тому, що вони принесли додому засекречені файли. Принаймні один з них використовував на своєму персональному комп'ютері антивірус *Kaspersky*.

Це викликало особливу занепокоєність, адже 2015 року в мережі *Kaspersky* проникли ізраїльтяни, дізналися, що програми використовувалися для пошуку засекречених документів США, і попередили американців. Розвідслужби дійшли спільної думки, що в такий спосіб росіяни отримали принаймні деяку інформацію *Shadow Brokers*. Викриття сильно вдарили по *Kaspersky Lab*, яка насолоджувалась успіхами від публічного розкриття американських висококласних шкідливих програм, починаючи зі *Stuxnet*. *Kaspersky* визнала, що отримала декілька секретних файлів від державного службовця США, хоча заявила, що видалила їх. США заборонили використання продуктів цієї компанії у федеральних органах влади.

У росіян були мотиви, засоби й можливість викрасти хакерські інструменти США. Крім того, Росія була одним із небагатьох підозрюваних, які мали стільки власних інструментів, що могли дозволити собі розкрити американські замість притримати їх для себе. Час подій особливо цікавий, оскільки витоки з АНБ почалися в серпні 2016 року, за два місяці після розкриття вторгнення в НКД. Росія влаштувала хаос і сум'яття в агентствах, які були найліпше здатні знайти джерело хакерських атак на НКД і здійснити контрудар.

Пам'ятаючи ту історію, варто переглянути особистість Фінеаса Фішера. У матеріалах провідних медіа майже не згадувалось, що *Gamma Group* і *Hacking Team* зазвичай не продавали Росії чи її найближчим союзникам. Вони продавали хакерські інструменти Заходу, а Фінеас викрав їх і оприлюднив, так само як група *Shadow Brokers* зробить за кілька тижнів з інструментами АНБ. До того ж *Gamma Group* особливо цікавилася *Kaspersky*. Два колишні працівники Kaspersky повідомили мені[9], що компанія витягла неактивний код з комп'ютера *Gamma Group* після того, як хтось необачно встановив їхній антивірусний софт.

І ще є питання щодо вибору Фінеасом інших мішеней і щодо того, що нам тепер відомо як російська стратегія сіяння розбрату в Європейському Союзі, США та інши стратегічних країнах. Атака на профспілку каталонської поліції вписується в налаштування регіонів проти іспанського уряду, коли парламент Каталонії кинув виклик Конституційному суду Іспанії та провів референдум щодо незалежності. Коли Іспанія наказала усунути з посади каталонського лідера, лояльність поліції мала величезне значення.

Було б дивно, якби висококваліфікований, готовий порушувати закон і морально вмотивований хакер завдав удару Gamma Group і *Hacking Team* та був серйозно зацікавлений проблемами іспанської політики. Як мінімум, ви б очікували причетності іспанця до тієї комбінації. Але це не все, що зробив Фінеас. Він також здобув та оприлюднив дані звичайних турецьких громадян у період конфронтації Росії і Туреччини. Хоча цей контекст не висвітлювали в більшості матеріалів про хакінг, Росія і Туреччина перебували в конфлікті відтоді, як у листопаді 2015 року турецькі військові збили російський Су-24. У наступні пів року Путін збільшував тиск на турецького президента Реджепа Ердогана санкціями на імпорт турецьких продуктів і забороною на продаж турпакетів у Росії. Ердоган, жорстко переслідуючи медіа й активістів, втрачав популярність на Заході. Водночас Росія й Туреччина переслідували різні цілі в Сирії, країні-сателіті Росії. Ердоган мав вибрати між Вашингтоном і Москвою, та зрештою вибрав останнє. Хоч і вважалося, що збитий літак перебував у турецькому повітряному просторі, Ердоган відступив і в червні 2016 року написав Путіну: «Я ще раз висловлюю свій жаль і глибокі співчуття членам родини вбитого російського пілота і прошу в них вибачення»[10].

Ердоган запланував чистку серед військових, і це стало поштовхом до спроби державного перевороту в липні 2016 року. Росія була першою країною, яка засудила путч. Але у грі брало участь багато фігур водночас. Ослаблення влади Ердогана через спостереження за членами його партії мало б для Росії сенс, так само як розкриття персональних даних офіцерів каталонської поліції могло би допомогти влаштувати сум'яття.

Можливо, Росія робила ставки на обидві сторони конфлікту Ердогана та військових, тому, хай хто вийшов би переможцем, опинився б у неї в боргу. Хай там як, в оприлюдненні такої інформації було би більше сенсу для Росії, ніж для політично активного хакера в Іспанії чи деінде.

У поясненнях Фінеаса, що він намагався зробити і що пішло не так, сенсу обмаль. «Я хакнув ПСР (панівну партію в Туреччині), тому що підтримую суспільство, яке намагаються збудувати [курди] в Рожаві та Бакурі, і їх атакує Туреччина»[11],— написав він у липні. І він додав заплутану розповідь, чому було оприлюднено конфіденційну інформацію про звичайних людей. За словами Фінеаса, він дістав файл з електронними листами з серверів партії і надіслав його людям у неспокійних регіонах, запитуючи, що робити з цим доступом. Самі листи не були цікаві. Люди просили відремонтувати дорогу чи допомогти знайти роботу. У них не було нічого від Ердогана чи осіб з його близького оточення. «Між деякими з цих людей сталося непорозуміння»,— написав Фінеас, і хтось злив інформацію *WikiLeaks*. Він сказав, що хоча особа, яка передала файли, усвідомила помилку й попросила *WikiLeaks* не публікувати їх, вона все одно це зробила.

Але потім Фінеас сам оприлюднив нові файли, зокрема базу даних простих членів ПСР і, що гірше, базу даних майже всіх дорослих жінок у Туреччині, з мобільними номерами й адресами багатьох з них. Ті бази даних копіювали та поширювали люди на взір британського сек'юріті-активіста Томаса Вайта[12], який твітив в акаунті @CthulhuSec і зажив певної скандальної слави,

публікуючи результати багатьох великих хаків. *WikiLeaks* розмістила у Твіттері посилання на ті бази даних, наражаючи на небезпеку мільйони жінок, і розлютила колишніх прихильників Фінеаса, як-от активістку *Electronic Frontier Foundation* Еву Ґалперін. «Хто стоїть за не таким уже й чудовим витоком турецьких імейлів? — написала вона у Твіттері.— Це @GammaGroupPR, чиєю попередньою роботою я захоплювалася». Три місяці по тому Вайт припинив розміщувати посилання на злиті дані, скаржачись, що мотиви хакерів тепер дурні. Ще за три місяці Фінеас заявив журналу *Vice*, що зробить перерву в хакінгу[13].

Отже, перед нами хакер з надзвичайно розвинутими навичками, етичними мотивами й досить широким мисленням, щоб обрати своєю мішенню звичайних офіцерів поліції в Барселоні й турецьку панівну партію, але достатньо недбалий, щоб виставити на привселюдний огляд телефонні номери мільйонів жінок у патріархальному суспільстві разом з номерами пересічних членів партії. Здається малоймовірним. Навіть без зв'язку з *WikiLeaks* існує однаково логічне пояснення — Фінеас Фішер є проєктом російської розвідки. Це дійсно була особиста думка Вашингтону. У розвідці США «загалом припускають, що це росіяни», — сказав Джим Лівайс, давній впливовий високопосадовець Держдепартаменту та учасник переговорів з глобальних інтернет-питань.— Це узгоджується з російською діяльністю в інших сферах».

Якщо росіяни дійсно намагалися знищити *Gamma Group і Hacking Team*, вони мали власні інструменти для шпигування за громадянами й ворогами та просто ускладнювали життя західним урядам. Це не

обов’язково означає, що ті компанії не заслуговували викриття. Кемаль, наприклад, не вагаючись поаплодував витокам, навіть якщо вони походили з Кремля та завдали шкоди його старому другу Мюнчу. «Я дуже цьому радий,— прокоментував він оприлюднення інструментів *Gamma Group*.— Їх слід викрити й знищити».

[x x]

Навіть якщо Фінеас не росіянин, є підстави поглянути на картину загалом. Ми вимушені визнати, що хактивізм часто забруднений геополітикою — як це зробив Лейрд — і що викрити такий вплив неможливо. Якщо це мало тривожить, ось глибше усвідомлення ситуації. Могутні держави світу змагаються одна з одною відкрито і таємно, використовуючи зброю та гроші, дипломатію та шпигування, фальшивий активізм і відносини з громадськістю. Водночас більшість урядів має схожі інтереси стосовно свого народу. Ніхто з них не хоче, щоб громадяни мали можливість таємно спілкуватися, навіть у Сполучених Штатах. 2018 року ФБР досі виступало проти можливості використання людьми шифрування, яке постачальники не здатні зламати, і його союзники в Конгресі погрожували заборонити такий захист.

Кемаль побачив тенденцію посилення державної влади над особою настільки гнітючою, що 2011 року пішов з галузі безпеки, і надовго. Так само як інші в *cDc*, він вважав, що остання надія на збереження особистих свобод — найбільші постачальники на кшталт *Apple* та *Google*, які теоретично могли б нацькувати уряди один на одного та в процесі захистити користувачів, і подібні

до *Signal* приватні стартапи, які вважають, що прагнуть речей, важливіших за гроші.

Apple була на лінії фронту. Вона була родиною для ветеранів *@stake* Віндоу Снайдер, Девіда Лічфілда та Роба Бека й багатьох інших однодумців *cDc*. Деякі з них допомогли опиратися спробі ФБР примусити компанію до зламування *iPhone* терориста з Сан-Бернардіно. *Apple* стверджувала, що уряд може самостійно знайти спосіб зламати телефон і що її згода написати нову програму для цього означатиме висловлювання думки під примусом, що визнано неконституційним. ФБР програвало суперечку, коли раптом знайшла неназваного підрядника з вразливістю нульового дня, за допомогою якої можна було виконати завдання й закрити справу. *Google* була ще однією зоною бойових дій, у якій було повно членів і шанувальників *cDc*. Вона усвідомила, що АНБ — ворог, коли документи Сноудена викрили вторгнення агентства до її мереж за кордоном, де йому не був потрібен дозвіл суду. *Google* запровадила ретельніше шифрування. Обидві компанії також боролися з вимогами уряду щодо створення бекдорів і заборонами на наскрізне шифрування.

Усередині великих компаній теж відбувалася боротьба. Але провідні світила в битві за шифрування також витрачали більше часу на допомогу стартапам. Інші почали більше думати про значення свободи слова, коли гострою проблемою в багатьох країнах була не неможливість висловитися, а ризик загубитися серед штучних думок, керованих урядами та великими економічними силами. Лейрд та інші в *cDc* були в шоці від компаній, подібних до Gamma Group, і шкодували, що зіграли якусь роль у злеті кар’єри Мартіна Мюнча.

Але хоча вони, можливо, схвалювали дії Фінеаса, самі вони не хотіли порушувати закони. Коли хактивістські бойовища перемістилися до хакінгу, витоків та інформаційної війни, їм довелося шукати інші способи допомогти.

Повернувшись із Індії до Німеччини, Лейрд пішов працювати на колишнього гендиректора *Ciphire Labs*, провайдера зашифрованої електронної пошти, на якого також працювали Кемаль і Мюнч. У його ексгендиректора Еррікоса Піцоса була ідея платформи для серйозних дискусій, яку він назвав *Kialo*. Програма спрямовувала обговорення, показуючи дерева рішень, що позначали, які учасники з якими точками зору погодилися. Модератори відхиляли некорисні коментарі. Піцос сам фінансував проєкт, прагнучи створити «інструмент для колективних міркувань»[14], і Гарвардський та інші університети випробовували приватні його версії для занять. Навряд чи це допомогло би позбутися ботів і тролів у Твіттері, але це було принаймні дещо позитивне. Лейрд почав писати книжку про засоби інформаційної війни.

Деякі з тих, хто схвально ставився до кібероперацій США, як-от Мадж, теж бачили чіткі етичні аргументи на користь санкціонованих нападів. Вони вирішили, що хакінг для шпигування, підготування поля бою на випадок подальшого конфлікту й проведення вузькоспрямованих руйнівних атак, як зі *Stuxnet*, набагато краще, ніж війська та бомби. Інші в *cDc*, бачачи, як змішуються мотиви з підвищенням геополітичних пріоритетів, вирішили повернутися до основ захисту. Поліпшуючи безпеку інтернету для кожного, вони могли поступово зруйнувати

несправедливу перевагу, яку мережа надавала нападникам від самого початку.

Розділ 12.
МАДЖ І КРІСТІАН

Пейтер Затко, відомий навіть для близьких друзів як Мадж[1], не був найактивнішим керівником у @stake, хоча був головним творцем першої хакерської консалтингової групи. Більшу частину часу найвідоміший член «Культу мертвої корови» перебував десь в іншому місці, воюючи з власними демонами та, після терористичних атак 11 вересня, з демонами Америки. Побачене дуже його налякало. Він знав не менше за інших про основні проблеми технологічної безпеки та їхні першопричини. Винахідники інтернету збудували його на довірі, і він вийшов на свободу у своїй тестовій версії[2] до того, як Вінтон Серф і його команда змогли запропонувати надійний захист.

В усіх програмах є баги, деякі з котрих можна експлуатувати. Нашарування одного софту на інший робить його менш безпечним. Постачальники софту ухилилися від юридичної відповідальності за неякісну роботу й майже не мали стимулів виділяти багато ресурсів для поліпшення безпечності своїх продуктів. (Цей суворий аспект відповідальності почне лякати тільки 2018 року в крайніх випадках, як-от у зв'язку зі смертями, у яких обвинуватили програмування автоматизованих транспортних засобів.) Регулювання не було взагалі на більшості комерційних ринків і було незначним у галузях на кшталт фінансових послуг, охорони здоров'я та розподілу електроенергії. Це

означало, що все ненадійне і буде тільки менш надійним зі зростанням залежності економіки від технологій.

Це було класичне фіаско ринку, загострене політичним провалом. Про основні причини політичного провалу можна сперечатися, але серед них було потрапляння регуляторів під вплив галузей, які не хотіли регулювання, гонитва короткострокових керівників бізнесу за короткостроковими комерційними вигодами та неспроможність розрізнити, коли приватні компанії мають бути відповідальними за власний захист, а коли має втручатися федеральний уряд. Останнє було нетривіальною справою, оскільки ті самі методи могли використовувати кримінальні хакери, протидія яким загалом вважалася корпоративною відповідальністю, та національні шпигуни, боротьба з якими вважалася обов'язком Національної безпеки чи ФБР за підтримки Міністерства оборони. А якби правила були чіткими, що робити зі злочинцями, які працюють на шпигунів, чи шпигунами, які вечорами халтурять як злочинці? Бездіяльність Конгресу набирала загрозливих масштабів. Але хоч на вулицях і не лилася кров, у Маджа було мало надії, що незабаром щось зміниться.

2003 року, коли здебільшого російські організовані злочинні групи взяли на себе провідну роль у розповсюдженні комп'ютерних вірусів для спаму та вимагань, Мадж побачив, що загальна ситуація ось-ось загостриться ще сильніше. Він дійшов думки, що найліпший спосіб допомогти — піти туди, де найкраще розуміють проблему, мають найпотужніші ресурси для боротьби з нею та найвищу відповідальність, тобто до федеральних розвідувальних агентств. Зважаючи на його підозрілі зв'язки та загальне негативне ставлення

до істеблішменту, звертатися напряму до ЦРУ чи АНБ було б складно. Але Мадж міг почати принаймні там, де він був відомою величиною, і там, де в нього був захист від людей з нашивками й зірочками на уніформі. Мадж знову приєднався до *BBN Technologies* за рік після звільнення його головного урядового спонсора Річарда Кларка з Білого дому Буша. Починаючи з 2004 року, він працював у BBN над дослідженнями й розробкою для розвідувальних агентств США та навчав людей, які стануть основою елітного хакерського підрозділу АНБ, Операцій спеціального доступу. Протягом наступних шести років він працював над багатьма речами, про які не може розповісти. «Гадаю, коли почали використовувати мої ідеї, було врятовано багато життів моїх співвітчизників»,— казав Мадж. Він повідомив мені, що життя на Близькому Сході теж були врятовані, тому що замість бомб застосували його інструменти.

2010 року нова директорка Агентства передових оборонних дослідницьких проєктів (*DARPA*) запросила Маджа очолити роботу агентства з кібербезпекою. Мадж і раніше думав про *DARPA*, але був не в захваті від попереднього керівництва. Нова шефиня, Регіна Дуган, сподобалася йому. І в *DARPA*, заснованому 1958 року у відповідь на приголомшливий запуск радянського «Супутника-1», була найкрутіша місія в уряді: «створення та стримування стратегічних несподіванок»[3]. Подібно до багатьох посад у DARPA, ця позиція мала фіксований трирічний строк, протягом якого він надаватиме гранти на захисні й оборонні проривні проєкти у сфері безпеки. Перспектива була неймовірною. Це агентство керувало створенням мережі *ARPANET*, яка стала сучасним інтернетом. «Само

собою, я хотів подбати, щоб речі, від яких залежу я, моя родина та друзі, були безпечними,— казав Мадж.— І я багато чим завдячую своїй батьківщині. Багато країн не дозволили б мені вплинути на розвідувальну спільноту й Міністерство оборони. Сподіваюся, це допомогло їм зробити менше дурних помилок».

Особистим девізом Маджа здавна було «зробити вм'ятину в Усесвіті». Тепер він запросив з десяток найрозумніших хакерів[4], яких знав, щоб з'ясувати, як саме. Він велів їм приготуватися до обговорення, у чому полягають проблеми сек'юріті-галузі, що їх як дослідників найбільше обурює та чим може допомогти DARPA. Вони зібралися в Арлінгтоні, Вірджинія, у будівлі, де розміщувався великий підрядник розвідслужб — *Booz Allen Hamilton*. У цій компанії працюватиме Едвард Сноуден. Заклик Маджа зібрав «купу білих ворон», за висловом Дуга Сона, який теж був серед них. У складі групи були ветерани @*stake* Дейв Айтель, який тепер керував компанією-продавцем вразливостей нульового дня *Immunity Inc.*, і Діно Даї Зові, колишній дослідник федеральних лабораторій і головний науковець урядового постачальника вразливостей нульового дня *Endgame*. Також у ній був колишній розвідувальний підрядник Г. Д. Мур. Він створив *Metasploit*, інструмент для тестових проникнень, який використовував вразливості, щойно їх розкривали, часто протягом доби. Вірний послідовник *Ninja Strike Force* та підрядник розвідслужб Вел Сміт теж приїхав.

На зборах Мадж сказав, що його посада в *DARPA* нарешті надала всій хакерській спільноті «місце за столом». Що ж, зазначив він, «не змарнуймо цю можливість». Поки група складала список пріоритетів,

Сон попросив про дещо особливе: зміну процесу. *DARPA* фінансувала великих гравців — військових підрядників, інші великі компанії та деякі університетські кафедри. Ті організації знали, як давати раду паперовій роботі, робити гладенькі презентації та використовувати свої результати. Це залишало осторонь маленькі команди й окремих людей, які мали чудові ідеї та не знали, куди з ними йти. Сон, син власника винного магазину, використав грант для малого бізнесу, щоб заснувати *Arbor Networks*. Він сказав, що *DARPA* теж має взятися до малих грантів, і Сміт погодився.

Мадж провів достатньо часу в урядових колах, щоб усвідомити справедливість їхньої думки, та переконав Регіну Дуган. «Сам процес був перешкодою»,— сказала вона. Незабаром Мадж анонсував створення *Cyber Fast Track*, першої програми *DARPA* з надання малих грантів малим командам замість великих сум великим командам. Він фінансував майже двісті пропозицій, кожна з яких надавала дослідникам змогу зберегти свою інтелектуальну власність. Серед отримувачів був Моксі Марлінспайк, чий винахід, *Signal*, побачить світ за кілька років, і Чарлі Міллер, який досліджував вади в *NFC* — комунікаціях ближнього поля, коли ці протоколи більше входили в ужиток у смартфонах.

На Def Con 2011 року Міллер робив презентацію[5] про *NFC* і наштовхнувся на Маджа, у якого теж був запланований виступ. Міллер розповів йому дещо про свої інтереси та спитав, чи купить йому *DARPA* авто для спроби хакінгу. «Подай заявку та дізнайся»,— відповів той, що Міллер і зробив. Він отримав машину та хакнув її комп’ютер. Пізніше, спираючись на результати тієї роботи, Міллер зламав джип, яким керував репортер

Wired. Це спричинило масове відкликання автомобілів і привернуло глобальну увагу до проблем безпечності комп'ютеризованих транспортних засобів. Початкове обладнання та фінансування — непогана річ. Але підтримка *DARPA* стала ще важливішою, коли автомобільна компанія, стурбована відкриттями Міллера, пригрозила позовом. Мадж попередив їх: якщо вони це зроблять, Пентагон приєднається до справи на боці Міллера і з великою групою добре підготовлених юристів.

«Ті гранти надали дослідженням певної легітимності, яка дуже допомагала, коли виникали заперечення,— казав Міллер.— Зараз ви бачите багато проєктів, яких ніколи б не було без грантів *Cyber Fast Track*, як-от нашого з хакінгу авто». Усі в Пентагоні хотіли отримати документи досліджень. Але перш ніж отримати папери брифінгу, вони мали висидіти демонстрацію від хакерів, тому дійсно розуміли матеріал. У наступні роки інші відділи Пентагону почали копіювати розроблену Маджем програму.

[x x]

Мадж досяг набагато більшого, ніж просто раціоналізації способу, у який федеральний уряд збирав гарні ідеї. Він узявся до фундаментальної проблеми методу, у який уряд та всі інші оцінювали безпеку. Протягом десятиліть ніхто не запропонував обґрунтований метод визначення цінності продуктів безпеки, які привертають увагу переважно тоді, коли не справджують очікувань. Так само *DARPA* не могло знайти логічну основу для визначення, що саме фінансувати. «Ми не схвалимо

жоден новий проєкт, доки не виконаємо глибоку стратегічну роботу»,— сказала Дуган. Вона наполягла, щоб Мадж і його бос, давній керівник з розробки у *DARPA* Ден Кауфман, знайшли новий спосіб розгляду проблеми.

Вони запропонували систему кібераналітики[6]. Основна ідея: коли передбачувана складність підвищується, робота захисників ускладнюється швидше, ніж робота нападників. Щоб проілюструвати проблему, Мадж використав звичну мову Вашингтону та презентацію. Найбільше вражала діаграма, яка показувала, що за останнє десятиліття передовий захисний софт роздувся настільки, що містить у середньому 10 мільйонів рядків коду. А середня кількість рядків у зловмисних програмах становила стабільні 125.

Оскільки кожна тисяча рядків коду містила від одного до п’яти багів, це означало, що великі продукти безпеки погіршують ситуацію. DARPA потребувало простих й елегантних підходів. За словами Дуган, «це було чітке формулювання тенденцій». Мадж почав запитувати кандидатів на фінансування проєктів, тактичні чи стратегічні їхні підходи, як їхній проєкт збільшить чи зменшить поверхню атак і як би вони атакували самі.

Цей підхід став основою витрат Міністерства оборони поза *DARPA*, і він здобув для агентства деякі гроші, які б за інших обставин відійшли Кібернетичному командуванню США. Це була одна з кількох речей, які дратували Кіта Александера, керівника Кібернетичного командування та директора АНБ. Мадж не звертав на це уваги. Александер очолював величезну експансію глобального й американського спостереження та

організаційну культуру, яка допускала існування кількох викривачів і хакінг працівників.

Мадж обожнював робити ставки на перспективні ідеї, але також вважав своїм обов'язком придушувати погані в зародку. Ще залишаючись зовнішнім підрядником, він відкрито засуджував продукт, який автоматизував деякий «активний захист» — галузевий термін для засобів, які варіювалися від блокування підозрілих підключень до виведення з ладу комп'ютерів, використовуваних нападником. Більшість спеціалістів розвідслужб вважає це поганою ідеєю, яка може призвести до хаосу та, можливо, ненавмисної війни. На думку Маджа, автоматизація — «жахлива ідея, тому що ззовні вами можуть маніпулювати».

Він витрачав багато зусиль, виступаючи проти вимог створення бекдорів у шифруванні. Співробітники розвідслужб і військові стверджували, що в їхніх установах роботу з бекдорами влаштовано добре — доступ до них реєструють і контролюють, порушення рідкісні. Але це були закриті системи, у яких керівництво мало цілковиту владу над середовищем. Зовні, у звичайному світі, організаційні структури були слабкіші та дозволяли витоки доступу.

Мадж не припинив говорити правду тільки через те, що був наділений владою. Можливо, допомагало те, що строк його посади завершиться лише за три роки, тому службовці очікували менше підлещування. Мадж інформував Об'єднаний комітет керівників штабів і міністра оборони, допомагаючи зрозуміти, коли хтось зі збройних сил чи підрядник заявляв про неправдоподібну здібність у боротьбі за вплив чи бюджет. «Об'єднаний

комітет керівників штабів і Пентагон запрошували мене, тому що я міг пояснити їм реальну ситуацію»,— казав він.

Мадж залишився критично налаштованим. Посеред повсюдного обурення постійними атаками на постачальників оборони, невдовзі після свого звільнення з *DARPA* Мадж зауважив, що в підрядників є стимул допускати викрадення своїх систем. Коли це відбувається, розмірковував Мадж на конференції Black Hat, вони можуть попросити Пентагон заплатити за нову й поліпшену версію їхньої системи, яка ще не потрапила до рук ворога. «Теорія ігор — паршива штука»,— казав він.

Утім, внутрішня гра добре йому вдавалася. *DARPA* завжди відправляло свої продукти до нових місць у Пентагоні чи розвідувальних установах, де вони мали найкращі шанси розвитку. Оскільки Александер та інші були схильні неприязно ставитися до роботи Маджа, іноді він ішов на хитрощі, передаючи справу працівнику середнього рівня, який міг прибрати ознаки походження проєкту. На одному брифінгу з заступником міністра оборони Александер пояснив, що в нього є п’ять «ідеальних рішень», які він може застосувати в кібероперацiях. «Три з них — мої»,— задоволено подумав Мадж.

Завдяки йому Пентагон перестав вважати хакерів природними ворогами. По суті, він показав, що люди, які подорослішали, точно знаючи, де межа, зазвичай більше прагнуть не перетинати її, ніж люди, постійно захищені своєю уніформою, бюрократією та юристами. В одній дискусії у великому агентстві за присутності

Дена Кауфмана працівник спитав Маджа, чи могло б агентство зламати систему, щоб отримати інформацію, яку він простежує. «Безсумнівно,— відповів йому Мадж. — Але це незаконно та неправильно». Він зберігав моральний компас навіть у *DARPA*.

[x x]

Через випадковий вибір часу запланований вихід Маджа з урядових кіл відбувся у квітні 2013 року, за два місяці до того, як викриття Сноудена перетворили АНБ і розвідку США на глобальні об'єкти глузувань. Залишаючи організацію, Мадж отримав від міністра оборони найвищу нагороду за цивільну службу[7]. У подяці було сказано, що гранти Маджа створили понад сотню нових можливостей, що його новий метод виявлення кібершпигунства прийнятий розвідувальними агентствами та що він удосконалив здатність Міністерства оборони проводити онлайн-атаки.

Мадж пішов слідом за Регіною Дуган у *Google*, де працював над кількома секретними проєктами. У найвідомішому з них на карту пам'яті помістили захищену операційну систему[8]; програмне забезпечення працювало б належно, навіть якби під загрозою опинився комп'ютер загалом. Серед функцій була незмінювана система протоколювання подій. Софт належатиме до найкращих можливих способів захисту від масового спостереження, про яке розповів Сноуден. *Google* ще не випустила готову версію, коли Мадж залишив компанію заради нової справи — неприбуткової організації, яка досліджувала коди

бінарних файлів і оцінювала їх на основі стандартних характеристик безпеки.

Він і *Cyber Independent Testing Lab (CITL)* його дружини Сари діяли як лабораторії в Consumer Reports, шукаючи цифрові еквіваленти автоматичних гальмівних механізмів і пасків безпеки без потреби в доступі до вихідного коду. Скориставшись фінансуванням *DARPA*, Фонду Форда й інших, *CITL* показала, що на тодішній операційній системі Mac хакерам набагато складніше атакувати браузер *Google Chrome*[9], ніж *Safari* чи *Firefox*. Мадж прагнув перетворити докладнішу версію таких оцінок на дещо схоже на обов'язкові для їжі етикетки з позначенням харчової цінності, які допомагають покупцям ухвалювати інформовані рішення, що відповідають їхнім пріоритетам.

Борючись із раком нирки, який повернув його посттравматичний стресовий розлад, Мадж підтримував проєкт у перший рік, відтак передав повсякденний контроль Сарі, досвідченій працівниці федерального підрядника *BBN*. Він став керівником з питань безпеки у Stripe, компанії з обробки електронних платежів. (Інвестиційний раунд у вересні 2018 року оцінить цю компанію у 20 мільярдів доларів.) У вільний час він надавав консультації сенатору Марку Ворнеру, співголові фракції Сенату з кібербезпеки. «Мадж дуже допоміг нам у розумінні безпеки софту, і це вплинуло на нашу роботу над, наприклад, поліпшенням безпеки пристроїв інтернету речей»,— розповів Ворнер, посилаючись на нові класи підключених до інтернету ґаджетів, як-от камери відеоспостереження й термостати. Ворнер як популярний демократ також працював у комітеті Сенату з розвідки, що робило його

провідним демократом у розслідуванні російського хакінгу, який 2016 року допоміг обранню Трампа. Було б логічно припустити, що досвід Маджа допомагав Ворнеру й там, хоча жоден з них не обговорював це зі мною. (2018 року Мадж твітнув, що 2016-го радив Демократичній партії посилити захист, але більшу частину його порад проігнорували.)

[x x]

Ще один великий технологічний розум золотої ери *cDc*, Крістіан Dildog Pio, взявся до дещо схожого на роботу лабораторії Маджа: глибокого аналізу безпеки програм без доступу до вихідного коду. Але він пішов цілковито іншим шляхом і відхилив можливість працювати на уряд.

У період роботи в *@stake* Крістіан приділяв багато часу дослідженням бінарних файлів. Вихідний код у тому вигляді, у якому його написали програмісти, набагато легше сприймати. Але він може приховувати купу проблем. Проте від погляду на одиниці й нулі болить голова. Тому Крістіан написав якомога більше інструментів для обробки бінарних файлів. Це зберегло багато часу й надало йому можливість проводити аналіз, який галузь називає статичним аналізом коду. Коли *Symantec* настільки поглинула *@stake*, що її стало неможливо відрізнити від решти гігантської компанії, Крістіан вирішив створити стартап, щоб фінансувати власний пошук дечого подібного до Святого Граалю — програми, яка декомпілює всі бінарні файли в читабельний код.

З 2006 року Крістіан працював провідним науковцем нової компанії, що називалася *Veracode*. Він запросив Кріса Вісопала, свого колегу в *L0pht* і *@stake*, стати співзасновником і головним технічним директором. Він закликав служити споживачам, а не виробникам, як-от *Microsoft* і *Oracle*, у яких були мотиви економити на безпеці. Коли основна програма добре працюватиме, розмірковував Крістіан, покупці зможуть переконати своїх постачальників дозволити *Veracode* проаналізувати безпечність бінарних файлів. У разі успіху постачальники посилатимуться на схвалення *Veracode* як знак пошани та рекомендуватимуть споживачам, щоб *Veracode* виконав нову перевірку найновішої версії софту.

У теорії все було блискуче. На практиці це означало багато роботи. «Це був п'ятирічний план, на виконання якого пішло десять років»,— сказав Крістіан. Перший раунд фінансування надійшов від *In-Q-Tel*, венчурної фірми з Кремнієвої долини, створеної для задоволення потреб розвідувальних агентств США. Її очолював колишній гендиректор *@stake* Кріс Дербі. Він вірив, що Крістіан зробить код набагато безпечнішим, і вважав, що це слід застосувати в системах озброєння США,— для впевненості, що коди, які контролюють ракети й таке інше, здатні вистояти проти більшості хакерських атак.

Дербі влаштував Крістіану візит до розвідувальної бази глибоко під землею для демонстрації можливостей *Veracode*. Старший офіцер секретних операцій привітався й додав: «Я великий фанат *L0pht*». Крістіан подякував йому. «Який люб'язний,— подумав він.— Можливо, він убиває людей». На спеціально підготовленому ноутбуці Крістіан проаналізував трішечки

наданого йому бінарного коду, можливо, зі шпигунського інструмента, створеного агентством. Він залишив програму працювати протягом обідньої перерви та повернувся якраз вчасно, коли вона видала результати. Серед іншого, вона виявила індивідуальну модифікацію стандартного алгоритму шифрування. Ввічливий убивця був у шоці. Однак специфіка угоди спантеличувала. *Veracode* могла надати свою програму, але не могла бути поруч, щоб надавати підтримку.

Дербі хотів, щоб Крістіан все одно зосередився на оптимізації коду для подібних угод. Проте Крістіан усвідомив, що його основними клієнтами будуть федеральний уряд і кілька його близьких союзників. «Це може бути не дуже вигідно для мене, доведеться працювати на глибині 500 футів під землею й ніколи не бачити сонячного світла»,— подумав він. Він аж ніяк не хотів проходити через тяганину отримання допуску до державних секретів. Що важливіше: «Я хочу сильніше вплинути на світ і не думаю, що це відбудеться в надрах уряду».

Щойно *Veracode* вирішила залишити своїм пріоритетом комерційний світ і команда Крістіана зібрала прототип свого основного декомпілятора, він і Вісопал почали скликати старих друзів, які тепер працювали у великих компаніях — розробниках софту. Серед них був Бред Еркін, ветеран *@stake*, який 2008 року був старшим директором з безпеки в *Adobe Systems* — можливо, найбільш критикованого за всюдисущі вади постачальника у Кремнієвій долині. «Всі знають, що у твоєму *Flash Player* повно багів,— сказав Крістіан Ріо Еркіну, обіцяючи виявити всі проблеми.— Ми можемо зробити сканування за місяць». Еркін погодився. Але

база коду була хаосом такого масштабу, якого Крістіан ніколи в житті не бачив. На додачу до звичайних слабких місць програмування плеєр містив неясні кодові частини для відтворення матеріалу, записаного в усіх типах форматів і на різних пристроях. Це постійно призводило до проблем з декомпілятором. Коли місяць минув, Крістіан заявив, що не голитиметься, доки не завершить сканування *Flash Player*. Це підтримувало його мотивацію. Але знадобився цілий брутальний рік, і його обличчя жахливо свербіло. «Ненавиджу *Adobe*»[10],— скаржився він.

Ця робота значно поліпшила продукт *Veracode*. Компанія додала до списку своїх клієнтів великі компанії і, працюючи через військових підрядників на кшталт Boeing, могла також обслуговувати АНБ і ЦРУ. *Veracode* переконала покупців софту вимагати від своїх постачальників, щоб вони дозволяли їй проводити аудит бінарних файлів, які зберігалися на максимально захищених комп'ютерах. На початку більшість постачальників це ненавиділи. Але замість негайно викривати їхні слабкі місця, *Veracode* надавала їм кілька шансів виправитися та поради, де і як це зробити.

Як і в багатьох розробників і сервісних компаній, обсяги продажу Veracode зазнавали злетів і падінь; найбільші коливання відбувалися наприкінці кварталів через виплати комісійних. Коли цю проблему було розв'язано та продажі досягли 120 мільйонів доларів на рік, *Veracode* обміркувала вихід на фондовий ринок. Також компанію можна було продати іншій компанії з більшими кишенями, яка збільшила б кількість клієнтів для Veracode. Зрештою обрали кращий варіант — продати *Veracode* компанії *CA Technologies*, раніше відомій як

Computer Associates, 2017 року за 614 мільйонів доларів. Наступного року відбувся продаж і перепродаж, останнього разу за 950 мільйонів доларів. Після переїзду до нового корпоративного дому Крістіан зміг приділяти більше часу побічному проєкту *Hailstone*, який дозволяє розробникам перевіряти свій код на наявність вад безпеки у процесі його написання. Тоді як програма Veracode зазвичай коштувала 10000 доларів на рік, спробувати *Hailstone* можна було безкоштовно.
У березні 2019 року Крістіан остаточно пішов з *Veracode*.

[x x]

Більшість членів «Культу мертвої корови» зрештою пішли працювати в технологічні компанії з людьми, яким невідома їхня біографія. Серед них були Люк Бенфі, Пол Леонард, Метт Келлі, Міша Кубека та Кемаль Акман. Джош Бухбіндер, який пішов раніше, досі працює у сфері безпеки в Сан-Франциско. Джон Лестер живе в Монреалі: він багато років працював на розробника *Second Life*, потім зосередився на електронних інструментах для інтерактивної медицини й освіти. Ден Макміллан пішов у бізнес і став керівником продажів і консалтингу у великих компаніях — розробниках софту. Ґленн Курцрок, який завжди хотів саджати поганих хлопців у тюрму, сімнадцять років працював помічником районного прокурора на Лонг-Айленді, а 2017 року почав приватну практику. Керрі Кемпбелл — дослідниця-фрилансерка поблизу Сіетлу. Співзасновник Білл Браун навчає зйомкам документальних фільмів.
У співзасновника Брендона Брюера, колишнього Сіда Вішеза, життя серйозніше не буває: старший

віцепрезидент агентства нерухомості Republic Title у Форт-Ворт.

Сем Ентоні влаштувався програмістом у лабораторії Гарвардського університету, потім відкрив там магістратуру, працюючи над біологічними моделями обчислень. 2018 року він здобув докторський ступінь. За цей час він став співзасновником компанії, що досліджує безпілотні автомобілі, Perceptive Automata. Автономні транспортні засоби «прекрасно знають, де дорога, як швидко рухається машина та що перед нею, дерево чи людина,— пояснював Сем.— Але вони не вміють розв'язувати психологічну проблему — здогадатися, що в людини в голові. Методи, які ми розробили, поки я писав дисертацію, ідеальні для ситуацій, коли ви хочете, щоб комп'ютер навчився робити щось, у чому люди неймовірні». Компанія Сема записувала на відео пішоходів, показувала їх людям і ставила запитання, наприклад, чи поводяться об'єкти так, немов хочуть перейти вулицю. Він застосовував методи машинного навчання, щоб навчити комп'ютери розуміти людей. На виставці *International Consumer Electronics Show* у січні 2019 року *Perceptive Automata* могла пишатися інвестиціями від *Toyota*, *Honda* та *Hyundai*.

Кевін Вілер роками продовжував працювати в музичній сфері. На додачу до продюсерської роботи в гуртах він удавав, що має три різні звукозаписні студії. Він надсилав записи й пресрелізи музичним виданням, щоб переконати їх написати про гурти. Якби хтось погодився, він завжди міг би заплатити комусь, щоб надати реальний запис. Цей гамбіт не вдався. 1999 року він з другом приїхав працювати до Нью-Йорку. Вони встигли записати два саундтреки для офф-бродвейських театрів

до того, як партнер Кевіна зустрів жінку та 2001 року переїхав з нею до Тайбею. Потім терористичні атаки 11 вересня знищили офіс, де працював Кевін, і він втратив роботу. Найбільшою проблемою був виїзд його партнера, тому що Кевін завжди досягав більшого як член команди. «Я не Oxblood Ruffin,— зауважив він.— Я був ведучим. Можу розрекламувати щось, пропіарити, подати з гумором. Я найбільш продуктивний, коли мене підштовхує партнер, як Franken Gibe на початку».

Інше музичне партнерство принесло невеликий хіт. Учень старшої школи та майбутній письменник Г'ю Ґаллагер, засмучений нереалістичними вимогами до есею для вступу в коледж, написав дивний текст-пародію з помпезністю та самоіронією у стилі *cDc*. Есей закінчувався словами: «Я вирощую відзначених винагородою морських молюсків. Я переміг на кориді в Сан-Хуані, змаганнях з пірнання зі скель на Шрі-Ланці та зачаровую бджіл у Кремлі. Я зіграв Гамлета, провів операцію на відкритому серці та спілкувався з Елвісом. Але я ще не пішов у коледж». Ґаллагер не тільки вступив до Нью-Йоркського університету. Він переміг на національному конкурсі, зажив помірної слави та отримав замовлення від журналу *Rolling Stone*. Пізніше він виступив під сценічним ім'ям *Von Von Von* у театрі «Аполло» в Гарлемі з музикою, яку створив Кевін. На відео з понад мільйоном переглядів на Ютубі Ґаллагер викрикнув зі сцени його ім'я[11]. Погравшись із кар'єрою гравця в покер, Кевін перейшов до торгівлі валютою вдома. Він знову став сором'язливою людиною, якою насправді був, коли не писав під своїм ніком чи не виступав на сцені, підтримуючи якийсь проєкт чи колегу.

На 2018 рік «Культ мертвої корови» відійшов на задній план. Майже кожен чув про хактивізм, навіть більша частина громадськості, але зазвичай люди асоціювали його з «Анонімусом» чи іншими наступниками *cDc*. Як буває з величним учителем інших учителів, найочевиднішим спадком групи були дії тих, кого вона надихнула, та наступного покоління, чию увагу їй вдалося привернути. Це була велика група активістів з неприбуткових організацій, дослідників і деяких найкращих розумів уряду та сек'юріті-галузі. Засновниця команди з безпеки в *Google* Гізер Едкінс виросла, читаючи інтернет-чати з *cDc*, і взяла уроки щодо розкриття інформації близько до серця. На її думку, вони створили основу для діяльності на зразок *Project Zero*, команди *Google*, яка шукала баги в програмах з тримісячним календарним планом публічного розкриття. За чотири роки група виявила 1400 вразливостей[12]. «Культура розкриття сьогодні розвиненіша, але ставки набагато вищі,— говорить Едкінс.— Компанії зобов'язані захищати користувачів. Як показати їм шлях? Історично склалося, що технологічні компанії мають тільки одну мету — заробляти гроші. Але до того, як хтось втручається та змінює ситуацію».

До членів *cDc*, які власними силами досягали видатних результатів, виконуючи місію групи, належали Oxblood Ruffin, Мадж, Крістіан та ще одна людина — Psychedelic Warlord. Так само як інші, він розумів: оскільки технології набувають вирішальної ролі в житті, критичне мислення, яке розвинулося разом з ними, теж потребує більшої уваги.

Розділ 13. КОНГРЕСМЕН І ТРОЛІ

Коли 2006 року Керрі Кемпбелл покидала поштову розсилку «Культу мертвої корови», у своєму прощальному листі вона віддала належне людині, яка привела її в групу у 1980-ті. «До речі, Psychedelic Warlord робить швидкі успіхи в політиці в Ель Пасо. Я так пишаюся ним. Ми не повинні згадувати, що він один із нас, аби не зашкодити розвитку його кар'єри». Вона додала посилання на сторінку Вікіпедії про техасця з його справжнім ім'ям: Роберт Beto O'Рурк.

Деякі новіші члени не знали його імені, а більшість ніколи з ним не зустрічалися. Востаннє Бето бачився з групою на конференції *HOPE* 1997 року — того ж року, коли Лейрд Браун розповів аудиторії про «Гонконгівських блондинок». Але всі в *cDc* вшанували прощальне бажання Керрі. Престиж Бето в Ель Пасо зростав, а тим часом його юнацька приналежність до *cDc* залишалася таємницею. Після навчання в школі закритого типу у Вірджинії він вступив до Колумбійського університету, потім працював на нью-йоркського інтернет--постачальника. Також він грав у панк-гурті *Foss*[1] — тому самому, який приймав у себе Керрі в Сіетлі. Повернувшись додому, він відкрив скромний бізнес із вебдизайну, який мав додаткове джерело доходів — альтернативний сайт новин. Далі Бето пішов за батьком у політику та обрався в міську раду. Ель Пасо було одним із найбідніших міст Америки[2], ще

й розташованим неподалік від місця масових, пов'язаних з наркоторгівлею вбивств у Сьюдад-Хуарес. Бето відстоював закони з лібералізації наркотиків і разом зі своїм союзником у міській раді написав невелику книжку[3], у якій стверджував, що легалізація марихуани скоротить прибутки гангстерів, які були причиною кровопролиття.

Бето поклав око на місце в Конгресі, але в партії йому порадили зачекати, доки звільниться нинішній представник від демократів. Натомість Бето пішов на зважений ризик і кинув йому виклик на первинних виборах. Ветеран недооцінив Бето, який обігнав його, постукавши у шістнадцять тисяч дверей. Він продемонстрував виборцям енергію[4], яку здатен присвятити їхнім інтересам. 2013 року він виграв первинні та основні вибори й приєднався до Конгресу.

2016 року, коли Бето й інші організували сидячий страйк у Палаті представників, щоб добутися обговорення контролю над зброєю, спікер оголосив перерву. Це означало застосування правила Конгресу, за яким мережа *C-SPAN* не може транслювати події, якщо сесія не відбувається. Тому Бето почав транслювати подію зі свого телефону через Фейсбук[5]. Цей трюк привернув широку увагу до відмови партії більшості навіть обміркувати життєво важливе питання і показав готовність Бето мислити як хакер, щоб обійти усталені технологічні, політичні й медійні процедури.

Як демократ у переважно республіканському Техасі Бето гідно давав раду статусу меншості. Коли в березні 2017 року через хуртовину скасували рейси з Техасу до

Вашингтону, він улаштував 29-годинну поїздку з республіканцем із сусіднього округу, прагматичним колишнім співробітником ЦРУ Віллом Гердом. Дорогою до Капітолійського пагорба вони були в прямому ефірі[6]: спілкувалися, відповідали на запитання від глядачів і слухали музику. Вони обговорювали російське втручання у вибори, пропозицію побудувати стіну на кордоні з Мексикою та законодавство у сфері охорони здоров'я. Відео стало вірусним і зібрало мільйони переглядів.

Після обрання Трампа Бето знав, що в Палаті представників багато не досягне. Навіть якби демократи отримали більшість, йому знадобилося б чимало років, щоб піднятися до керівника великого комітету. З іншого боку, якби йому вдалося знову перемогти, цього разу у змаганні з техасцем-республіканцем Тедом Крузом за місце в Сенаті, він міг би одразу робити щось важливе. Відповідно до закону Бето спочатку мав відмовитися від свого місця в Конгресі, оскільки не міг балотуватися водночас у Палату представників і Сенат. Це була б ситуація «все або нічого».

Коли на початку 2017 року Бето оголосив про свої наміри поборотися за пост сенатора, республіканці контролювали Білий дім та обидві палати Конгресу. Демократа не обирали сенатором Техасу роками, і Круз був одним із найкраще фінансованих членів Сенату. Видатне становище Круза посилилося тим, що він був другим республіканцем під час праймеріз 2016 року. Трамп починав роботу в Білому домі, Джеймс Комі досі очолював ФБР і ніякий спецпрокурор не розслідував потенційної змови росіян і Трампа. Бето був

ліберальнішим за середнього техаського демократа, що робило його легкою мішенню багатьох глузувань Круза.

Але в нього були й переваги. За результатами опитувань, Круз мав серйозні недоліки поряд з позитивними рисами. Підтримка Трампа похитнулася в громадських опитуваннях, що вдарило по всіх республіканцях. А в Бето були навички комунікації, побудови соціальних зв'язків і критичного мислення, що зародились тоді, коли він був хакером-початківцем. Якщо він вважав популярну політику неправильною, так і говорив. Технологічна обізнаність Бето, хоч вона аж ніяк не скидалася на рівень Маджа чи Крістіана Ріо, робила його на голову вищим від середнього члена Конгресу в цій сфері та допомагала привертати молодших виборців, а також людей, стурбованих технологіями, що загрожують приватності й традиційним робочим місцям і розповсюджують дезінформацію. Звісно, він сильно контрастував з тими членами Конгресу, які допитували Марка Цукерберга та плуталися в простих концепціях на кшталт залежної від реклами бізнес-моделі та відмінностях між Фейсбуком і Твіттером.

Знайомство Бето з технологіями також допомогло йому знайти спонсорів у Кремнієвій долині й в інших місцях. Члени cDc тихо розповіли його історію кільком з найнадійніших і найбагатших технічних спеціалістів, яких знали. Один друг організував захід із збирання коштів у Лос-Анджелесі, а Сем Ентоні — в Бостоні. Керрі з радістю возз'єдналася з Бето в Сіетлі. Він розповів усім, що жив у домі Керрі як басист панк-гурту та з'їв усі її сухі сніданки. Коли захід закінчився, вона обміркувала

все, чого досяг Бето з їхньої останньої зустрічі, і обняла його на прощання зі сльозами гордості на очах.

[x x]

Не тільки політикам було потрібно більше думати про технології та їхню унікальну багатопланову роль у світі. Люди технологічної сфери також мали набагато більше думати про політику. Обрання Трампа розпалило в багатьох бажання дати відсіч тому, що вони побачили як внутрішню інформаційну кібервійну. Експерти з безпеки відчували особливі муки сумління, адже проникнення в Національний комітет Демократичної партії, комітет з виборів у Конгрес і зламування *gmail*-акаунту Джона Подести зіграли вирішальну роль у виборах. За моделлю, яку допоміг поширити Джейк Еплбаум, зміст тих електронних листів розповсюджувався *WikiLeaks*, фанатичною та панівною пресою й активно циркулював у соціальних мережах.

2017 року, коли з'явилися докази глибини та витонченості прагнень підвищити популярність Трампа у Фейсбуку, Твіттері та Інстаграмі, великий прошарок американської громадськості обернувся проти технологічних компаній. Усередині гігантів Кремнієвої долини виник розкол. Меншість була невибачливими прихильниками Трампа, як-от засновник *Palantir* і член правління «Фейсбук» Пітер Тіль, або користувалася його домінантним впливом як нагодою висловитися проти того, що вважала дискримінацією щодо гетеросексуальних білих чоловіків, як інженер з *Google*, який заявив, що його звільнили через публікацію про внутрішні упередження.

Але багато хто перебував в етичній кризі, якої Долина ще не бачила. Деякі хотіли використати зароблені гроші, свої мережі та деякі технологічні навички, щоб виправити ситуацію. Засновник стартапу Мацей Цегловські спостерігав, як президент заборонив в'їзд громадян декількох переважно мусульманських країн. Така політика особливо дратувала багатьох у техіндустрії, тому що чимала кількість засновників бізнесу й працівників походила з-за кордону. І ті, хто раніше вибачав експансію технологічного спостереження за попередніх адміністрацій, тепер були стурбовані потраплянням такої сили до рук виконавчої влади, яка відкрито зневажає судовий нагляд.

Цегловські почав організовувати зустрічі занепокоєних працівників, які згодом об'єдналися в громадську групу *Tech Solidarity*. Відгалуження тих зборів, очолюване інженеркою *Slack* і жертвою Джейка Еплбаума Лі Ганівелл, започаткувало рух «Ніколи знову»[7] — обіцянку протистояти аморальній поведінці та за потреби робити публічні заяви. Її підписали понад 2800 працівників. Серед іншого, вони обіцяли виступати проти утримання даних, які можна використати для атак на етнічні чи релігійні групи, та відстоювати наскрізне шифрування.

На зборах *Tech Solidarity* залучали кошти для адвокатів іммігрантів і координували волонтерські проєкти з програмування. З наближенням проміжних виборів 2018 року, за участю мільярдерів на іншому краю політичного спектра, які витрачали невідстежувані «темні гроші» на просування кандидатів правого напряму, Цегловські у відповідь на це фінансував прогресивних кандидатів в округах, у яких, на його

думку, він міг змінити ситуацію. У цьому маленькому колі конспіраторів був Адам О'Доннелл. Вони консультували десятки компаній, сподіваючись запобігти повторенню хаків 2016 року.

У самій *cDc* майже не було прихильників Трампа. Але через її багатогранний спадок у неї були протеже з обох боків боротьби. Вони билися на сторінках Фейсбуку та навіть у керівних лавах компанії. На правому флангу були деякі особливо балакучі члени фан-клубу та запасного складу *cDc — Ninja Strike Force*.

Роб Бек, друг *cDc* з *Microsoft* і *@stake*, деякий час очолював NSF, а потім передав керівництво іншим. Як розповів Сем Ентоні, членство стало неорганізованим й «одне відділення перетворилося на жахливе сплетіння Геймергейту, неонацизму та російської розвідки, яке руйнує світ». Організовані тролі Геймергейту переслідували журналісток ігрового середовища атаками в соціальних мережах, до того як зрештою згуртуватися на боці Трампа. На 2012 рік *NSF* існувала переважно як група у Фейсбуку. Члени розміщували посилання на повідомлення про порушення безпеки в новинах і будь-що інше, що вважали цікавим. Деякі були ветеранами 4chan, які хотіли провокацій, і вдалися до публікації расистських карикатур і жартів. Декілька - вважали це невинним тролінгом і відкидали обвинувачення в расизмі. Але багато головних членів *cDc* були сильно ображені. «*cDc* вплинула на всіх цих людей. Але не було ніякої структури, нав'язування ідей чи перевірок»,— сказав Бек, який знову приєднався до *NSF* після років осторонь і був шокований побаченим. Він почав надсилати найбільш екстремістські дописи

Сему, Люку Бенфі та Кевіну Вілеру, просто щоб упевнитися, що вони в курсі.

У червні 2012 року Люк відправив членам *cDc* листа з посиланнями на расистські карикатури з Фейсбук-сторінки *NSF*. «На мою думку, це дуже, дуже ганебно, що таке асоціюється з *cDc*»,— написав він. Пол Леонард, який підтримував відносини з деякими кривдниками, погодився, що зміни в NSF зайшли надто далеко. «У деяких хлопців праві погляди, деякі просто еджлорди[9] — вони не мають конкретної ідеології, лише кидають усюди бомби». Пол написав двом авторам образливих дописів: «Загалом я вважаю хлопців із *NSF* людьми, з якими хочу спілкуватися. Тепер я маю поставити ці відносини під сумнів, і це мене бісить. Мене не хвилює ваша політика, мене не хвилюють навіть ваші расові переконання, щирі вони чи це просто тролінг. Мене турбує, що у вас, здається, немає ніякого внутрішнього редактора, який може розрізнити кумедну зухвалість і той тип образливого матеріалу, якому взагалі не слід рухатися кудись далі».

Лейрд Браун написав Люку: «Мені боляче про це писати. Якщо це продовжуватиметься і ніхто нічого не вдіє, я буду вимушений покинути *cDc* і забрати *Hacktivismo* з собою. Не можу мати стосунок до цієї гидоти». Варіантів дій було небагато, адже 2007 року хакер *NSF* Колтон Самнерс створив групу у Фейсбуку та контролював її як адміністратор. «Я дав усім аутсайдерам можливість висловитися»,— заявив він. Люк повідомив Фейсбуку про дописи *NSF* як про образливі. Поки група обмірковувала жорсткіші заходи, у справу втрутився Кевін. Він написав Самнерсу: «Це гірше, ніж я думав. Мені потрібен адміністраторський

доступ до групи *NSF*, ці расистські дурниці мають щезнути. Це не стратегічно та завдає мені проблем. Дякую!» Після тривалої боротьби адміністраторів стара гвардія *cDc* повернула контроль.

Самнерс, творець браузера *Xerobank* Стів Топлец і кілька інших членів *NSF*, включно з самопроголошеним «чорним капелюхом» і білим націоналістом Тімоті Matlock Нунаном, створили власну групу, *DSSK Corp*. Як Matlock[8] Нунан відмовився обговорювати зі мною більшу частину своєї роботи. Він сказав, що виріс на текстах *cDc*, але робота команди стала нецікавою, неактуальною та мало причетною до хакінгу. Він зізнався в одному незаконному хаку, виведенні з ладу педофільського сайту, на який націлювався «Анонімус», 2012 року. Легенда *cDc* Кріс Такер, відомий як Nightstalker, нещодавно помер, і Нунан оприлюднив пресреліз з символікою *cDc* і *NSF*, заявляючи, що цю атаку здійснив Nightstalker. Нунан і Топлец також робили послуги уряду США, наприклад передали трафік, виявлений після зламування іранських серверів. Подібно до старих текстових файлів *cDc*, *DSSK* писала про різні пригоди. Але політика була зовсім іншою. 2015 року стаття *DSSK* повідомила про поїздку Нунана до Східної Європи на зустріч з Ендрю Ауернгеймером, відомим онлайн як weev — мабуть, найвідомішим тролем усіх часів. Пол Леонард знав Ауернгеймера з дитинства, коли він ще не був расистом. «Він був переважно дратівливим, зухвалим лузером, який бавився з расизмом заради сміху, поки не потрапив у тюрму,— пригадав Пол, віддзеркалюючи думки інших. — Він вийшов на волю помітно іншою людиною».

На момент того візиту Ауернгеймер мав татуювання зі свастикою і жив у країнах, які не видавали людей Сполученим Штатам. Деякий час він жив в Україні, потім у невизнаній республіці Придністров'я. Він працював над *The Daily STormer*, нацистським сайтом Ендрю Енгліна, який провів достатньо часу в Росії, щоб відправити звідти бюлетень заочного голосування. Обидва чоловіки закликали расистів-протестувальників застосувати силу на марші в Шарлоттсвіллі, Вірджинія, де фанат *The Daily STormer* в'їхав на машині в натовп і вбив контрпротестувальницю Гізер Геєр. Поки що неясно, що ще зробив Ауернгеймер, щоб допомогти Трампу. Але його підозрювали в розміщенні сфальсифікованих документів у період французьких виборів 2017 року з метою допомогти кандидатці Марін Ле Пен[9].

Занепад *NSF* спонукав *cDc* до боротьби з Франкенштейном, якого вона створила.

[x x]

Поки *cDc* і *NSF* билися на сторінках Фейсбуку, назрівав серйозніший конфлікт за лаштунками власне компанії «Фейсбук», імовірно, відправної точки інформаційної війни у період виборів. Поза відвертою підтримкою від Пітера Тіля, який виступив на користь Трампа на Національному з'їзді Республіканської партії, база даних користувачів Фейсбуку, а також нечіткі політики щодо того, які застосунки можуть збирати дані та в кого, дозволили секретній мережі компаній, включно з *Cambridge Analytica*[10], зібрати інформацію про 87 мільйонів американців. Компанії, фінансовані мільярдерами Робертом і Ребекою Мерсерами, заявили,

що на основі психологічних складників тих даних можуть сказати, яка реклама та для кого буде найефективнішою. Як відомо, інформація допомогла Трампу. Але до того, протягом праймериз, вона допомагала його конкуренту Теду Крузу, техаському сенатору, з яким Бето зіткнеться через два роки.

У «Фейсбуку» також був Алекс Стеймос, колишній консультант *@stake*. Після розкриття Едвардом Сноуденом, що багато технологічних компаній тісно співпрацюють з АНБ, тодішній співзасновник *iSec Partners* Стеймос виступив з промовою на *Def Con–2013*, стверджуючи, що експерти з безпеки соціально відповідальні та мають обміркувати своє звільнення, перш ніж заподіяти шкоди громадськості. «Я корпоративний білокапелюховий зрадник,— відверто визнав він.— Ця розмова про те, у який спосіб, якщо ви вирішите бути корпоративним білокапелюховим зрадником, можна зробити це якомога етичніше». Стеймос описав, як нині звичайні компанії втягують у війну, наводячи як приклад криптографічну атаку на *Microsoft*, що уможливила встановлення за кордоном шкідливих програм, приписуваних США, а також постійні атаки Китаю на *Google* й інші технологічні компанії. Як онук бідних іммігрантів, Стеймос сказав, що пишається тим, що він американець, але більше відданий цінностям країни, ніж тимчасовій групі лідерів. Як і лікарі, технічні спеціалісти й особливо спеціалісти-практики у сфері безпеки відіграють надзвичайно важливі ролі, які вимагають морального обов'язку. «Можливо, це означає, що всі люди заслуговують надійних технологій»,— припустив він і запропонував слухачам низку гіпотетичних ситуацій. Він попросив підняти руки, щоб побачити, хто що зробив би.

У першому сценарії Стеймоса ви виявляєте серйозну ваду. Ви оголосите про неї, продасте своєму уряду, продасте покупцю з найвищою пропозицією, скористаєтеся нею самі, використаєте як засіб тиску для укладання консалтингової угоди з розробником чи працюватимете з постачальником над виправленням і тоді розкриєте? Більшість обрала останній варіант — координоване розкриття, започатковане *L0pht*. Інша ситуація: що, як органи національної безпеки хочуть неформальної бесіди з вами? Ви погодитеся на зустріч, ухилитеся від неї чи попросите корпоративного юриста написати електронного листа? Приблизно чверть аудиторії сказала, що зустрілася б, навіть після викриттів Сноудена. Стеймос сказав, що донедавна мав таку саму думку і торік витратив години на спілкування з органами влади на тій самій конференції. Тепер, сказав він, залучив би юриста. Що робити з корпоративним бекдором, який збирає дані ваших споживачів, якщо ваш бос наказує вам забути про нього? Проігноруєте його, повідомите вищому керівництву всередині організації, тихо пошукаєте роботу в іншому місці або відкрито звільнитеся та розірвете свою угоду про нерозголошення з поясненнями причини? Стеймос сказав, що обирав би між двома останніми відповідями.

Він завершив виступ, закликаючи старших і досвідченіших професіоналів ділитися своїми тяжкими рішеннями, ухваленими разом з новими молодшими спеціалістами, та обміркувати можливі сценарії, щоб не бути заскоченими зненацька. «Прагніть аналізувати своє життя»,— порадив він. Пізніше, 2013 року, я виявив, що сек'юріті-компанія *RSA* взяла 10 мільйонів доларів за створення бекдору АНБ в інструментарії, поширюваному

для захисту вебсайтів[11]. Стеймос був одним із десяти спікерів, які відмовилися виступати на *RSA Conference* 2014 року. Це були єдині збори в сек'юріті-галузі, більші за *Def Con*, і за іронією долі започатковані для боротьби з федеральними вимогами контролю над шифруванням. Замість залишитися вдома, Стеймос організував контр-конференцію, *TrustyCon*, влаштовану водночас із конференцією *RSA*, але присвячену реагуванню на неналежний урядовий вплив й інші загрози безпеці й приватності.

Пізніше того року *Yahoo* найняла Стеймоса директором з інформаційної безпеки за відкритість його суджень, частково у відповідь на махінації уряду, які викрив Сноуден. Але 2015 року Стеймос пішов з Yahoo[12]. Він пояснив своїм співробітникам, що нова гендиректорка Yahoo Марісса Меєр не попередила його про наказ Суду у справах спостереження за іноземною розвідкою, який таємно збирається для схвалення прослуховувань підозрюваних у міжнародному шпигунстві. Цей наказ вимагав від компанії встановлювати нові програми, щоб перевіряти кожен оброблюваний системою електронний лист на наявність певних електронних сигнатур, як-от встановлені на комп'ютері користувача *cookie*-файли чи шифрувальний ключ. Після того як члени команди Стеймоса знайшли на поштових серверах *Yahoo* дещо схоже на хакерський руткіт, вони злякалися, що це повернулися російські хакери, які завдали їм проблем у минулому, та сповістили Стеймоса. У понеділок о п'ятій годині ранку він зібрав усіх в офісі. Коли інженери електронної пошти запропонували порадитися з юридичним відділом, Стеймос так і зробив, дізнався,

що спостереження було санкціонованим, піднявся до самої Меєр і тихо пішов.

Ціль розвідувальних агентств США була легітимною. Але засоби, якими вони шукали кореспонденцію підозрюваних, і прихована співучасть *Yahoo* зробили посміховисько з річних звітів про прозорість, у яких *Yahoo* оцінила, скільки імейл-акаунтів вона перевірила для уряду. І якщо вона шукатиме одну секретну порцію інформації в усіх до єдиного електронних листах, що завадить їй зробити це знову, шукаючи фразу, наприклад, з висловленням ворожості щодо чинного чи наступного президента? Через цю історію деякі оголосили, що Стеймос зробив себе чимось на кшталт канарки у вугільній шахті, і якщо він піде з «Фейсбуку», користувачам слід узяти це до уваги.

[x x]

У «Фейсбук» Стеймос передовсім захищав саму компанію. Він також стояв між користувачами та організованими злочинцями, сексуальними хижаками та шахраями. Але під час виборів 2016 року він був насторожі щодо діяльності групи, відомої як *APT28*, яка мала зв'язок з ГРУ. Це була одна з груп, що зламала Національний комітет Демократичної партії, і члени команди Стеймоса виявили, що вона приховувалася за Фейсбук-сторінкою, присвяченою *DCLeaks* — вебсайту, який публікував викрадені електронні листи демократів. У серпні 2016 року вони встановили, що *DCLeaks* була «неавтентичною»,— політично нейтральна підстава для заборони,— але міжнародне занепокоєння щодо можливої упередженості відклало бан до жовтня. Група

Стеймоса виграла битву тільки після того, як *DCLeaks* оприлюднила телефонні номери, що мали стосунок до фінансиста Джорджа Сороса, порушуючи політику Фейсбуку щодо розкриття персональної інформації.

Після виборів і до вступу Трампа на посаду розвідувальні агентства США одностайно погодилися, що Росія втрутилася, щоб допомогти Трампу, та розповсюдила у Фейсбуку фейкові новини. Внутрішня оперативна група Фейсбуку дослідила їх і виявила переважно проплачених спамерів, які намагалися заманити людей на свої сторінки тенденційними історіями. Важливішими пріоритетами у Фейсбуку були прийдешні вибори в Західній Європі. Франція та Німеччина настійно просили про допомогу. Працюючи з французьким агентством кібербезпеки *ANSI*, яке спеціалізувалося тільки на захисті, експерти Фейсбуку виявили розвідку ГРУ стосовно працівників виборчої кампанії[13] та сотні тисяч пов'язаних з Росією фейкових французьких акаунтів, які поширювали публікації, здатні посіяти чвари. Тільки після того, як співробітники розвідки США повідомили журналу Time, що російські пропагандисти купували рекламу на Фейсбуку[14], компанія зрозуміла, що дослідження рекламних оголошень — це напрям дій, який передбачає криміналістичний аналіз великого обсягу даних.

Члени команди Стеймоса занурилися в них і знайшли масивний кластер Агентства інтернет-досліджень, структури зі штаб-квартирою у Санкт-Петербурзі, та дізналися, що фейкові активісти поширювали крайні ліві та праворадикальні тексти й меми. Спецпрокурор Роберт Мюллер зробив судові запити на матеріали, які

2018 року стали основою його обвинувачень[15] у втручанні в американські вибори проти тринадцяти росіян і трьох компаній. Найголовніша з тих компаній, Агентство інтернет-досліджень, придбала тисячі рекламних оголошень для провокування чвар у соціальних мережах. В одному з них чорношкірі чоловіки нападали на поліцейського; рекламу показували користувачам, які цікавилися або *Fox News*, або сенатором Тедом Крузом. Круз теж отримував твіти підтримки від акаунтів, створених Агентством інтернет-досліджень[16].

Стеймос намагався вчинити правильно[17], але заплатив за це високу ціну. Його керівники постійно мінімізували інформацію про російську активність у своїх публічних звітах. Коли він розповів правлінню компанії «Фейсбук» про те, що виявив у вересні 2017 року, директори спитали, чи видалив він усі фейкові акаунти. Він чесно відповів, що ні. Тоді вони накинулися на гендиректора Марка Цукерберга та головну операційну директорку Шеріл Сандберг з запитаннями, чому вони не повідомили їм, наскільки все погано. Сандберг зірвалася й накричала на Стеймоса: «Ти підставив нас!»

Стеймос ніколи не контролював увесь апарат безпеки в компанії, і сварка з правлінням закріпила його репутацію надто різкої людини. У грудні, коли Стеймос запропонував звітувати перед кимось ще, крім головного юридичного радника, інші керівники, які очолювали основний сервіс та інжиніринг Фейсбуку, сказали, що можуть упоратися з ширше інтерпретованою безпекою — тепер це тема глобального занепокоєння.

Стеймос, який 2015 року збільшив свій штат з 60 до 120 осіб, був витіснений, залишився з трьома працівниками та нечіткими повноваженнями щось вдіяти для безпеки виборів, як-от надання консультацій щодо планів протидії пропаганді. Він і Гізер Едкінс з *Google* допомогли проєкту «Захист електронної демократії» у Гарвардській школі державного управління імені Джона Ф. Кеннеді, яка, своєю чергою, консультувала виборчі кампанії та навчала службовців з тридцяти восьми штатів.

Стеймос пішов до кінця у професійній етиці, яку виклав на *Def Con* 2013 року. Але його контроль був меншим, ніж припустило багато людей за межами компанії, і він міг би зробити цей факт поширенішим. З іншого боку, він став директором з інформаційної безпеки у Фейсбуку до того, як інші зрозуміли, що найважливішою битвою буде не зламування та проникнення, а пропаганда. Стеймос домовився про звільнення з «Фейсбуку» у серпні 2018 року заради посади у Стенфордському університеті, щоб спробувати створити там форум для обговорення великими інтернет-компаніями серйозних проблем на нейтральній території. «Я не корпоративна шишка,— казав він.— Не мій рівень. Це “Гра престолів”». У прощальному службовому листі[18] він написав, що приймає на себе частину провини за маніпуляцію виборами, та закликав тих, хто залишався, «вилучити з пріоритетів короткостроковий розвиток» і «бути готовими обрати сторону, коли виникають чіткі етичні чи гуманітарні питання».

Коли *The Guardian* повідомила, що секретна фірма з урядового й політичного консультування *Cambridge Analytica* зібрала персональну інформацію десятків

мільйонів користувачів Фейсбуку через обманливе опитування і не видалила їх, коли Фейсбук попросив, Стеймоса не можна було змусити прийняти удар на себе. З технічної точки зору це не було порушення: це була помилка базових процесів розміщення реклами, над якими Стеймос не мав контролю. Натомість Цукербергу довелося йти в Конгрес вибачатися та обіцяти дати користувачам більше контролю над їхніми даними. Тим часом колишні керівники з Facebook і *Google* почали засуджувати своїх колишніх працівників за сприяння дезінформації. Трістан Гарріс, колишній спеціаліст з етики дизайну в *Google*, створив Центр гуманітарних технологій і попередив, що Фейсбук і Ютуб дозволили декільком найпотужнішим у світі зразкам штучного інтелекту з'ясувати, як утримувати увагу людей,— відповідь полягала в демонстрації наруги та екстремізмі. Прості технічні працівники[19] вимагали, щоб *Google* відмовилася від контракту з Пентагоном щодо створення штучного інтелекту для аналізу відеозаписів з безпілотника, який можна використовувати для точкових ліквідацій. Протести поширилися на сферу контрактів технологічних роботодавців з прикордонними органами, які відділяли дітей від батьків-іммігрантів.

[x x]

2017 року Адам О'Доннелл зв'язався зі Стеймосом, щоб поговорити про Бето. Він знав Стеймоса з часів *iSec* і захоплювався його етикою. Також він знав, що Стеймос вшанує найбільший секрет *cDc* — що Бето був одним із них. Стеймос відчув водночас шок і захват.

«Я маю підтримати цього хлопця, людину, яка активна в цьому світі з підліткового віку,— сказав Стеймос.— Можна на власні очі побачити співпрацю таких людей, як Бето і Герд». Він сказав друзям, що Бето знається на комп'ютерних технологіях, не згадавши його членство в *cDc*. У листопаді він допоміг Адаму організувати в його домі політичний збір коштів. Того вечора Бето виклав свої переконання та підхід. Бето поділяв погляди більшості членів *cDc* та спільноти Кремнієвої долини не тільки щодо технологічної політики, а й щодо легалізації легких наркотиків. Так само як Патрік Крупа і лібертаріанці-засновники *EFF*, Бето бачив, як прибутки від нелегальних наркотиків стають причиною вбивств, що руйнують Мексику та переходять її національний кордон. (Бето також ставав на бік республіканців у низці голосувань щодо скорочення регулювання і податків.) Найлегше, чим можна його заплямувати, сказав він, це два арешти двадцятирічної давнини, один за крадіжку зі зломом і другий за керування автомобілем у нетверезому стані. Жоден не закінчився засудженням. Бето сказав, що спілкувався з тими, хто потрапив у гіршу ситуацію і через це не міг голосувати. І він вірив у другий шанс.

Незмінно оптимістичні, шанси О'Рурка зростали, у той час як Трамп ішов хиткою ходою від кризи до кризи, постійно втручаючись, щоб допомогти Росії, навіть коли його найголовніші помічники публічно попередили про негативні наслідки. Круз підтримав Трампа попри свої попередні заперечення. «Круз — рідкісний і цінний талант[20]. Його настільки ненавидять, що будь-який прохідний демократ з мізерним шансом витиснути його мав привернути більше уваги та викликати більше надії,

ніж обіцяла політична динаміка»,— написав Френк Бруні у своїй недільній колонці в *New York Times* у квітні 2018 року, за місяць після того, як Бето переміг на первинному голосуванні. «Але Бето — більш ніж прохідний кандидат. На багатьох заходах його оточують натовпи прихильників. Люди вишукуються для селфі, а потім просять обіймів». Бруні зазначив, що Бето вільно володіє іспанською, любить класичний панк-рок і сучасну кантрі-музику та що журнал Vanity Fair назвав його «схожим на Кеннеді»[21]. На середину 2018 року Бето зібрав більше грошей, ніж Круз, й опитування щоразу сильніше наближали його до суперника, врешті-решт з різницею у статистичну похибку. Найбільшими перешкодами були слабке впізнання його імені та історія низької явки виборців, яку він намагався змінити. «Люди приходять, тому що не хочуть прикордонної стіни,— сказав Бето на Національному громадському радіо[22].— Вони приходять, тому що не вважають пресу ворогом. Вони вважають, що це найкращий захист від тиранії». Бето відмовився від допомоги консультантів і великих даних, а також від грошей з комітетів політичних дій, приймаючи малі окремі пожертвування та подорожуючи з міста в місто «у найпритаманніший панк-рок-гурту спосіб, який я знаю».

Бето, звісно, так не говорив, але це також був найпритаманніший хакеру спосіб, який він знав. Завдяки висловленню своїх думок у підпільній газеті своєї ери, на електронних дошках, а потім на альтернативному сайті новин в Ель Пасо, Бето навчився шукати нові ідеї, з комфортом бути собою та говорити з гумором, чесно спілкуючись із тими, хто відрізнявся замість пристосовуватися. Він дотримувався такої поведінки,

коли дедалі більше людей теж починали скоса дивитися на панівну політичну структуру, яку Трамп повів у новому та тривожному напрямку. А Круз дуже скидався на опортуніста й витвір тієї владної структури. Він назвав Трампа патологічним брехуном і запросив його приїхати агітувати за нього в Техасі.

Приїзди до всіх 254 техаських округів, навіть до тих, що здавна вважалися безнадійно республіканськими, без опитувань чи фокус-груп — це була хакерська політика. У вересні 2018 року на Бето чекатимуть найбільші натовпи, а поки його маленька команда використовувала айфони та соціальні мережі, щоб ділитися унікальними моментами. В одному з таких моментів чоловік спитав, чи співчуває він футбольним гравцям, які стають на одне коліно під час звучання національного гімну. Трамп неодноразово порушував питання, називаючи гравців, багато з яких були чорношкірими, непатріотичними «сучими синами»[23]. Бето, якому ніколи раніше не ставили такого запитання[24], подякував чоловіку. Потім він розповів коротку, енергійну, не підготовлену заздалегідь історію мирних протестів проти расистських політик і насильства і як це допомогло змінити Глибокий Південь. «Я не можу уявити щось більш американське, ніж мирно стояти чи стати на коліно, захищаючи свої права, будь-коли, будь-де, всюди»,— сказав Бето. Відео зібрало понад 40 мільйонів переглядів і принесло Бето телевізійне висвітлення подій у національному масштабі.

Поки діаграми в газетах прогнозували зміщення контролю над Сенатом ліворуч, одна з них показала, що якщо всі інші перегони відбудуться відповідно до

прогнозів, контроль залежатиме від того, чи виграє Бето. Навіть якщо він програє, було важко уявити його зникнення. Здавалося, національна політична сцена — так чи інакше його доля. Наближалися вибори, і він продовжував наступати на п'яти Крузу. Почалися порівняння з першим балотуванням Обами. «О'Рурк пропонує не просто шлях до перемоги в Техасі[25], а антидот до нещирості американської політики в епоху Трампа,— гучно повідомляв Vanity Fair.— Він щирий, енергійний і самостійно мислить. На якій ще планеті Бето О'Рурку бути кандидатом у президенти, навіть якщо він програє?»

[x x]

Хоча Бето був зобов'язаний обговорити свої арешти в 1990-ті, ніхто не знав про його підліткове хакерство, не кажучи вже про давній зв'язок з тими, хто роками був найвідомішою у світі групою технологічно обізнаних порушників правил, і зі зрозумілих причин він не розкривав цю інформацію. Втім, коли я сказав, що хочу включити його біографію до книжки після виборів[26], він був готовий розповідати. Значення членства в «Культі мертвої корови» анітрохи не бентежило його.

«Круто бути пов'язаним з людьми, які були членами cDc і частиною ранньої інтернет-культури,— сказав мені Бето.— Я був на периферії, але дуже хотів бути таким класним, як ці люди, бути таким досвідченим, технологічно майстерним, обізнаним і розумним, як вони. Цього не сталося, але здатність мати щось спільне з ними важила дуже багато для мене».

Бето народився на кілька років пізніше від засновників *cDc* і, за його словами, багато в чому був схожий на інших перших членів. «Мені було дуже тяжко пристосуватися до суспільства та йти традиційним маршрутом». Коли Бето навчався в середній школі, його батько, відомий місцевий суддя, приніс додому *Apple II* з модемом на 300 бод. Тож він почав шукати електронні дошки. Він знайшов декілька в Техасі, серед них *Demon Roach Underground* Кевіна Вілера в Лаббоку. Для відвідування віддалених дощок були потрібні вкрадені телефонні коди, «тому я не збільшував домашній рахунок за телефон». Частково дошки приваблювали тому, що були «чудовим способом завантажити зламані ігри». Пізніше він усвідомив свої неправильні рішення.

Але не ігри були тим, що спонукало Бето щоразу повертатися. «Брати в цьому участь, створити власну електронну дошку — все це, по суті, спричинено бажанням бути частиною спільноти»,— сказав він. Це також був пошук культури окремо від популярних фільмів і музики на радіо, протестованої ринком, неавтентичної та нудної, принаймні для Бето й інших підлітків у шуканні своєї ідентичності. «Це була контркультура: журнал *Maximumrocknroll*, купівля за каталогом аудіозаписів, які було неможливо знайти в музичних магазинах. *cDc* була певною мірою домом для людей, зацікавлених у тій частині контркультури». Бето теж шукав знань, «розуміння того, як функціонує світ — буквально, як працює телефонна система та як усі ми пов’язані одне з одним. У *cDc* всі були вільнодумними людьми».

Бето заходив на дошки переважно наприкінці 1980-х і на самому початку 1990-х, до навчання в Колумбійському

університеті. Пізніше він відвідував їх епізодично, почуваючись ближче до культурного флангу *cDc*, ніж до зірок-техногіків. Хоча Бето не був видатним програмістом, після випуску з коледжу він створював вебсайти і працював над високошвидкісними підключеннями в Нью-Йорку. Потім було повернення до Ель Пасо, власна маленька інтернет-компанія та низка політичних кампаній у статусі непопулярного кандидата. Вона почалася з сенсаційної перемоги, що принесла йому місце в міській раді. Серед інших неортодоксальних ходів був фінансований Бето захід 2009 року, який закликав до національної дискусії щодо легалізації марихуани.

Бето був переконаний, що його мислення сформувалось під впливом *cDc*. Він не в останню чергу боровся за відновлення мережевого нейтралітету. «Я розумію демократизаційну силу інтернету, як вона змінила мене особисто та як вона застосувала надзвичайні інтелектуальні здібності цих людей, які ділилися ідеями та методами,— висловився він.— Якщо ви ставите під загрозу здатність ставитися до всього цього рівно, це йде всупереч етиці груп, частиною яких ми є. І ви розумієте, що це заподіє шкоди розвитку малого бізнесу. Це обмежує можливість ділитися тим, що ви створюєте, — есеєм, піснею чи витвором мистецтва. І тому цей досвід впливає на те, що ми робимо зараз».

Бето сказав, що його біографія викликає в нього бажання просувати широке обговорення максимальної реалізації потенціалу обдарованих технічних спеціалістів й інших мислителів з нестандартними ідеями, які можуть справити більший вплив, адже відходять від закономірностей і традицій. Це була та сама ідея, яку

Мадж привніс у *DARPA*: додання схожих, але ускладнених засобів захисту не допомагає. «Дуже важливо вміти відійти від системи, критично поглянути на неї та розважитись у процесі,— сказав Бето.— На мою думку, «Культ мертвої корови» — чудовий цьому приклад. У такий спосіб ви зміцнюєте суспільство загалом, як було з програмними вразливостями: люди могли виявити їх, привернути увагу інших і взяти участь у виправленні».

«У контркультурі та контрсистемі було дещо дуже цінне. Реалізуючи ті таланти, ви поліпшуєте світ для всіх. Я приклад цього, починаючи від створення бізнесу з друзями і закінчуючи виборами в міську раду, Конгрес і балотуванням у сенатори. Частиною мого успіху було спілкування з людьми, які нестандартно мислили та досліджували, як улаштований світ. Існують альтернативні способи служити й досягти успіху. Важливо пам'ятати про це».

У день виборів за Бето проголосували 4,02 мільйони техасців проти 4,24 мільйонів голосів за Круза — з різницею менш як 3 відсоткові пункти. Явка в демократичних районах різко збільшилася: тільки в районі Г'юстону проголосувало на пів мільйона осіб більше, ніж на попередніх проміжних виборах. Той ентузіазм позбавив республіканців влади в найбільшому місті штату, змінив колір двох місць у Палаті представників і забрав більший кусень законодавчого органу штату. Професор Техаського університету Джеймс Генсон назвав це «початком кінця однопартійного правління в Техасі»[27].

Це була частина масштабної догани Трампу, яка здобула демократам Палату представників, і перша багатозначна перевірка влади президента. Хоча поразка Бето засмутила лідерів й активістів Демократичної партії, вони були настільки в захваті від його діяльності у штаті та на національному рівні, що почалися обговорення, чи варто йому балотуватися у Сенат від Техасу 2020 року або прагнути президентства, адже країна загалом значно менш консервативна за Техас. На першій сторінці першого недільного випуску New York Times після виборів політичні репортери написали, що демократи обговорюють, як їм діяти 2020 року — з помірними поглядами чи як ліберали, і «в центрі цих дебатів Бето О'Рурк»[28]. Через місяць[29], коли балотування Бето в президенти здавалося все більш імовірним, газета написала, що він усвідомив: в епоху Трампа довгий список досягнень має менше значення, ніж ентузіазм мас. Поки Бето обмірковував свій наступний крок, зіграла свою роль історія, яку, як він знав, буде розкрито в цій книжці.

Що стосується його юнацьких арештів і короткої панк-рок-кар'єри, республіканці неминуче використають його підліткові тексти та зв'язки, щоб очорнити його як культурно невідповідну й радикальну людину. Але цей спадок також здобуде глибоку лояльність деяких технічних спеціалістів Кремнієвої долини, яким уже було до вподоби його розуміння їхніх проблем, його ліберальний підхід до деяких питань і його лібертаріанство щодо інших. Вимушені внаслідок президентських виборів 2016 року обміркувати свою роль у суспільстві в менш приємному світлі, ті технічні

спеціалісти могли вважати Бето серйозним шансом виправлення ситуації.

Бето завершив свою службу в Конгресі та провів більшу частину січня, подорожуючи кількома штатами та спілкуючись з усіма, кого зустрічав, зважуючи свої наступні дії. Повернувшись, він домовився про інтерв'ю на шоу Опри Вінфрі та заінтригував політиків і публіку, сказавши, що незабаром ухвалить рішення. 14 березня, одразу після виходу документального фільму про його балотування в Сенат і провідної статті в Vanity Fair з біографією, Бето заявив про свій намір балотуватися на посаду президента США. «Це визначальний момент істини для цієї країни,— почав він своє відеозвернення. — Взаємопов'язані кризи нашої економіки, нашої демократії та нашого клімату серйозні як ніколи, і вони або поглинуть нас, або нададуть нам найпрекраснішу можливість реалізувати геній Сполучених Штатів Америки».

Наступного дня після оголошення, коли Бето опинився у вищому ешелоні перегонів і наша заборона на розкриття його юнацької таємниці втратила силу, агентство *Reuters* випустило об'ємне повідомлення на основі цього рукопису. Новина розлетілася країною, потрапила в кожну велику газету та вебсайт і спричинила більш як 50 мільйонів переглядів контенту в соціальних мережах. Такер Карлсон на *Fox News* висміяв вульгарний вірш про корову — т-файл, який Бето розмістив, коли був підлітком. На каналі *HBO* ведучий Білл Мар висловив у своєму вступному монолозі іншу точку зору: «Деякі цікаві паралелі між Трампом і Бето. Підлітком — це правда — Бето належав до хакерської групи, що називається "Культ мертвої

корови”. А Трамп як дорослий належить до хакерської групи, що називається Росією».

Загальні результати виявилися для його кампанії помірно позитивними. Багато молодих виборців, які раніше не були вражені Бето, сказали, що це було першим, що їх зацікавило, а в технічних спеціалістів голова пішла обертом. «Це одна з найдивовижніших речей, що колись опинялися в моїй стрічці у Твіттері, яка ніколи не була поганою»,— твітнула Робін Грін, керівниця «Фейсбуку» з питань конфіденційності та колишня співробітниця Американської спілки захисту громадянських свобод. Коли його про це запитували, Бето сказав, що за деякі свої перші тексти йому ніяково. Схвильовано спостерігаючи за подіями, головні члени *cDc* сподівалися, що мали рацію, що розкриття допоможе йому привабити молодих і невдоволених урядом виборців, не втративши забагато традиціоналістів. Ба більше, вони сподівалися, що Бето розкриє своє минуле та — хоч пан, хоч пропав — покаже, що майбутнє, яким керують хакери, може бути прекрасним.

ЕПІЛОГ

На самому початку головні питання етики для підлітків у «Культі мертвої корови» полягали в тому, наскільки припустимо зловживати картками для міжміських дзвінків і наскільки образливими мають бути їхні онлайн-дописи. Але, подорослішавши, хакери швидко стали критичними мислителями в епоху, коли ця навичка була дефіцитною. В еволюції, яка віддзеркалила, а відтак повела розвиток інтернет-безпеки, *cDc* перейшла до пошуку консенсусу щодо складного, але дуже важливого питання — розкриття вразливостей, показала, що створення стійкої безпеки може бути життєздатним бізнесом, і поєднала хакерський дух з активізмом на захист прав людини. І вона зберігала простір, якого вистачало для підтримки як актів громадянської непокори, так і роботи на військових, поки ця діяльність мала тверді принципи. Усі вони допомогли проштовхнути реалістичне розуміння проблем безпеки та етичні міркування в провідні обговорення у Кремнієвій долині та Вашингтоні. Оскільки загальна ситуація з безпекою гіршає, ті обговорення — найліпша надія, яка в нас є.

Перший урок з видатної історії «Культу мертвої корови»: ті, хто створює кодекс персональної етики й дотримується його в незнайомих обставинах, здатні на дивовижні речі. Другий: маленькі групи зі спільними цінностями можуть досягти ще більшого, особливо якщо їхні члени мають різні професії, життєвий досвід і точки зору. На початку великих змін різнопрофільні групи

першопрохідців здатні справити величезний вплив на їхню траєкторію. Після цього велику роботу можуть виконати уряди й великі компанії. Інші завдання, важливі для прогресу людства, потрібно виконувати в інших колах — малих і відданих своїй місії компаніях, університетах і неприбуткових організаціях. З часом стає складніше підтримувати цілісність групи, але вплив *cDc* живе в тих, кого найняли, навчили й надихнули її члени. Це означає, що рух не може контролювати своїх послідовників. *Citizen Lab* і Tor — одна річ, а *Lulz Security* та *Gamma Group* — геть інша. Тролінг і фейкові новини теж дечим завдячують *cDc*, і пишатися тут нічим.

Коли я завершував написання книжки, один помірно відомий фахівець з безпеки спитав своїх підписників у Твіттері про чинні етичні проблеми, з якими стикається галузь. Його стрічку завалили запитаннями. Якщо ви живете там, де шифрування заборонено, ви все одно допомагаєте активістам шифрувати? Якщо ви дізнаєтеся про застосування зловмисного софту, який, схоже, націлено на терористичну групу, ви розкажете про нього? Якщо ви створюєте моніторинговий інструмент, чи продасте його не підданим санкціям, але репресивним режимам? Якщо органи влади хочуть, щоб ви продали вразливість нульового дня брокеру замість попередити про неї постачальника, ви зробите це? Якщо уряд просить вашу антивірусну компанію пошукати в комп'ютерах конкретну сигнатуру, яка не є зловмисною програмою, ви погодитеся? Запитанням не буде краю, і мають бути кращі способи організації дискусій та отримання відповідей. Цьому допоможе зрушення в бік технологій, використовуваних у громадських інтересах, як це зробила *Citizen Lab*. Очікується, що юристи виконуватимуть волонтерську роботу, і, як зауважив

Брюс Шнаєр, є багато можливостей працювати на користь громадськості. Поки що це не стосується технічних спеціалістів.

Починаючи приблизно з 2000 року, після того як більшість людей у цій книжці закінчили коледж, акредитовані програми з інжинірингу й комп'ютерних наук у США зобов'язані містити навчання з питань етики, як правило, окремий курс. Ці курси надто часто викладають філософи, які не мають практичного досвіду. Найкращі тексти в галузі містять приклади на кшталт вибуху шатлу «Челленджер». До катастрофи зовнішній інженер не рекомендував запуск за холодної погоди, а потім дозволив керівництву переконати себе.

Деякі найкращі професійні об'єднання, як-от Інститут інженерів з електротехніки та електроніки (*Institute of Electrical and Electronics Engineers*)[1], мають кодекси етики на стадії повільного розвитку. Але їхнє членство обмежене, кодекси виконують, тільки якщо хтось скаржиться, а деякі настанови дуже неповні й не допомагають, коли члени звертаються за інформацією. Немає регулювання чи вимоги продовження освіти, як для юристів-практиків. Навіть канонічну літературу з безпеки мало читають. «Інженери справляють величезний вплив на суспільство,— сказав президент *IEEE* та чинний декан інженерного коледжу Моше Кам.— Але, відверто кажучи, це не приносить слави».

Навіть ті, хто наполегливо б'ється над такими питаннями, зрідка говорять про них на публіці, а це означає, що інші не можуть у них навчитися. Алекс Стеймос з «Фейсбуку» є винятком. Ще одним є Дуг Сон, мічиганський експерт, який починав у хакерській групі

w00w00 та заснував *Duo Security*, 2018 року придбану *Cisco* за більш як два мільярди доларів. 2016 року в промові перед студентами Мічиганського університету Сон стверджував, що етичні міркування мають бути основою благородних зусиль, адже технології — єдине, що підвищує людську продуктивність. «Суть безпеки в тому, як ви конфігуруєте владу[2], хто до чого має доступ. Це політичне питання»,— сказав він.

На його думку, замість уявляти світ як бінарний, тобто як добро та зло, корисніше обміркувати рольову систему гри *Dungeons&Dragons*, де одна вісь світогляду персонажа — це добро та зло, а інша — порядок і хаос. Дарт Вейдер, пояснив він, це законослухняне зло: він бажає порядку, просто заради поганої мети. Хакерську групу *w00w00* він охарактеризував як нейтральну в обох вимірах. Едвард Сноуден, можливо, є хаотичним добром, АНБ — законослухняним злом. Журнал *Phrack* був хаотичним злом, група *L0pht* — законослухняною нейтральною, а «Культ мертвої корови» — хаотичним добром. Хай що говорить закон, Сон вважає, що професійна етика вимагає від нього діяти на соціальне благо.

З усіх діячів технологічної галузі, що бурхливо розвивається та зараз має у своєму складі сім найдорожчих компаній світу, експерти з безпеки, як-от у *cDc*, були першими, хто щоденно стикається з питаннями совісті та величезних наслідків для захисту, приватності та спостереження. Але ці питання зараз розповсюджуються на весь технологічний світ. Фейсбук, Твіттер і Ютуб погано виконують завдання протидії пропаганді та дозволяють автоматизації просувати контент, який привертає увагу через те, що він

екстремістський. Google обмірковує повернення цензурованого пошуку в Китаї, звідки вона принципово пішла 2010 року. Втім, вона піддалася тиску працівників і відмовилася від контракту з Пентагоном щодо аналізу відеозапису з безпілотника, який можна використовувати для точкових ліквідацій. *Apple* билася з ФБР, відмовляючись створювати бекдори, але погодилася зберігати користувацькі дані в Китаї. Працівники Amazon проти, щоб компанія продавала поліції технологію розпізнавання облич, а люди в *Microsoft* борються з іммміграційними органами влади Трампа, які розділяють родини на кордоні. Технології як ціле заглиблені в явище, що може виявитися довгостроковою моральною кризою, і найкращий спосіб шукати мудрості в боротьбі з нею — звернутися до людей, які вже проходили крізь це, хоч де вони працюють: у гігантських компаніях, стартапах, неприбуткових організаціях чи Конгресі.

Що сильнішими стають машини, то більш виточеною має бути людська етика. Якщо сполучення бездумних, спрямованих на отримання вигоди алгоритмів, рішуче налаштованих геополітичних супротивників й опортуністів у США за останні кілька років і навчило нас чогось, ось цей урок: серйозне прикладне мислення є формою життєво важливої інфраструктури. Найкращі хакери — майстри прикладного мислення, і ми не можемо дозволити собі ігнорувати їх.

Так само їм не слід ігнорувати нас. Цей світ потребує більше добра. Якщо воно не може бути законослухняним, хай буде хаотичним.

Сан-Франциско — Бостон — Нью-Йорк — Вашингтон — Остін — Лос-Анджелес

ПОДЯКИ

Двадцять років тому деякі люди поскаржилися, що «Культ мертвої корови» прагне забагато уваги від медіа. Я мав справу з цією скаргою в основній частині книжки та вважаю, що вона несправедлива. Особисто я можу сказати, що не всі в групі вимагали пильної уваги, якої я тут цьому приділив.

Деякі члени дуже хотіли допомогти та ділилися особистою інформацією, навіть якщо вона могла зашкодити їм, і я хочу подякувати їм найбільше. Особлива подяка людям, які дозволили мені бути першим, хто назвав їх членами «Культу мертвої корови» під їхніми справжніми іменами: Кемаль Акман, Сем Ентоні, Люк Бенфі, Білл Браун, Керолін Кемпбелл, Метт Келлі, Міша Кубека, Ґленн Курцрок, Пол Леонард, Ден Макміллан, Адам О'Доннелл, Бето О'Рурк, Чарлі Родес, Майк Сірі, Ділан Ші та Кевін Вілер. Також варто зауважити, що деякі взагалі не хотіли говорити. Засновник групи Кевін Вілер місяцями не відповідав на повідомлення Люка, свого фактичного заступника протягом двадцяти років, щодо допомоги проєкту. Тільки після того, як Люк пригрозив надіслати йому співочу телеграму, Кевін нарешті погодився обговорити свою потенційну участь. Я вдячний, що він та інші дали свою згоду.

Багато людей, згаданих і не згаданих у цій книжці, люб'язно приділили мені свій час, і я дуже ціную їхні пояснення. За привітне прийняття й турботу про мене

в моїх дослідницьких подорожах я хочу подякувати Ральфу та Шону Логанам, Андреа Шеллкросс і Джонатану Берну, Рейчел Лейн і Джону Малруні, Барбарі Бестор і Тому Стерну та різним родичам. Також я у боргу перед низкою талановитих і працьовитих авторів, які зробили зрозумілими різноманітні аспекти історії та поточних проблем безпеки. Зокрема, це Джон Маркофф, Філ Лепслі, Фред Каплан, Рональд Дейберт, Шейн Гарріс, Енді Грінберг, Брюс Стерлінг, Стівен Леві та Ґабріелла Колман. Для тих, кому цікаво дізнатися більше про епоху електронних дощок, рекомендую багатосерійний документальний фільм Джейсона Скотта Садофського та його колекцію текстових файлів. Усе це доступно онлайн. Крім того, хочу висловити особливу подяку моїй гострозорій редакторці Колін Лоурі, агенту Девіду Паттерсону та радниці зі зв'язків із медіа Елінор Міллс.

Мені пощастило з 2012 року бути співробітником агентства *Reuters*, де працюють деякі найкращі журналісти у світі. Компанія надала мені можливість досліджувати складні та іноді ризиковані історії, які проклали шлях до цієї книжки. Крім того, Reuters люб'язно надала мені дві відпустки: 2014 року для відновлення здоров'я та у 2017–2018 роках для написання більшої частини цієї книжки. Гарна журналістика має величезне значення, і я радий, що багато людей підтримують її.

ПРИМІТКИ

Розділ 1. Вечір у Сан-Франциско

1. Я відвідав цей захід; цитати й описи взяті з моїх нотаток.

2. Якщо я цитую чиїсь думки у цій книжці, вони майже напевно надійшли від людини у прямому інтерв'ю. Я зазначаю, коли це не так. Якщо я згадую чиїсь дії, це означає, що я їх спостерігав, та людина розповіла мені про них пізніше або, у кількох випадках, про них мені розповіли декілька свідків.

3. Критик *cDc* під ніком Jericho написав, що це слово вперше з'явилось у маловідомому міннесотському друкованому виданні *InfoNation* 1995 року, https://jerichoattrition.wordpress.com/2014/02/17/on-the-origins-of-the-term-hacktivism/. Але огляд вживає це слово у значенні створення й використання альтернативних видань, а не технологічної підтримки прав людини. Внутрішні електронні листи щодо підготування *cDc* до *Def Con* показують, що члени групи вважають, що отримали нове слово, і вживали його в інтерв'ю, щоб сприяти його поширенню.

4. Це рік, який зараз називає засновник, але він передує першим електронним файлам. У друкованій версії

інтернет-видання *cDc* 1988 року оголошено, що група з'явилася 1986-го.

5. Я був присутній на тій промові. Усі згадувані презентації з конференцій я бачив або особисто, або на відеозаписах. Вони переважно доступні на Ютубі або інших сайтах, але я не надаю вебадрес більшості з них, тому що вони постійно змінюються.

Розділ 2. Техаські т-файли

1. Розповідь про юність Кевіна переважно надходить від нього самого. Те саме стосується більшості інших героїв книжки. Основну частину інформації отримано в особистих інтерв'ю з головними дійовими особами телефоном або засобами електронної комунікації.

2. Так свої слова пригадує Кевін. Коли я цитую когось, у переважній більшості випадків цитована особа сказала ці слова мені напряму, зазвичай в особистій розмові. Іноді коментарі надавали телефоном, електронною поштою чи в інших електронних повідомленнях. Якщо коментар отримано якось інакше, я згадаю це в примітках.

3. Swamp Rat, "Gerbil Feed Bomb", 1985, www.cultdeadcow.com/cDc_files/cDc-0001.html. Більшість текстових файлів, які я згадую, досі доступні онлайн на www.cultdeadcow.com або www.textfiles.com. Однак додання сюди посилання не гарантує, що текст згодом

зберігатиметься онлайн. Також зауважую, що не все на сайті *cDc* точне.

4. Цитата з електронного листа другові в *cDc*.

5. Інтерв'ю з Брюером.

6. Franken Gibe, "The Book of Cow", 1987, http://textfiles.com/groups/CDC/book.of.cow.

7. З останнього текстового файлу Franken Gibe, "Retro Cow", 1989, www.cultdeadcow.com/cDc_files/cDc-0100.html.

8. "Gibe's UNIX COMMAND Bible," 1987, http://textfiles.com/groups/CDC/cDc-0014.txt.

9. Ця фраза та її близькі варіації з'явились у файлах і публічних заявах *cDc*, зокрема на www.cultdeadcow.com/cDc_files/cDc-0100.html.

10. Psychedelic Warlord, "Visions from the Last Crusade", 1988, www.textfiles.com/groups/CDC/visions/crusade.

11. Psychedelic Warlord, "A Feature on MONEY — Today's Monster", 1987, http://textfiles.com/groups/CDC/cDc-0031.txt.

12. Psychedelic Warlord, "Interview with Neo-Nazi 'Ausderau", 1988, http://textfiles.com/groups/CDC/cDc-0059.txt.

13. Історія Кріса Такера взята з інтерв'ю з Осбандом, Маджем, Кевіном та іншими у cDc.

14. Найкраща розповідь про коеволюцію їппі та фрикерів — у книжці Філа Лепслі Exploding the Phone (New York: Grove Press, 2013).

15. Nightstalker, “Political Rant #1”, September 1, 1997, www.cultdeadcow.com/cDc_files/cDc-0339.txt.

Розділ 3. Конференції

1. Я не зміг зв’язатися з Джессі через близьких друзів, родичів, пошуки в базах даних чи старі адреси електронної пошти. Ця розповідь про його кар’єру спирається на інтерв’ю з його матір’ю, колишніми сусідами по житлу, близькими друзями та членами *cDc*.

2. Коментар з інтерв’ю з Саллі Манн. Вона також показала мені уривок зі своїх мемуарів, *The Band’s with Me* (self-pub., Big Gorilla Books, 2018), epub.

3. Phrack #32, November 17, 1990, www.phrack.org/issues/32/10.html.

4. Історію двох груп і суду над Нейдорфом я склав на основі інтерв’ю з членами *LoD* і *MoD* та іншими учасниками конференцій. Також я використав матеріали з книжок Bruce Sterling, *The Hacker Crackdown* (New York: Bantam Books, 1992) та Michelle Slatalla, Joshua Quittner, *Masters of Deception* (New York: HarperPerennial, 1995).

5. Дрю зробив серйозну кар'єру в *Tymnet*, *MCI* та *Level 3 Communications*, де був директором з інформаційної безпеки. Він не відповів на моє прохання дати інтерв'ю.

6. Більше про Бренда і зв'язки між психоделіками та великими технологічними інноваціями див. у John Markoff, *What the Dormouse Said* (New York: Viking, 2005).

7. John Perry Barlow, *"Crime and Puzzlement,"* Electronic Frontier Foundation, June 1990, www.eff.org/pages/crime-and-puzzlement. Сайт містить й інші його тексти.

8. Один із колишніх членів *MoD*, Red Knight, теж був у *cDc*. Пізніше він написав чотирьом ветеранам *cDc*, що після початку арештів кинув хакінг і пішов у будівельний бізнес.

9. Ґогганс розповів це журналу *Gray Areas* 1994 року. Він і Чейсін не відповіли на моє прохання надати коментарі.

10. Запис його промови є у приватному фільмі з основними моментами конференції, який показав мені член *cDc*.

11. Джессі сказав це в документальному фільмі «Несанкціонований доступ» Анналізи Севідж, доступному тут: https://archive.org/details/Hacker_Documentary_-_1994_-_Unauthorized_Access_by_Annaliza_Savage.

12. Patrick Kroupa, *"Voices in My Head,"* Excited Delirium, February 14, 1992, http:// exciteddelirium.net/voices-in-my-head-mindvox-overture/.

13. Загальну гульню описало багато свідків.

14. Цю історію мені розповіли і Мосс, і Беднарчик.

15. Наприклад, його подруга Анджела Дормідо розповіла мені, що Джессі надіслав їй фотографію гурту *Marilyn Manson* і сказав, що подорожував у турі з її гітаристом Джорді Вайтом та іншими. Дормідо була подругою Шутера, сина Вейлона Дженнінга — музиканта, який був в автобусному турі з Вайтом. Шутер зателефонував Анджелі та передав слухавку Вайту: той ніколи не чув про Джессі.

Розділ 4. Бостонський андеграунд

1. Я інтерв'ював півдесятка учасників. Кожну згадану мною подробицю підтвердили щонайменше двоє людей. Це моє загальне правило для цієї книжки, за винятком спогадів дитинства й незначних фактів.

2. Я спираюся на власне інтерв'ю з Джоном Лестером і те, що він дав *Decipher*, блогу компанії *Duo Security*, який 2018 року розповів історію *L0pht*. Dennis Fisher, *"'We Got to Be Cool About This': An Oral History of the L0pht, Part I",* Decipher, March 6, 2018, https://duo.com/decipher/an-oral-history-of-the-L0pht.

3. The Mentor, *"The Conscience of a Hacker",* Phrack #7, January 8, 1986, http://phrack.org/issues/7/3.html#article.

4. Крім Ріттера й Феннінга, у цьому виданні я згадую інших з моєї книжки про *Napster*: Перрі Барлоу, Джобі Бенджаміна, Білла Ґейтса, Стіва Джобса, Яна Кума, Кевіна Митника і Дуга Сона. Співзасновник *Napster* Шон Паркер став першим президентом компанії «Фейсбук», консультував Марка Цукерберга у відносинах з венчурними капіталістами та допомагав йому утримувати вплив на голосування в компанії, коли вона почала перетворюватися на одну з найважливіших у світі.

5. Mark Mueller, *“Hackers Go into Hiding as FBI Hunts for ‘u4ea”,* Boston Herald, March 10, 1996.

Розділ 5. Back Orifice

1. Це за словами Маджа, який іноді перебільшує.

2. Історію Йорка описали Мадж, Ден Макміллан і деякі сучасні онлайн-джерела. Його промову на HoHoCon можна побачити в приватному фільмі про цей захід. Я не зміг його знайти. Це не старший чоловік з таким самим ім’ям, який працював автором статей для *National Review*, *The Hill* та інших видань.

3. Ця частина розділу спирається на інтерв’ю з кількома людьми, які були тоді присутні.

4. Цим спеціалістом був Маркус Ранум, який створив першу електронну пошту для Білого дому та винайшов сучасну систему виявлення вторгнень. Обговорення

відносин Маджа зі зловмисним хакінгом спирається на інтерв'ю з ним у жовтні 2018 року.

5. Запис інтерв'ю зробив Міша, який змінив ім'я Люка. Текст доступний тут: www.cultdeadcow.com/oldskool/dateline.html.

6. Chris Williams, *"Air Force in Dogfight with Hackers",* San Antonio Express-News, August 11, 1996. Той самий матеріал вийшов у Rocky Mountain News тижнем пізніше під іншим заголовком. Обидві версії зараз не доступні онлайн.

7. Ця заява з'явилась у новинах на вебсайті *cDc*, зокрема тут: www.cultdeadcow.com/news/medialist.htm.

8. Omega, *"cDc Response to Newsday Magazine by Omega",* December 1, 1996, https://w3.cultdeadcow.com/cms/1996/12/cDcs-response-t.html.

9. Це слова хакера Майка Сіпі, який використовував нік Reid Fleming. Сіпі був старим другом Міші й давнім активним членом *cDc*.

10. Слоган зі сторінки *«The Yes Men»*, http://yeslab.org/theyeslab.

11. Розповідь з мого інтерв'ю з Джошем.

12. Matt Richtel, *"Hacker Group Says Program Can Exploit Microsoft Security Hole",* New York Times, August 4, 1998, https://archive.nytimes.com/www.nytimes.com/library/tech/98/08/cyber/articles/04hacker.html.

13. Знятий матеріал цього інтерв'ю надав мені член *cDc*.

14. Члени *cDc* отримали різноманітні службові записки та інші записи ФБР через запит відповідно до Закону про свободу інформації та показали їх мені, але не оприлюднили.

15. Оригінальне повідомлення *Microsoft* наразі видалене з її сайту. *cDc* розмістила його з покроковим спростуванням тут: www.cultdeadcow.com/tools/bo_msrebuttal.html.

Розділ 6. Мільйон доларів і монстр-трак

1. В електронному листі до групи.

2. Див., серед іншого, Austin Bunn, *"Beyond HOPE Hacks into Big Time",* Wired, August 11, 1997, www.wired.com/1997/08/beyond-HOPE-hacks-into-big-time, та Pamela Ferdin, *"Into the Breach",* Washington Post, April 4, 1998, www.washingtonpost.com/archive/politics/1998/04/04/into-the-breach/8ae3cf86-fbd7-4037-a1b6-842df39d9db7.

3. Більше про Eligible Receiver і Moonlight Maze див. Fred Kaplan, *Dark Territory* (New York: Simon & Schuster, 2016) та Thomas Rid, *Rise of the Machines* (New York: W. W. Norton, 2016).

4. Різні члени *L0pht* розповіли трохи різні версії того, як Кларк відвідав L0pht і як було організовано надання свідчень. Я використовую розповідь Кларка.

5. Жарт зі спогадів Маджа. Інші пригадують частину, коли Кларк дивується, що *L0pht* зміг зробити те, що зробив, без урядової підтримки.

6. Кріс Томас, найкращий архіваріус членів *L0pht*, розмістив запис слухання тут: www.spacerogue.net/wordpress/?p=602.

7. Немає ясності, на який баг посилалася група. На *Def Con* 2018 року Мадж повідомив, що виявив його на своїй основній роботі в *BBN*. Він сказав мені, що виробників роутерів сповістили до надання свідчень.

8. Коментар Вісопала на панелі *Def Con 2018*, що відзначала двадцятиліття тієї події.

9. Члени *cDc* отримали записи ФБР через запит відповідно до Закону про свободу інформації та показали їх мені, але не оприлюднили.

10. За показаними мені розсекреченими документами Кримінально-розслідувальної служби.

11. Член *cDc* Майк Сірі надав потрібну тисячу доларів. Юристкою була Сінді Кон.

12. За журналом ретрансльованого інтернет-чату, який не доступний публічно. Чоловік сказав у чаті, що тоді працював на *ISS*, але його профіль в *LinkedIn* показує, що він приєднався на повну ставку 2000 року.

13. Мадж сказав це режисеру фільму. Я бачив знятий матеріал.

14. Лист, підписаний ніком Майка Сірі, цитує *BBC* та інші. Повний текст є на www.mail-archive.com/siglinux@locutus.csres.utexas.edu/msg04587.html.

15. Те, як інфікувалися диски, мені розповів Крістіан й інші члени *cDc*. Фрід відмовилася дати інтерв'ю.

16. Коментар Кевіна в електронному листі членам *cDc*. Редакційна стаття газети вийшла 15 липня 1999 року. Зараз недоступна онлайн.

17. Bruce Schneier, *"Back Orifice 2000", Cryp-to-Gram* (newsletter), *Schneieron Security* (blog), August 15, 1999, www.schneier.com/crypto-gram/archives/1999/0815.html#BackOrifice 2000.

18 Електронний лист був відправлений підписникам групи *NTBugtraq*.

19. Цю історію мені розповіли Керрі та Роб Бек.

20. *"Bizarre Answers from Cult of the Dead Cow,"* Slashdot, October 22, 1999, https://news.slashdot.org/sTory/99/10/22/1157259/bizzare-answers-from-cult-of-the-dead-cow.

Розділ 7. Oxblood Ruffin

1. Count Zero, *“HoHoCon 1994 The Insanity Continues”,* January 6, 1995, www.cultdeadcow.com/oldskool/HoHo94.html.

2. Пізніше він сказав мені, що був волонтером у торонтівській групі *Web Networks*, яка створювала вебсайти для прогресивних груп, корінних племен та урядових агентств, і забезпечував себе іншою сторонньою роботою.

3. Вважаю себе зобов’язаним нагадати читачам, що спираюся на власні слова Лейрда про його життя до членства в *cDc*.

4. Електронний лист, надісланий групі.

5. John Perry Barlow, *“A Declaration of the Independence of Cyberspace”*, Electronic Frontier Foundation, February 8, 1996, www.eff.org/cyberspace-independence.

6. Я інтерв’ював його в будинку для літніх людей у Сан-Франциско наприкінці його життя.

7. Arik Hesseldahl, *“Hacking the Great Firewall”,* Wired, December 1997, 120, www.scribd.com/doc/237686960/Hacking-the-Great-Firewall.

8. Oxblood Ruffin, *“The Longer March,”* July 15, 1998, www.cultdeadcow.com/cDc_files/cDc-0356.html.

9. Arik Hesseldahl, *“Hacking for Human Rights?”,* Wired News, July 14, 1998, www.cultdeadcow.com/news/wired/19980714/.

10. *“President Clinton’s Visit to China in Context”,* Human Rights Watch, n.d., www.hrw.org/legacy/campaigns/china-98/visit.htm.

11. Naomi Klein, *“Computer Hacking New Tool of Political Activism”,* Toronto Star, July 23, 1998, reprinted at www.cultdeadcow.com/news/newspapers/Toronto_star72398.txt. Кляйн також написала про «Блондинок» у своїй книжці «No Logo», у якій пояснила, що підтвердила правдивість інтерв’ю Лейрда з Вонгом у «суб’єкта» тієї статті. Кляйн неодноразово відхилила прохання дати інтерв’ю.

12. *“St. Paul, Back Door Boom Boom, and All the Tea in China”* (press release), August 6, 1998, http://cultdeadcow.com/news/response.txt.

13. Maggie Farley, *“Dissidents Hack Holes in China’s New Wall”,* Los Angeles Times, January 4, 1999, http://articles.latimes.com/1999/jan/04/news/mn-60340.

14. Oxblood Ruffin, *“Chinese Checkers”,* cDc text file #361, December 23, 1998, www.cultdeadcow.com/cDc_files/cDc-0361.html.

15. *“LoU Strike Out with International Coa-lition of Hackers: A Joint Statement by 2600, the Chaos Computer Club, the Cult of the Dead Cow, !Hispahack, L0pht Heavy Industries, Phrack and Pulhas”* (press release), January 7, 1999, www.cultdeadcow.com/news/statement19990107.html.

16. Член *LoU* розповів Міші внутрішню історію під час обговорення, присвяченого демонстрації документального фільму про Анонімус, «Ми — легіон».

Член *LoU* Бронк Бастер пізніше приєднався до Hacktivismo та працював над ранньою, чорновою версією Peekabooty — браузера, що захищає приватність.

17. Oxblood Ruffin, *“Blondie Wong and the Hong Kong Blondes”,* Medium, March 23, 2015, https://medium.com/emerging-networks/blondie-wong-and-the-hong-kong-blondes-9886609dd34b.

18. Усю декларацію викладено в спільному пресрелізі *cDc-Hacktivismo*: *“International Bookburning in Progress”*, July 4, 2001, www.cultdeadcow.com/cDc_files/declaration.html.

19. В електронному листі Лейрда іншим у cDc.

20. *“The Hacktivismo FAQ v1.0,”* 2000–2001, www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html.

21. Перехресне опитування Болла доступне на вебсайті Міжнародного трибуналу щодо колишньої Югославії. Запитання щодо «Культу мертвої корови» датовано 14 березня 2002 року, на сторінці 2228 протоколу суду. www.icty.org/x/cases/slobodan_milosevic/trans/en/020314IT.htm.

22. Alexander Howard, *“Exit Interview: Alec Ross on Internet Freedom, Innovation and Digital Diplomacy”,* Huffington Post, March 12, 2013, www.huffingtonpost.com/alexander-howard/exit-interview-alec-ross-_b_2860211.html.

23. Розповідь про роботу О'Доннелла на ЦРУ спирається на інтерв'ю з двома людьми, знайомими з нею.

Розділ 8. Ставки ростуть

1. Вісопал пригадує, що першим виданням, яке оприлюднило їхні імена, був *Newsweek*. Мадж говорить, що його ім'я розкрив Білий дім, через що він увійшов до списку учасників тієї зустрічі з президентом.

2. Цю історію незалежно розповіли троє старших керівників *@stake*.

3. Снайдер є основним джерелом розповіді про її перебування в *Microsoft*.

4. Лічфілд розповів цю історію сам у статті в *Threatpost*: David Litchfield, *"The Inside Story of SQL Slammer",* Threatpost, October 20, 2010, https://threatpost.com/inside-story-sql-slammer-102010/74589/.

5. Dan Geer et al., *"CyberInsecurity: The Cost of Monopoly",* http://geer.tinho.net/pubs.

6. Історія походить з кількох інтерв'ю з Родрігесом.

7. Про захист приватності місцезнаходження, визнання щодо «Гонконгівських блондинок» і «одинокого вовка» розповів Мадж.

8. Перше публічне визнання Маджем його проблем із психічним здоров'ям відбулось у серії статей *Washington Post* про те, чому проблеми безпеки інтернету залишаються невирішеними: *"A Disaster Foretold — and Ignored",* Washington Post, June 22, 2015, www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/.

9. Інформація з розповіді самого Стівенса.

10. Про це повідомлено в Sean Naylor, *Relentless Strike* (New York: St. Martin's Press, 2015).

11. Річард Тім надіслав мені електронні листи від ветеранів.

12. «Енді Грінберг розповів про ветерана @*stake*, який називає себе Grugq, у *"Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits",* Forbes, March 23, 2012, www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/. Пізніше я написав статті для Reuters: *"Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback"*, Reuters, May 10, 2013, www.reuters.com/article/us-usa-cyberweapons-specialreport/special-report-u-s-cyberwar-strategy-stokes-fear-of-blowback-idUSBRE 9490EL20130510, *"Booming 'Zero-Day' Trade Has Washington Cyber Experts Worried,"* Reuters, May 10, 2013, www.reuters.com/article/us-usa-cyberweapons-policy/booming-zero-day-trade-has-washington-cyber-experts-worried-idUSBRE9490EQ20130510.

13. Я висвітлюю еволюцію ботнетів і причину поширеності російських шкідливих програм у *Fatal System Error* (New York: PublicAffairs, 2010).

14. *“Canvassing All Security Cracks”*, Sydney Morning Herald, April 22, 2005, www.smh.com.au/technology/canvassing-all-security-cracks-20050422-gdl620.html. Айтель не відповів на моє прохання дати інтерв’ю.

15. Інтерв’ю з Велом Смітом.

16. *“Phrack Prophile on the UNIX Terrorist”,* Phrack #65, November 4, 2008, http://phrack.org/issues/65/2.html.

17. Розповідь про *iSec* спирається на мої інтерв’ю зі Стеймосом і електронне листування з Рубіном.

Розділ 9. *Tor* і *Citizen Lab*

1. Robert Lemos, *“Long Haul Ahead for Social Hackers”,* ZDNet, February 19, 2002, www.zdnet.com/article/long-haul-ahead-for-social-hackers/. Барановські відмовився дати інтерв’ю. Де Вілла погодився.

2. Дейберт дякує Лейрду Брауну не тільки у своїх коментарях для мене, але також у своїй книжці *Black Code* (Toronto: Signal, 2013).

3. Ранню сферу застосування описано в книжці Дейберта.

4. Дослідження *Blue Coat* привернуло увагу панівних медіа. Компанія обвинуватила посередників продажу своїх продуктів.

5. Дослідження лабораторії висвітлено на її вебсайті: https://citizenlab.ca/category/research/.

6. Наприклад, Azam Ahmed, *"Spyware Trailed Investigators in Mexico"*, New York Times, July 9, 2017, www.nytimes.com/2017/07/10/world/americas/mexico-missing-students-Pegasus-spyware.html.

7. Я написав про балканізацію дослідження безпеки у *"Politics Intrude as Cybersecurity Firms Hunt Foreign Spies",* Reuters, March 11, 2015, www.Reuters.com/article/us-cybersecurity-fragmentation-insight/politics-intrude-as-cybersecurity-firms-hunt-foreign-spies-idUSKBN0M809N20150312.

8. Оригінальний звіт про *GhostNet* — *"Tracking GhostNet: Investigating a Cyber Espionage Network",* March 28, 2009 — тут: https://issuu.com/citizenlab/docs/iwm-GhostNet.

Розділ 10. Джейк

1. Ранню біографію Джейка висвітлили кілька журналістів, як-от Натаніель Річ у статті *Rolling Stone* (*"The American WikiLeaks Hacker",* December 1, 2010,

www.rollingstone.com/culture/culture-news/the-american-WikiLeaks-hacker-238019/). Давній друг Джейка підтвердив основні моменти в матеріалі *Rolling Stone*. Сам Еплбаум не відповів на мої прохання про інтерв'ю електронною поштою та особисті повідомлення у Твіттері.

2. Rich, *"The American WikiLeaks Hacker"*.

3. Найкраща книжка про Ассанжа — Andy Greenberg, *This Machine Kills Secrets* (New York: Plume, 2012). Його електронні листи групі Cypherpunks доступні в її архіві, який іноді переміщується в мережі.

4. Див. Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy* (Brooklyn, NY: Verso, 2014); Parmy Olson, *We Are Anonymous* (New York: Back Bay Books, 2012).

5. *"Cyberactivists Warned of Arrest",* Financial Times, February 4, 2011, www.ft.com/content/87dc140e-3099-11e0-9de3-00144feabdc0. Серед інших моїх статей про «Анонімус» і LulzSec — *"They're Watching, and They Can Bring You Down",* FT Magazine, September 23, 2011, www.ft.com/content/3645ac3c-e32b-11e0-bb55-00144feabdc0#axzz1YtFTuZd2.

6. Ryan Gallagher, *"Why Hacker Group LulzSec Went on the Attack",* Guardian, July 14, 2011, www.theguardian.com/technology/2011/jul/14/why-LulzSec-decided-to-disband.

7. В електронному листуванні зі мною.

8. Olson, *We Are Anonymous*, 326–329.

9. Правоохоронні працівники США і СК повідомили це мені, коли я писав про «Анонімус» для *Financial Times*. Я провів інтерв'ю з Кассандрою Фейрбенкс.

10. Як Сноуден обрав журналістів, виявилося набагато пізніше його публічних заяв. Цю версію розповіли на пам'ятному заході на честь Джона Перрі Барлоу (на якому я був присутнім). Відеозапис заходу доступний онлайн і вартий перегляду: https://supporters.eff.org/civicrm/event/info?reset=1&id=191. Про публікацію документів Сноудена розповів Тревор Тімм; обговорення починається приблизно на 1:32:00.

11. У центрі цієї історії документ, відомий як Каталог *ANT*, зі списком пристроїв і технологій електронного шпигунства. *The Guardian* та інші видання утрималися від указування пристроїв і програм, які може зламати АНБ,

12. Гарними доповідями про обхід Агентством стандартів є Nicole Perlroth, Jeff Larson, and Scott Shane, *"N.S.A. Able to Foil Basic Safeguards of Privacy on Web",* New York Times, September 5, 2013, www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html; James Ball, Julian Borger, and Glenn Greenwald, *"Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security,"* Guardian, www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; "Dual EC DRBG," Project Bullrun, July 31, 2005, https://projectbullrun.org/dual-ec/index.html.

13. Ці подробиці розповіли троє людей, які були в курсі подій.

14. Первинна заява Ектона доступна тут: https://Signal.org/blog/Signal-foundation/. Друга цитата — з його інтерв'ю зі мною.

15. Пойтрас підтвердила ці стосунки у своєму фільмі «Ризик». Жардін підтвердила їх в електронному листі.

16. Челсі Комло розповіла свою історію анонімно для вебсайту JacobAppelbaum.net, а пізніше — під своїм ім'ям. Після цього я поспілкувався з нею. Також я опитав Лі Ганівелл й інших, хто був причетний до розслідування в Tor. Як зазначено раніше, Еплбаум не відповів на прохання дати інтерв'ю. Бернштейн теж. Гілмор захищав Джейка в приватному електронному листі.

17. Leigh Honeywell, *"He Said, They Said",* hypatia.ca, June 7, 2016, https://hypatia.ca/2016/06/07/he-said-they-said/.

18. З інтерв'ю з людиною, причетною до розслідування.

19. Ферр написав це в дописі в *Medium*. Пізніше він видалив його, кажучи, що не хоче ще більше розколювати спільноту інформаційної безпеки. Архів оригіналу доступний тут: https://web.archive.org/web/20160606222408/https://medium.com/@nickf4rr/hi-im-nick-farr-nickf4rr-35c32f13da4d.

20. *"CULT OF THE DEAD COW Statement on Jacob Appelbaum / ioerror"* (press release), June 6, 2016,

http://w3.cultdeadcow.com/cms/2016/06/cult-of-the-dead-cow-statement-on-jacob-appelbaum-ioerror.html.

21. Oxblood Ruffin, *“Public Figures & Anonymous Victims,”* Medium, June 8, 2016,

https://medium.com/@oxbloodruffin/public-figures-anonymous-victims-543f0b02d684.

22. *“Read Mueller Probe Indictment of 12 Russians for Hacking Democrats”,* Washington Post, n.d., http://apps.washingtonpost.com/g/documents/national/read-mueller-probe-indictment-of-12-russians-for-hacking-democrats/3087/.

Розділ 11: Мікстер, Мюнч і Фінеас

1. «Коментарі Марлінспайка наведено в дуже гарній статті Енді Грінберга в журналі *Wired*: *“Meet Moxie Marlinspike, the Anarchist Bringing Encryption to All of Us”,* Wired, July 31, 2016, www.wired.com/2016/07/meet-moxie-marlinspike-anarchist-bringing-encryption-us/.

2. Мюнч не відповів на мої прохання про інтерв’ю.

3. Часткова версія є онлайн на https://archive.org/stream/186_201106-ISS-ELAMAN1/186_201106-ISS-ELAMAN1_djvu.txt.

4. Lorenzo Franceschi-Bicchierai, *“Hacker ‘Phineas Fisher’ Speaks on Camera for the First Time — Through a Puppet”,* Motherboard, July 20, 2016, https://motherboard.vice.com/en_us/article/78kwke/hacker-phineas-fisher-hacking-team-puppet. Інтерв’ю провів журналіст *Vice* Лоренцо Франческі-Біккере, який чудово дослідив хакінг *Gamma Group* і декілька наслідувальних атак на постачальників шпигунських програм. Він не без підстав відмовився передати Фінеасу моє прохання про інтерв’ю.

5. Enric Borràs, *“Phineas Fisher; ‘I’m Wanted by Much More Powerful Police Forces than Catalonia’s and for Much Worse Crimes”,* Ara, June 6, 2016, www.ara.cat/en/Im-much-powerful-Catalonias-crimes_0_1590441016.html. Автор тієї статті теж відмовився допомогти мені зв’язатися з Фінеасом для інтерв’ю.

6. Група розмістила своє часто цитоване попередження та поради на https://pastebin.com/raw/Y1yf8kq0.

7. Gabriella Coleman, *“The Public Interest Hack,”* Limn, issue 8 (February 2017), https://limn.it/articles/the-public-interest-hack/.

8. Роботу очолював *International Consortium of Investigative Journalists* (www.icij.org) за головною участю компанії *McClatchy* та газети *Miami Herald*.

9. Коли я спитав Євгенія Касперського щодо тих заяв, він підтвердив, що софт компанії іноді збирає неактивний код. Joseph Menn, *“Kaspersky Acknowledges Taking Inactive Files in Pursuit of Hackers”,* Reuters, November 3, 2017, www.Reuters.com/article/us-cyber-summit-

Kaspersky/Kaspersky-acknowledges-taking-inactive-files-in-pursuit-of-hackers-idUSKBN1D328B.

10. Alec Luhn and Ian Black, *“Erdogan Has Apologised for Downing of Russian Jet, Kremlin Says”,* Guardian, June 27, 2016, www.theguardian.com/world/2016/jun/27/kremlin-says-erdogan-apologises-russian-jet-turkish.

11. Dissent, *“Notorious Hacker ‘Phineas Fisher’ Says He Hacked Turkey’s Ruling Political Party”,* July 21, 2016, https://www.databreaches.net/notorious-hacker-phineas-fisher-says-he-hacked-turkeys-ruling-political-party/.

12. Пізніше Вайт видалив з мережі свій особистий сайт.

13. Lorenzo Franceschi-Bicchierai, *“Hacking Team Hacker Phineas Fisher Is Taking a Break Because of Stress”,* Motherboard, February 9, 2017, https://motherboard.vice.com/en_us/article/xy5enw/hacking-teams-phineas-fisher-will-return-but-only-after-a-break-at-the-beach.

14. Піцос так описав платформу *Kialo* газеті *Financial Times* у статті *“Meet the Start-Up That Wants to Sell You Civilised Debate”*, January 24, 2018, www.ft.com/content/4c19005c-ff5f-11e7-9e12-af73e8db3c71.

Розділ 12. Мадж і Крістіан

1. Є багато історій, звідки з'явився найвідоміший нік Маджа. Правда нудна: як пояснив Мадж технологічній журналістці Елінор Міллс, це було справжнє прізвище його однокласника.

2. Інтерв'ю з Серфом.

3. Дуган використала цю версію фрази в різних розмовах, але вона бере початок від створення агентства. Схоже формулювання є в довідковому матеріалі про *DARPA*: www.DARPA.mil/attachments/DARPA_Fact_Sheet_1_07-25-17.pdf.

4. Моїми основними джерелами інформації про цю зустріч є Сон і Мадж. На відео в Ютубі Мадж завдячує Сону ідеєю *CFT*.

5. Історію фінансування проєкту Міллера розповіли і Мадж, і Міллер.

6. Частини системи засекречено, але Мадж обговорив інші її аспекти зі мною та в розмовах, запис яких доступний на Ютубі. Повідомлялося, що інший проєкт Маджа, з відстеження незвичайної активності в мережі, був спрямований на виявлення таємних агентів і викривачів. Але Мадж рішуче це заперечує, кажучи, що проєкт полював на дії з облікових записів, викрадених сторонніми. Кауфман підтримує його версію.

7. Я бачив відредаговану вручну версію подяки.

8. Мадж розповів про проєкт на річній конференції розробників Google 2015 року; запис можна подивитися

тут: www.YouTube.com/watch?v=mpbWQbkl8_g.

9. Мадж і Сара Затко виклали результати роботи лабораторії на *Black Hat* й інших конференціях.

10. Значна частина злочинних і геополітичних шкідливих програм роками спиралася на вразливості у *Flash Player*. Його слабка захищеність була однією з причин, з яких Apple припинила підтримку *Flash*. 2018 року він майже не використовується.

11. Hugh Gallagher, *"White Boy Rocks Harlem",* YouTube video, 2:40, June 28, 2006, www.YouTube.com/watch?v=Hv1ihFI5iKI.

12. Дані, розкриті кураторкою *Project Zero* і *Google Chrome* Парісою Табріз у промові на *Black Hat* 2018 року, доступні тут: Seth Rosenblatt, *"Google's 'Security Princess' Calls for Stronger Collaboration",* Parallax, August 8, 2018, www.the-parallax.com/2018/08/08/Google-security-princess-parisa-tabriz-black-hat/.

Розділ 13. Конгресмен і тролі

1. У складі групи також був Седрик Бікслер-Завала, згодом соліст *The Mars Volta*, гурту-переможця премії Ґреммі. 1994 року Foss виступала на телешоу в Ель Пасо: *"Foss on Let's Get Real TV show — El Paso, TX-1994 Pt 3- The Song",* YouTube video, 9:59, June 30, 2012,

www.YouTube.com/watch?time_continue=2&v=eI5GGPFnX24.

2. Пізніше на восьмому місці за рейтингом *CBS News* у лютому 2015 року: Bruce Kennedy, *“America’s 11 Poorest Cities”,* MoneyWatch, CBS News, February 18, 2015, www.cbsnews.com/media/americas-11-poorest-cities/.

3. Beto O’Rourke and Susie Byrd, *Dealing Death and Drugs: The Big Business of Dope in the U.S. and Mexico* (El Paso, TX: Cinco Puntos Press, 2011).

4. Є багато гідних статей про кар’єру та кампанію Бето, хоча жодна не описує його юнацьке хакерство та дописи на електронних дошках. До найкращих матеріалів належить Patrick Svitek, *“Rep. Beto O’Rourke, in Long-Shot Bid for Senate, Is No Stranger to ‘Calculated Risks’ ”,* Texas Tribune, April 7, 2017, www.texastribune.org/2017/04/07/beto-orourke-2018-senate-bid-ted-cruz/; Eric Benson, “What Makes Beto Run?”, Texas Monthly, January 2018, www.texasmonthly.com/articles/makes-beto-orourke-run/.

5. Allana Akhtar and Paul Singer, *“Facebook Live, Periscope Have Big U.S. Political Moment with House Sit-In”,* USA Today, June 23, 2016, www.usatoday.com/story/tech/news/2016/06/23/Facebook-live-periscope-have-big-political-moment-house-sit-/86297956/.

6. Великі фрагменти трансляції можна знайти за гештеґом #BipartisanRoadtrip.

7. https://neveragain.tech.

8. Після інтерв'ю з ним антифашистська група розкрила його справжнє ім'я. Потім двоє помічників Нунана підтвердили його мені. 2019 року Нунан сказав мені, що залишив минуле позаду: «Я кинув політику та переконую праворадикальних активістів і білих націоналістів, з якими був у Шарлоттсвіллі, не приймати "кислоту" й кетамін у спробі переосмислити своє життя та зберегти значення для суспільства, а не падати в кролячу нору».

9. Eric Geller, *"Neo-Nazi Activist May Be Behind Fake Macron Accounts",* Politico, January 28, 2018, www.politico.eu/article/neo-nazi-activist-may-be-behind-fake-macron-documents/. В електронному листуванні зі мною 2019 року Ауернгеймер відмовився відповідати на запитання щодо його діяльності під час американських чи французьких виборів, але сказав, що не співпрацював з Росією.

10. Висвітлення ситуації з *Cambridge Analytica*, включно з установленням особистості викривачем, очолювала газета Guardian.

11. *"Exclusive: Secret Contract Tied NSA and Security Industry Pioneer"*, Reuters, December 20, 2013, www.Reuters.com/article/us-usa-security-RSA-idUS-BRE9BJ1C220131220. Продовження тут: Joseph Menn, "Exclusive: NSA Infiltrated RSA Security More Deeply than Thought — Study", Reuters, March 31, 2014, www.Reuters.com/article/us-usa-security-nsa-RSA/exclusive-nsa-infiltrated-RSA-security-more-deeply-than-thought-study-idUSBREA2U0TY20140331?irpc=932.

12. Joseph Menn, *“Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence — Sources”,* Reuters, October 4, 2016, www.Reuters.com/article/us-Yahoo-nsa-exclusive/exclusive-Yahoo-secretly-scanned-customer-emails-for-u-s-intelligence-sources-idUSKCN1241YT.

13. Joseph Menn, *“Exclusive: Russia Used Facebook to Try to Spy on Macron Campaign”,* Reuters, July 26, 2017, www.Reuters.com/article/us-cyber-france-Facebook-spies-exclusive/exclusive-russia-used-Facebook-to-try-to-spy-on-macron-campaign-sources-idUSKBN1AC0EI. У цей час я ретельно висвітлював Фейсбук, пропаганду та хакінг і проінтерв’ював джерела з розвідки, Конгресу, Фейсбуку та зовнішньої безпеки.

14. Massimo Calabresi, *“Inside Russia’s Social Media War on America”,* Time, May 18, 2017, http://time.com/4783932/inside-russia-social-media-war-america/.

15. *“13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign”,* New York Times, February 16, 2018, https://www.ny times.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html.

16. Josh Russell, *“If you go look at the Clemson researchers database there are at least 4500 tweets containing ‘Cruz’ dating all the way back to february 2015”,* Twitter, September 13, 2018, 7:39 p.m., https://twitter.com/josh_emerson/status/1040429696792637440.

17. Про інцидент у правлінні повідомлено в статті Sheera Frenkel et al., *“Delay, Deny and Deflect: How Facebook’s*

Leaders Fought Through Crisis", New York Times, November 14, 2018, www.nytimes.com/2018/11/14/technology/Facebook-data-russia-election-racism.html.

18. Ryan Mac and Charlie Warzel, *"Departing Facebook Security Officer's Memo: 'We Need to Be Willing to Pick Sides'",* Buzz-Feed News, July 24, 2018, www.buzzfeednews.com/article/ryanmac/Facebook-alex-stamos-memo-cambridge-analytica-pick-sides.

19. Daisuke Wakabayashi and Scott Shane, *"Google Will Not Renew Pentagon Contract That Upset Employees",* New York Times, June 1, 2008, www.nytimes.com/2018/06/01/technology/Google-pentagon-project-maven.html.

20. Frank Bruni, *"Watch Out, Ted Cruz, Beto Is Coming",* New York Times, April 7, 2018, www.nytimes.com/2018/04/07/opinion/sunday/ted-cruz-beto-orourke-texas.html.

21. Abigail Tracy, *"Meet the Kennedyesque Democrat Trying to Beat Ted Cruz",* Vanity Fair, May 31, 2017, https://www.vanityfair.com/news/2017/05/beto-orourke-ted-cruz-texas-senate-2018.

22. Wade Goodwyn, *"Texas Democrat's Underdog Bid to Unseat Ted Cruz Picks Up Momentum",* All Things Considered, NPR, March 5, 2018, www.npr.org/2018/03/05/590709857/texas-democrats-underdog-bid-to-unseat-ted-cruz-picks-up-momentum.

23. Adam Edelman, *"Trump Rips NFL Players After Anthem Protests During Preseason Games",* NBC News, August 10, 2018, www.nbcnews.com/politics/donald-trump/trump-rips-nfl-players-after-protests-during-preseason-games-n899551.

24. Daniel Kreps, *"Watch Beto O'Rourke Talk Trump's Texas Visit, NFL Kneeling Viral Video on 'Ellen'",* Rolling Stone, September 5, 2018, www.rollingstone.com/politics/politics-news/watch-beto-orourke-talk-trumps-texas-visit-nfl-kneeling-viral-video-on-ellen-719245/.

25. Peter Hamby, *"'It Seems Like Iowa in 2007': Is Beto O'Rourke the Left's Obama-Like Answer to Trump in 2020?",* Vanity Fair, August 29, 2018, www.vanityfair.com/news/2018/08/could-beto-orourke-be-the-next-obama.

26. Знаючи, що до групи належав конгресмен, я припустив, що це був Бето, на основі пресрепортажу про його перегони за Сенат з описом його бунтарської юності в Техасі. Але інші члени не підтвердили мої підозри, тому я дав слово, що не публікуватиму книжку до завершення виборів у листопаді 2018 року. Вони погодилися на мої умови, а потім я запропонував Бето таку саму угоду.

27. James Henson, *"Beto O'Rourke Should Run for Senate in 2020. He Could Win",* Washington Post, November 9, 2018, https://www.washingtonpost.com/opinions/beto-orourke-should-run-for-senate-in-2020-he-could-win/2018/11/09/99263192-e462-11e8-ab2c-b31dcd53ca6b_story.html?utm_term=.d75abaa157b8.

28. Jonathan Martin and Alexander Burns, *“Democrats Have Two Paths for 2020: Daring or Defensive. Can They Settle on Either?”,* New York Times, November 10, 2018, https://www.nytimes.com/2018/11/10/us/politics/democrats-2020-president.html.

29. Matt Flegenheimer and Jonathan Martin, *“Beto O’Rourke Emerges as the Wild Card of the 2020 Campaign-in-Waiting”,* New York Times, December 9, 2018, www.nytimes.com/2018/12/09/us/politics/beto-2020-presidential-race.html.

Епілог

1. Кодекс організації доступний за посиланням www.ieee.org/about/corporate/governance/p7-8.html.

2. Деякий час промова Дуга Сона була доступна на Ютубі.

ПРО АВТОРА

Джозеф Менн — репортер, який спеціалізується на розслідуваннях для Reuters, найдавніший і найбільш шанований провідний журналіст у сфері кібербезпеки. Він тричі отримав винагороду *Best in Business* від *Society of American Business Editors and Writers* і тричі був фіналістом премії імені Джеральда Льоба. Його книжка *Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet* розкрила співпрацю російського уряду з кримінальними хакерами та 2010 року ввійшла до десяти найкращих нехудожніх книжок за рейтингом *Hudson Booksellers*. Також він написав *All the Rave: The Rise and Fall of Shawn Fanning's Napster*, яка потрапила у фінал конкурсу «Книжка року» некомерційної організації *Investigative Reporters and Editors, Inc.* Раніше працював на *Financial Times*, *Los Angeles Times* і *Bloomberg* та виступав на конференціях *Def Con*, *Black Hat* і *RSA*. Виріс поблизу Бостону, мешкає у Сан-Франциско.

[1] Англ. *Cult of the Dead Cow*, далі вживається скорочена назва *cDc*.— *Прим. перекл.* Повернутися

[2] Англ. *«white hat»* означає фахівця, який спеціалізується на дослідженні та зламі комп'ютерних систем з метою виявлення вразливостей і, на відміну від кіберзлочинців, повідомляє про свої знахідки розробникам.— *Прим. перекл.* Повернутися

[3] Неофіційні кольори відповідно Демократичної та Республіканської партій.— *Прим. перекл.* Повернутися

[4] Американський співак і автор пісень, один з піонерів рок-н-ролу.— *Прим. перекл.* Повернутися

[5] Англ. «уіppy» від абревіатури *YIP — Youth International Party*.— *Прим. перекл.* Повернутися

[6] Від англ. *groupie* — шанувальниця поп- чи рок-гурту, яка супроводжує своїх кумирів під час гастролей.— *Прим. перекл.* Повернутися

[7] Хакери-початківці або взагалі некваліфіковані хакери, часто зависокої про себе думки, які використовують для атак на мережі готові хакерські інструменти, не розуміючи, як вони написані та як працюють.— *Прим. перекл.* Повернутися

[8] Район Мангеттена. Свою назву отримав через високий рівень злочинності, яка робила Пекельну кухню одним з кримінальних центрів Нью-Йорка з середини 1800-х до кінця 1980-х років.— *Прим. перекл.* Повернутися

[9] Автори дописів на інтернет-форумах, що або висловлюють нігілістичні думки, або містять посилання на Гітлера, фашизм, нацизм та інші табуйовані теми з метою шокувати або образити читачів.— *Прим. перекл.* *Повернутися*