NICOLE PERLROTH

CYBER BROŃ

i wyścig zbrojeń

Mówią mi, że tak kończy się świat

Książka biznesowa roku 2021 wg „Financial Times” i McKinsey

mt biznes

NICOLE PERLROTH

CYBER i wyścig zbrojeń BROŃ

Mówią mi, że tak kończy się świat

Książka biznesowa roku 2021 wg „Financial Times" i McKinsey

Przekład: Katarzyna Mironowicz

mt biznes

SPIS TREŚCI

Część V. OPÓR

Część VI. TORNADO

Część VII. BUMERANG

OD AUTORKI

Książka ta jest owocem siedmiu lat pracy nad wywiadami z ponad trzema setkami osób, które uczestniczyły, śledziły lub były bezpośrednio dotknięte przez podziemny przemysł cyberbroni. Wśród moich rozmówców znaleźli się hakerzy, aktywiści, dysydenci, naukowcy, specjaliści IT, przedstawiciele administracji USA i rządów innych krajów, biegli sądowi oraz zleceniobiorcy.

Wielu z nich nie wahało się poświęcić długich godzin, a nawet dni, na odtworzenie szczegółów określonych wydarzeń i rozmów przywołanych na stronach niniejszej książki. Prosiłam swoje źródła o udostępnienie, w miarę możliwości, dokumentacji w postaci umów, korespondencji mailowej, wiadomości oraz cyfrowych okruchów, które w wielu przypadkach zostały uznane za tajne lub uprzywilejowane na mocy umów zobowiązujących do zachowania poufności. Zdarzenia przywołane przez moje źródła znajdują potwierdzenie w nagraniach audio, zapiskach w kalendarzach oraz notatkach.

Ze względu na wrażliwy charakter omawianej materii wielu rozmówców zgodziło się na wywiad pod warunkiem nieujawniania ich tożsamości. Dwie osoby występują w książce pod zmienionym imieniem i nazwiskiem. Ich relacje – w miarę możliwości – zostały sprawdzone. Część moich źródeł wyraziła zgodę jedynie na zweryfikowanie relacji innych informatorów.

Czytelnik nie powinien zakładać, że jakakolwiek osoba wymieniona na tych stronach była bezpośrednim uczestnikiem opisywanych wydarzeń lub dialogów. Niejednokrotnie uczestnicy zdarzeń byli jednocześnie źródłem informacji, jednak niektóre relacje pochodzą od świadków, osób trzecich lub, jeśli było to możliwe, z pisemnych dokumentów.

W przypadku handlu cyberbronią nietrudno zauważyć, że hakerzy, nabywcy, sprzedawcy, a także rządy jak ognia unikają dokumentacji pisemnej. Wiele relacji i anegdot nie znalazło się na stronach książki ze względu na brak wiarygodnych informacji potwierdzających przytoczone fakty. Liczę na wyrozumiałość czytelników.

Zrobiłam wszystko, co w mojej mocy, jednak rynek handlu cyberbronią wciąż jest hermetyczny i poznanie wszystkich jego tajników graniczy z cudem. Wszelkie błędy biorę na siebie.

Głęboko wierzę, że moja praca pozwoli zajrzeć choćby przez dziurkę od klucza do tajemnego, wręcz niewidzialnego świata przemysłu cyberbroni, dzięki czemu każdy z nas, żyjący w centrum cyfrowego tsunami, będzie miał szansę zabrać głos, zanim będzie za późno.

Nicole Perlroth
listopad 2020

PROLOG

Kijów, Ukraina

Kiedy w 2019 roku w środku zimy lądowałam w Kijowie, nikt nie miał pewności, czy atak już się zakończył, czy najgorsze miało dopiero nadejść.

Gdy samolot znalazł się w przestrzeni powietrznej Ukrainy, na pokładzie dało się odczuć z trudem skrywaną panikę i wszechobecną paranoję. Samolotem miotały silne turbulencje. Z tylnej części pokładu dobiegały odgłosy walki z nudnościami. Moja sąsiadka, ukraińska modelka, chwyciła mnie z całych sił za rękę, zamknęła oczy i pogrążyła się w modlitwie.

Sto metrów pod nami Ukraina ogłosiła pomarańczowy alert. Gwałtowne wichury zrywały dachy budynków, porywając ich szczątki wprost na zatłoczone ulice miast. Wioski na obrzeżach stolicy i w zachodniej części Ukrainy ponownie pogrążyły się w ciemnościach. Jeszcze zanim samolot gwałtownie osiadł na płycie pasa startowego międzynarodowego portu lotniczego Kijów-Boryspol, żołnierze ukraińskiej straży granicznej pytali w nerwach: porywista wichura czy może kolejny rosyjski cyberatak? W tamtym czasie wszystko było możliwe.

Dzień wcześniej pożegnałam najbliższych i wyruszyłam na mroczną wyprawę do Kijowa. Pragnęłam się przekonać, co zastanę na miejscu po najpotężniejszym cyberataku w historii. Świat wciąż jeszcze nie otrząsnął się ze skutków rosyjskiego aktu cyberagresji na Ukrainę, który miał miejsce niemal dwa lata wcześniej, zakłócając działanie agencji rządowych, linii kolejowych, bankomatów, stacji benzynowych, urzędów pocztowych, a nawet monitorów promieniowania w nieczynnej elektrowni jądrowej w Czarnobylu. Opuściwszy granice Ukrainy, szkodliwy kod wyruszył na szaleńczy rajd po całym świecie – sparaliżował

działanie zakładów przemysłowych na dalekiej Tasmanii, zniszczył partie szczepionek farmaceutycznych gigantów, włamał się do komputerów firmy FedEx i w kilka minut zatrzymał w drodze tysiące kurierów najważniejszego gracza na rynku przewozu przesyłek.

Kreml perfidnie wybrał dzień ataku – ukraiński Dzień Konstytucji w roku 2017. Tego właśnie dnia, który stanowi odpowiednik amerykańskiego Dnia Niepodległości, wysłano Ukraińcom złowieszczą wiadomość. Niepodległość nie polega na świętowaniu. Matka Rosja nigdy nie zapomina o swoich dzieciach.

Atak był kulminacją serii eskalujących, perfidnych rosyjskich cyberataków przeprowadzanych w ramach zemsty za ukraińską rewolucję z 2014 roku, gdy tysiące Ukraińców zbuntowały się przeciwko dominacji Kremla. Zgromadzeni tłumnie na Placu Niepodległości w Kijowie żądali ustąpienia ze stanowiska marionetki Putina, prezydenta Wiktora Janukowycza.

W efekcie Putin udzielił obalonemu Janukowyczowi azylu, a następnie wysłał wojska na podbój Półwyspu Krymskiego, raju nad Morzem Czarnym, który jak drogocenny diament wieńczył południowe wybrzeża Ukrainy. Krymu, który Churchill ochrzcił mianem Riwiery Hadesu. Obecnie gorący półwysep znajduje się pod kontrolą Rosji jako szatański symbol putinowskich potyczek z Ukrainą.

To nie był pierwszy raz, kiedy Rosja wysyła swoją cyberarmię na wojnę z byłą republiką sowiecką. Kremlowscy hakerzy z zacięciem rozdają kuksańce na prawo i lewo za pomocą cyfrowego impulsu. Od pięciu lat przeprowadzają na Ukrainie tysiące cyberataków dziennie i nieustannie skanują tamtejsze sieci informatyczne w poszukiwaniu słabych punktów – łatwych haseł, wadliwych kodów, nielegalnego i niedopracowanego oprogramowania czy pospiesznie implementowanych zapór sieciowych. Ich celem stał się wielki cyfrowy chaos, a wszystko po to, by zasiać niezgodę i kwestionować prozachodnie przywództwo Ukrainy.

Kodeks postępowania hakerów Putina składał się z dwóch punktów. Po pierwsze zakaz działalności hakerskiej w kraju. Po drugie pełna dyspozycyjność wobec Kremla, bez względu na rodzaj zadania. Poza tym hakerzy cieszyli się szeroką autonomią, nie wspominając o przychylności wszechwładnego Putina. W rozmowie z grupą dziennikarzy w czerwcu 2017 roku Putin miał powiedzieć, że rosyjscy hakerzy są „jak artyści; budzą się rano w wyśmienitym nastroju, by stanąć przed

sztalugą, na której powstaje wielkie dzieło sztuki". Rozmowa ta odbyła się zaledwie 3 tygodnie przed rozmontowaniem systemów informatycznych Ukrainy. Rosyjski przywódca podkreślił: „Gdyby dopatrywać się pobudek patriotycznych, można wspomnieć o potrzebie walki z siłami, które atakują dobre imię Rosji".

Ukraina posłużyła Rosji jako poligon doświadczalny, wypalona ziemia, na której mogła przetestować narzędzia i triki hakerskie ze swojego cyfrowego arsenału bez obawy o odwet. Już w roku 2014, nie zwlekając, rosyjskie trolle i media storpedowały ukraińskie wybory zmasowaną kampanią dezinformacyjną, na zmianę zrzucając winę za prozachodnie powstania, na wojskową juntę lub określone siły w Ameryce i w Europie. Hakerzy uciekali się do kradzieży kampanijnej korespondencji mailowej, przenikali w struktury organów wyborczych, usuwali pliki, infekowali złośliwym oprogramowaniem krajowy system raportowania wyborów, fałszywie ogłaszając zwycięstwo niszowego, skrajnie prawicowego kandydata, co zostało wykryte przez Ukraińców tuż przed podaniem ostatecznych wyników wyborów do mediów. Eksperci uznali tę operację za najbardziej zuchwałą próbę manipulacji wyborami na szczeblu krajowym w historii.

Patrząc wstecz, wydaje się jasne, że tego rodzaju działania powinny postawić na baczność amerykańskich polityków. Jednak w roku 2014 ich uwaga koncentrowała się przede wszystkim na aktach przemocy w Ferguson w stanie Missouri, nieprzewidywalnych atakach ze strony ISIS, jak również na grudniowym ataku hakerów północnokoreańskich na Sony Pictures, czym zajmowałam się osobiście. Cyberżołnierze Kim Dzong Una dokonali w ten sposób zemsty za produkcję komedii autorstwa Setha Rogena i Jamesa Franco, której tematem był zamach na ich Słońce Narodu. Azjatyccy informatycy zaatakowali serwery wytwórni, wysyłając maile o treści upokarzającej kierownictwo Sony Pictures, dostarczając tym samym Putinowi doskonałego materiału instruktażowego.

Większość Amerykanów nie czuła żadnego związku z odległą Ukrainą. W programach informacyjnych pojawiały się wprawdzie zdjęcia osób protestujących na Placu Niepodległości i potem obywateli świętujących powołanie nowego, prozachodniego przywództwa w miejsce marionetkowego, uzależnionego od Rosji prezydenta, ale tylko nieliczni uważnie przyglądali się wydarzeniom na wschodzie Ukrainy. Szeroko

komentowano jedynie zestrzelenie przez Rosjan samolotu malezyjskich linii lotniczych z holenderskimi pasażerami na pokładzie.

Szkoda, że nie byliśmy bardziej uważni. Dostrzeglibyśmy wówczas wielkie, czerwone światło ostrzegawcze w postaci zagrożonych serwerów w Singapurze i w Holandii, przerw w dostawie energii elektrycznej, łamania kodów.

Nietrudno było zauważyć, że celem nie była Ukraina. Działa skierowano na nas.

Rosyjska ingerencja w proces wyborczy na Ukrainie to zaledwie pierwsza salwa w tej wojnie, znaczonej cyberagresją i destrukcją, jakiej świat wcześniej nie widział.

Rosjanie napisali swój podręcznik czasów zimnej wojny i nie wahają się teraz z niego korzystać. Jadąc taksówką z lotniska Boryspil do centrum Kijowa, mijałam Plac Niepodległości – krwawiące serce ukraińskiej rewolucji. Zastanawiałam się, którą stronę tego podręcznika teraz studiują i czy kiedykolwiek będziemy w stanie przewidzieć ich kolejny krok.

Istotą polityki zagranicznej Putina było podważenie kontroli Zachodu nad relacjami międzynarodowymi w wymiarze globalnym. Każdy atak hakerski, każda kampania dezinformacji prowadzona przez cyberarmię Putina miała na celu uwikłanie oponentów w konflikty wewnętrzne i tym samym odwrócenie ich uwagi od prawdziwego celu rosyjskiego przywódcy. Dla niego liczyło się osłabienie poparcia dla zachodniej demokracji, a co za tym idzie dla NATO – jedynej organizacji, która trzymała Putina w szachu.

Im bardziej Ukraińcy byli rozczarowani (tak przy okazji: gdzie podziali się ich zachodni protektorzy?), tym bardziej prawdopodobny wydawał się odwrót od wartości prodemokratycznych, prosto w lodowate objęcia Matki Rosji.

Cóż mogłoby bardziej zirytować Ukraińców i wywołać u nich większe wątpliwości co do nowego rządu niż odcięcie źródeł ciepła i prądu w środku zimy? 23 grudnia 2015 roku, zaledwie dzień przed Wigilią Bożego Narodzenia, Rosja przekroczyła cyfrowy Rubikon. Ci sami hakerzy, którzy miesiącami zastawiali pułapki i wywoływali cyfrowe eksplozje w mediach oraz instytucjach rządowych, ukradkiem mościli sobie gniazdko w krajowych elektrowniach. W grudniu włamali się

do systemów informatycznych kontrolujących sieci energetyczne i skrupulatnie wyłączali jeden obwód za drugim, pozostawiając setki tysięcy Ukraińców bez prądu. Na wszelki wypadek odcięli także telefony alarmowe, a jakby tego było mało – wyłączyli również zasilanie awaryjne centrów dystrybucyjnych na Ukrainie. W efekcie operatorzy błądzili w ciemnościach.

Przerwa w dostawie prądu nie trwała długo – niecałe sześć godzin. Jednak to, co wydarzyło się tego dnia na zachodzie kraju, nie miało dotychczas precedensu w historii. Prorocy cyberprzestrzeni oraz wyznawcy spiskowej teorii dziejów przez wiele lat ostrzegali przed cyberatakami na sieci energetyczne, jednak do 23 grudnia 2015 roku nikt nie odważył się porwać na atak na skalę całego kraju.

Putinowscy agresorzy zrobili, co w ich mocy, by ukryć swoje lokalizacje, prowadząc działania za pośrednictwem zainfekowanych serwerów ulokowanych w Singapurze, Holandii oraz w Rumunii, stosując przy tym niespotykany wcześniej poziom maskowania. Niebezpieczna broń wnikała w ukraińskie systemy w postaci niewinnie wyglądającego, drobnego oprogramowania rozbrajającego działanie detektorów zagrożeń. Randomizacja kodów pozwalała omijać zapory antywirusowe. Ukraińskie władze od początku nie miały jednak wątpliwości, kto stoi za zuchwałymi atakami. Czas i zasoby niezbędne do odpalenia ataku na sieć energetyczną o tak wysokim stopniu zaawansowania były po prostu poza zasięgiem otyłego, domorosłego hakera pracującego we własnym łóżku.

Wyłączenie prądu nie wiązało się z żadnymi korzyściami finansowymi. To było zadanie polityczne wysokiej rangi. W kolejnych miesiącach specjaliści do spraw bezpieczeństwa potwierdzili tę wersję zdarzeń. Dochodzenie doprowadziło ich do słynnej rosyjskiej jednostki wywiadowczej. Sprawa została nagłośniona. Atak miał na celu przypomnienie Ukraińcom, jak słaby jest ich rząd, jak silna jest Rosja oraz jak dalece cyfrowa armia Putina zadomowiła się w ich systemach informatycznych, że jest w stanie na każde zawołanie zgasić światło w całym kraju.

Aby rozwiać ewentualne wątpliwości, ta sama grupa rosyjskich hakerów przypomniała o sobie rok później, ponownie przerywając dostawy energii elektrycznej w grudniu 2016 roku. Tym razem jednak udało im się odciąć ogrzewanie i dopływ prądu w sercu Ukrainy – Kijowie.

Taki pokaz tupetu i zarazem wysokich kompetencji wywołał zaniepokojenie nawet amerykańskich odpowiedników rosyjskich hakerów w siedzibie Agencji Bezpieczeństwa Narodowego w Fort Meade w stanie Maryland.

Przez lata służby wywiadowcze uważały Rosję i Chiny za najpotężniejszych wrogów Stanów Zjednoczonych w cyberprzestrzeni. Wydaje się jednak, że to Chińczycy bardziej zaleźli Amerykanom za skórę, nie tyle ze względu na zaawansowane narzędzia walki, co niebywałą aktywność i kreatywność na polu kradzieży tajemnic handlowych. Dyrektor NSA (National Security Agency – amerykańska wewnętrzna agencja wywiadowcza – przyp. tłum.) Keith Alexander powiedział, że cyberszpiegostwo w wydaniu chińskim to „największy transfer bogactwa w historii". Chiny na potęgę kradły Stanom Zjednoczonym wszystko, co się dało ukraść w przestrzeni wartości intelektualnej, by następnie przekazywać je swoim przedsiębiorstwom państwowym do powielenia.

Na czele amerykańskiej listy cyberzagrożeń poczesne miejsce zajmują także Iran oraz Korea Północna, które zawsze demonstrowały wrogie nastawienie do Stanów Zjednoczonych. Iranowi przypisuje się winę za atak na internetowe strony amerykańskich banków oraz za zniszczenie komputerów Sands Casino w Las Vegas w akcie zemsty za to, że prezes zarządu spółki Sands Sheldon Adelson publicznie nakłaniał amerykańską administrację do zbombardowania Iranu. Irańscy cyberprzestępcy stoją za pojedynczymi atakami hakerskimi na szpitale, spółki, a nawet na całe miejscowości na terenie Stanów Zjednoczonych. Korea Północna infekowała amerykańskie serwery z zemsty za hollywoodzkie wycieczki pod adresem filmowych gustów Kim Dzong Una. Niedługo potem cyfrowa służba Słońca Narodu obrabowała jeden z banków w Bangladeszu na kwotę 81 milionów dolarów.

Bez wątpienia Rosja zawsze należała do światowej elity świata cyberprzestępców. Jej działania charakteryzowały się finezją i wysokim stopniem zaawansowania. Rosyjscy hakerzy zdołali włamać się do systemów Pentagonu, Białego Domu, kolegium Połączonych Szefów Sztabów oraz Departamentu Stanu, a rosyjska organizacja młodzieżowa Nasi – na bezpośredni rozkaz Kremla bądź z pobudek patriotycznych – w reakcji na zmianę lokalizacji pomnika upamiętniającego sowieckie

rządy w Estonii odcięła dopływ energii elektrycznej w całym kraju. Efektem jednego z cyberataków wycelowanych w islamskich fundamentalistów było wyłączenie 12 kanałów telewizyjnych we Francji. Rosjanie zostali też przyłapani na rozpracowywaniu systemu kontroli bezpieczeństwa spółki naftowej w Arabii Saudyjskiej, skąd tylko krok do wywołania sterowanej cyfrowo eksplozji. To oni storpedowali brytyjskie referendum w sprawie brexitu, zaatakowali sieć energetyczną USA, maczali palce w przebiegu amerykańskich wyborów w 2016 roku, starali się wpływać na wynik głosowania we Francji, a nawet na organizację samych igrzysk olimpijskich.

Jednak przez większą część 2016 roku amerykańskie służby wywiadowcze nie miały wątpliwości co do wyższości własnych możliwości w porównaniu z przeciwnikami. Kreml testował swój najbardziej zaawansowany arsenał broni cyfrowej na Ukrainie i, jak donosiły amerykańskie służby kontrwywiadowcze, jego siła rażenia nijak miała się do tego, czym dysponowały Stany Zjednoczone.

Niewykluczone, że przez pewien czas założenie to było zgodne z prawdą. Nikt nie był jednak wówczas w stanie przewidzieć, jak długo Stany Zjednoczone pozostaną hegemonem w cyberprzestrzeni. Jak się okazało, w latach 2016 i 2017 wrogo nastawione kraje na całym świecie nadrobiły zaległości. Począwszy od roku 2016 z bazy danych amerykańskiej agencji wywiadowczej NSA, gdzie biło serce cyberarmii USA, zaczęły wyciekać cenne informacje. Za przestępczymi działaniami stała tajemnicza grupa, której do dziś nie udało się zidentyfikować. Przez dziewięć miesięcy tajemniczy haker lub grupa hakerów – wciąż nie mamy pojęcia, kto uprzykrza życie NSA – funkcjonujący pod nazwą Shadow Brokers wyprowadzał z systemów NSA narzędzia hakerskie oraz kody krajów, cyberprzestępców lub terrorystów w celu wykorzystania ich na użytek własnych podbojów cyberprzestrzeni.

Wycieki danych przypisywane Shadow Brokers trafiały na pierwsze strony gazet, jednak jak większość informacji publikowanych w latach 2016–2017 nie utkwiły one na długo w amerykańskiej świadomości. Społeczne wyobrażenie o tym, co się wówczas dokonywało, było – delikatnie mówiąc – nieadekwatne do powagi sytuacji. Obywatele nie mieli pojęcia, w jakim stopniu już wkrótce mogą ucierpieć NSA, nasi sojusznicy, największe amerykańskie korporacje, jak również maleńkie miasteczka czy ogromne metropolie.

Za sprawą Shadow Brokers na światło dzienne wyciekły informacje dotyczące najpotężniejszej i najbardziej niewidocznej cyberarmii świata. Tajemniczym hakerom udało się obnażyć program rządowy zakrojony na niespotykaną wcześniej skalę, ujawnić cyberbroń i działania szpiegowskie skrywane tak pieczołowicie, że próżno by szukać wzmianki na ich temat w jakiejkolwiek dokumentacji. Tajne operacje prowadzone były pod przykrywką fasadowych korporacji, specjalnie w tym celu zatrudnianych pracowników, czarnych budżetów, umów o zachowaniu poufności oraz, we wczesnym okresie, za pomocą gigantycznych walizek wypchanych po brzegi gotówką.

Gdy Shadow Brokers rozpoczynali stopniowe wyprowadzanie z NSA informacji na temat cyberarsenału USA, ja już od czterech lat zajmowałam się rozpracowywaniem programu ofensywy amerykańskiej i udało mi się dotrzeć do dokumentów ujawnionych przez Edwarda J. Snowdena, byłego zleceniobiorcę NSA. Prześledziłam trzydziestoletnią historię programu. Miałam okazję spotkać ojca chrzestnego całego przedsięwzięcia. Poznałam zaangażowanych w projekt hakerów, dostawców i wynajętych pracowników. Nawiązałam bliskie kontakty z naśladowcami amerykańskich cyberwojowników na całym świecie. Z czasem poznałam historie mężczyzn i kobiet, których życie w wyniku przeprowadzonych cyberataków legło w gruzach.

Jedyne, czego nie udało mi się zaobserwować z bliska, to skutków przejęcia cybernarzędzi NSA przez siły wroga.

Nic dziwnego więc, że w marcu 2019 roku pojawiłam się na Ukrainie, by na własne oczy zobaczyć wojenne zgliszcza.

Rosyjskie ataki na ukraińską sieć energetyczną zapoczątkowały nowy rozdział w historii cyberwojen. Jednak nawet te przeprowadzone w 2015 roku nie mogły się równać z wydarzeniami, które miały miejsce dwa lata później, gdy Rosja weszła w posiadanie najpilniej strzeżonych narzędzi hakerskich NSA.

27 czerwca 2017 roku Kreml odpalił cyberbroń NSA na Ukrainie, co okazało się najbardziej destrukcyjnym i kosztownym cyberatakiem w historii świata. Tego popołudnia zgasły ekrany wszystkich urządzeń na terenie kraju. Ukraińcy nie mogli pobrać gotówki z bankomatu, zapłacić za paliwo na stacji benzynowej, wysłać lub odebrać maila, kupić biletu na pociąg, zrobić zakupów spożywczych, odebrać włas-

nego wynagrodzenia oraz, co najgorsze, monitorować poziomu promieniowania radioaktywnego w elektrowni w Czarnobylu. Konsekwencje ataku odczuwalne były także poza granicami Ukrainy.

Ucierpiały firmy prowadzące działalność na terenie tej byłej radzieckiej republiki. Każdy ukraiński pracownik międzynarodowej organizacji stanowił furtkę do sieci globalnej. Zaatakowano komputery spółek farmaceutycznych Pfizera oraz Mercka, gigantów na rynku przewozów i dostaw, czyli firm Maersk oraz FedEx, jak również producenta wyrobów czekoladowych Cadbury w jego fabrykach zlokalizowanych na Tasmanii. Fala ataków uderzyła rykoszetem w samą Rosję, gdzie ucierpiały bazy danych potentata naftowego Evraz oraz producenta stali będącego własnością dwóch rosyjskich oligarchów. Za pomocą wykradzionego z NSA kodu Rosjanie przypuścili więc atak rozsiewający złośliwe oprogramowanie na całym świecie. Atak, który tylko Mercka i FedEx kosztował miliard dolarów.

W czasie mojej wizyty w Kijowie w roku 2019 Ukraińcy wciąż jeszcze liczyli straty. W tym momencie szacowano je na ponad 10 miliardów dolarów. System dostaw i komunikacja kolejowa nie wróciły do pełnej sprawności. Na terenie całego kraju trwały poszukiwania przesyłek zaginionych w czasie załamania systemu. Do dziś nie wypłacono świadczeń emerytalnych wstrzymanych w efekcie ataku, podczas którego uległy zniszczeniu bazy danych osób uprawnionych.

Specjaliści z dziedziny bezpieczeństwa nadali tej napaści niefortunną nazwę: NotPetya. Początkowo winę za atak przypisano działaniu oprogramowania typu ransomware o nazwie Petya, wykorzystywanego do wyłudzania okupu, jednak z czasem stało się jasne, że Rosjanie celowo stworzyli oprogramowanie na wzór przeciętnego programu szantażującego. Nawet po wpłaceniu okupu istniały zerowe szanse na odzyskanie jakichkolwiek danych. Atak okazał się odpaloną w całym kraju cyfrową bronią masowego rażenia.

Na Ukrainie spędziłam następne dwa tygodnie smagana lodowatymi podmuchami wiatru z Syberii. Rozmawiałam z dziennikarzami. Stałam na Placu Niepodległości ramię w ramię z mieszkańcami protestującymi w celu upamiętnienia rewolucyjnych wydarzeń znaczonych rozlewem krwi. Penetrowałam zakamarki strefy przemysłowej, gdzie cyfrowi detektywi pokazali mi rumowisko, jakie pozostawił po sobie NotPetya. Spotkałam ukraińską rodzinę właścicieli firmy dostarczającej

każdej znaczącej organizacji i spółce oprogramowanie do rozliczania podatków. To oni odegrali dla hakerów rolę Pacjenta Zero. Rosjanie sprytnie rozesłali złośliwe oprogramowanie pod postacią uaktualnienia programu służącego do rozliczeń podatkowych. Po fakcie pracownicy firmy nie wiedzieli, czy śmiać się, czy płakać nad tym, jaką rolę odegrali w ogólnokrajowej cyberwojnie. Odbyłam rozmowy z szefem ukraińskiej policji ds. cyberprzestępczości oraz z każdym ministrem ukraińskiego rządu, który wyraził wolę spotkania się ze mną.

Odwiedziłam amerykańskich dyplomatów w ambasadzie USA tuż przed tym, jak zostali uwikłani w proces impeachmentu prezydenta Donalda Trumpa. W dniu, w którym złożyłam im wizytę, pracownicy placówki borykali się z problemem najnowszej rosyjskiej kampanii dezinformacyjnej – kremlowskie trolle zaatakowały na Facebooku strony chętnie odwiedzane przez młode ukraińskie matki, siejąc antyszczepionkową propagandę. Działo się to w czasie, kiedy kraj zmagał się z najgorszą we współczesnej historii epidemią odry. Ukraina wykazywała jeden z najniższych wskaźników szczepień na świecie, a Kreml skutecznie wykorzystywał panujący chaos. Gdy choroba zaczęła się pojawiać w USA, trolle Putina już były gotowe, by bombardować Amerykanów antyszczepionkowymi memami, na oczach bezradnych instytucji państwowych. Podobną niemocą urzędnicy wykazali się zresztą rok później, gdy Rosjanie rozpętali burzę propagandową wokół pandemii, szerząc teorie spiskowe na temat Covid-19. Jedna z nich wskazywała, że koronawirus to wyprodukowana w amerykańskich laboratoriach broń biologiczna, inna oskarżała Billa Gatesa o wywołanie kryzysu i zarabianie kolejnych miliardów na szczepionkach. Rosja wydawała się iść na całość, dzieląc i przejmując kontrolę nad chaosem.

Jednak zimą 2019 roku wszyscy byli zgodni co do tego, że akcja NotPetya to najbardziej zuchwały ze wszystkich dotychczasowych ataków Kremla. Nie spotkałam w Kijowie ani jednego mieszkańca, który pozostawałby obojętny wobec ataku. Każdy dokładnie pamiętał, gdzie się wówczas znajdował i co robił w momencie, gdy zgasły ekrany komputerów. Nazwali go Czarnobylem XXI wieku. Tymczasem w dawnej elektrowni atomowej, oddalonej o około 150 kilometrów na północ od Kijowa, komputery stały się „czarne, czarne, czarne" – wspominał Siergiej Gonczarow, gburowaty kierownik techniczny elektrowni w Czarnobylu.

Gonczarow wracał z przerwy na lunch, gdy zegar wskazał 13.12, i właśnie w tym momencie, zaledwie w ciągu 7 minut, zgasły ekrany 25 komputerów. Rozdzwoniły się telefony, wszystko przestało działać. Podczas gdy Gonczarow usiłował przywrócić działanie czarnobylskiej sieci, uzyskał informację, że komputery monitorujące poziom promieniowania w miejscu, w którym ponad trzy dekady wcześniej doszło do wybuchu, również przestały działać. Nikt nie miał pojęcia, czy promieniowanie pozostało na bezpiecznym poziomie, czy i tu mieliśmy do czynienia z aktem sabotażu.

„W tym momencie byliśmy całkowicie pochłonięci przywracaniem sprawności naszych komputerów, nie zaprzątaliśmy więc sobie głowy tym, co jest źródłem zamieszania" – powiedział mi Gonczarow. „Kiedy jednak tylko nieco ochłonęliśmy z pierwszego szoku i dostrzegliśmy tempo, w jakim rozprzestrzenia się wirus, stało się jasne, że padliśmy ofiarą poważnego, zmasowanego ataku".

Gonczarow chwycił megafon i nakazał każdemu, kto go słyszy, wyjąć wtyczkę komputera z gniazdka. Pozostałych poprosił, aby wyszli na zewnątrz i rozpoczęli ręczne monitorowanie poziomu promieniowania nad Strefą Wykluczenia.

Trudno nazwać Gonczarowa człowiekiem wylewnym. Nawet teraz, gdy opisywał najgorszy dzień swojego życia, jego głos wydawał się monotonny, jak zawsze. Rzadko targały nim silne emocje, jednak – jak mi powiedział – w dniu ataku NotPetya „przeżyłem prawdziwy szok". Dwa lata później trudno mi było stwierdzić, czy doszedł już do siebie.

„Nastały zupełnie nowe czasy" – powiedział. „Istnieje wyłącznie świat przed atakiem NotPetya i po nim".

Gdziekolwiek w ciągu tych dwóch tygodni pojechałam, wszędzie dało się odczuć to samo. Na przystanku autobusowym wysłuchałam opowieści mężczyzny, któremu odmówiono sprzedaży używanego samochodu. Czy to wyjątek na rynku pojazdów? Po zatrzymaniu systemu rejestracji – nie. W kawiarni spotkałam kobietę, którą atak pozbawił środków do życia. Jej niewielki internetowy sklep z artykułami dziewiarskimi zbankrutował, po tym jak w systemie poczty zniknęły wszystkie przesyłki. Zewsząd słychać opowieści, że ktoś borykał się z brakiem gotówki bądź utknął na drodze z pustym bakiem. W opowieściach, podobnie jak u Gonczarowa, przewija się motyw oszałamiającej szybkości, z jaką wyłączały się kolejne urządzenia.

Biorąc pod uwagę moment ataku – wigilię Dnia Niepodległości Ukrainy – mało kto miał wątpliwości. Znów przebudziła się ta stara, zgorzkniała diablica – Matka Rosja. Jednak Ukraińcy to naród twardych ludzi, od ponad dwudziestu siedmiu lat znaczonych tragedią i kolejnymi kryzysami. Gdy rzeczywistość okazuje się trudna do zniesienia, na ratunek przychodzi czarny humor. Niektórzy żartowali, że wyłączając wszystkie urządzenia Wowa, jak nazywają Putina, podarował im kilka dodatkowych Dni Niepodległości. Inni z zadowoleniem chwalili się, że dzięki atakowi po raz pierwszy od wielu lat zrobili sobie urlop od Facebooka.

Pomimo traumy i strat natury finansowej, jakie przyniosły czerwcowe wydarzenia w 2017 roku, Ukraińcy pocieszają się, że sprawy mogły potoczyć się o wiele gorzej. To prawda, systemy obsługi klienta uległy poważnym uszkodzeniom i bezpowrotnie przepadły liczne ważne dane. Niemniej jednak zamach nie wywołał awarii tak poważnej, by doprowadzić do katastrofy lotniczej lub poważnej eksplozji zakończonej śmiercią wielu osób. Poza awarią systemu monitorującego poziom napromieniowania w Czarnobylu wszystkie pozostałe elektrownie jądrowe na Ukrainie zachowały pełną zdolność operacyjną.

Podsumowując, na razie Rosja zadała jedynie kilka ciosów. Podobnie jak w przypadku wcześniejszego ataku na sieci energetyczne, gdy światła zgasły na wystarczająco długo, by wysłać ostrzeżenie, Rosja mogła posunąć się znacznie dalej, biorąc pod uwagę stopień rozpracowania ukraińskich systemów oraz arsenał skradzionej amerykańskiej broni, którą miała do dyspozycji.

Istnieje teoria, że Rosjanie za pomocą ataku na Ukrainę przy użyciu wykradzionych narzędzi chcieli jedynie zagrać na nosie NSA. Ukraińscy eksperci do spraw bezpieczeństwa wskazują na alternatywną, daleko bardziej niepokojącą koncepcję – ich zdaniem zarówno atak NotPetya, jak i zamach na sieć energetyczną należy traktować jako próbę generalną.

To właśnie powiedział mi pewnego wieczoru Oleh Derevianko, blondwłosy ukraiński przedsiębiorca z branży cyberbezpieczeństwa, gdy wspólnie biesiadowaliśmy, zajadając wareniki (gotowane pierogi nadziewane na słodko lub ostro) i chołodeć (mięsną galaretę). W czasie opisywanych ataków firma mojego rozmówcy znalazła się na pierwszej linii frontu. Eksperci kryminalistyki raz po raz wykazywali, że

Rosjanie przeprowadzali wyłącznie eksperymenty. Urzeczywistniali scenariusz stosowany w badaniach naukowych: testowali konkretną metodę, a po niej kolejną. Doskonalili własne umiejętności na Ukrainie i zarazem walczyli o uznanie rosyjskich mocodawców, demonstrując wachlarz swoich możliwości.

Derevianko wyjaśnił mi, dlaczego atak NotPetya miał tak daleko idące konsekwencje w postaci wyczyszczenia zawartości 80% ukraińskich komputerów. „Oni po prostu zacierali ślady. To nowy arsenał i nowy rodzaj wojny, a Ukrainę należy traktować jak rosyjski poligon. Jaki użytek zamierzają zrobić z tej broni? Nie mam pojęcia".

Przez dwa lata na Ukrainie nie odnotowano cyberataku na tak wielką skalę i choć pojawiały się doniesienia o planowanej w ciągu najbliższych dwóch tygodni ingerencji Kremla w wybory 2019 roku, fala cyberdestrukcji wyraźnie osłabła.

„To oznacza, że zrobili krok naprzód" – stwierdził Derevianko.

W milczeniu spałaszowaliśmy naszą galaretę, zapłaciliśmy rachunek i opuściliśmy restaurację. Po raz pierwszy miałam wrażenie, że gwałtowne wichury nieco ucichły. Jednak zwykle tętniące życiem, brukowane ulice starego Kijowa wciąż były puste. Odwiedziliśmy słynny Zjazd św. Andrzeja. To kijowski odpowiednik paryskiego Montmartre'u – stroma, brukowana uliczka, która wije się wśród galerii sztuki, antykwariatów i pracowni artystycznych w kierunku lśniącej bielą, błękitem i złotem cerkwi św. Andrzeja, pierwotnie zaprojektowanej w 1700 roku jako letnia rezydencja carycy Elżbiety.

Gdy dotarliśmy do świątyni, Derevianko zatrzymał się i uniósł głowę, spoglądając na żółtą poświatę latarni.

„Wiesz, my tutaj poradzimy sobie bez prądu przez kilka godzin" – powiedział. „Jednak jeśli coś takiego wydarzy się w twoim kraju...".

Zawiesił głos. Nie musiał kończyć. Słyszałam to już wiele razy, zarówno na Ukrainie, jak i z ust moich informatorów w Stanach Zjednoczonych.

Nikt z nas nie miał wątpliwości, jaki będzie ich kolejny krok.

To, co ocaliło Ukrainę, jednocześnie uczyniło Stany Zjednoczone najbardziej bezbronnym państwem świata.

Ta była republika radziecka pozostawała daleko w tyle w wyścigu technologicznym i jeszcze nie wszystko zostało tu podłączone do internetu. Tsunami o nazwie internet rzeczy, które całkowicie pochłonęło społeczeństwo amerykańskie w minionej dekadzie, wciąż jeszcze nie dotarło do Ukrainy. Tutejsze elektrownie jądrowe, szpitale, zakłady chemiczne, rafinerie, gazociągi oraz rurociągi naftowe, fabryki, gospodarstwa rolne, miasta, samochody, sygnalizacja świetlna, domostwa, termostaty, żarówki, lodówki, kuchenki, elektroniczne nianie, rozruszniki serca i pompy insulinowe funkcjonowały poza internetem.

W Stanach Zjednoczonych najważniejsza była i jest wygoda. Obecnie ma się ona nadzwyczaj dobrze. Amerykanie podłączają do sieci wszystko, co się da, z prędkością 127 urządzeń na sekundę. Dolina Krzemowa obiecała nam łatwe życie, a my jej uwierzyliśmy. Sieć oplata bez wyjątku każdą dziedzinę życia. Za pomocą internetu możemy zdalnie kontrolować naszą codzienność, gospodarkę oraz sieć energetyczną. Nie przyszło nam do głowy, by przez chwilę zastanowić się, że w coraz większym stopniu wystawiamy się na zmasowany atak wroga.

W NSA, której zadaniem jest zarówno koordynacja globalnych działań wywiadowczych, jak i ochrona tajemnic amerykańskich instytucji, już dawno zapomniano, że ofensywny wojownik potrafi również skutecznie się bronić. Na stu atakujących cyberżołnierzy przypadał jeden osamotniony analityk oddelegowany do działań defensywnych. Amerykański wywiad nigdy wcześniej nie ucierpiał tak bardzo, jak za sprawą przecieków Shadow Brokers. Snowden obnażył naturę amerykańskiego wywiadu, Shadow Brokers dostarczyli wrogom USA konkretną amunicję – kody.

Największą tajemnicą cyberwojny jest fakt – doskonale teraz znany każdemu naszemu przeciwnikowi – że kraj będący w posiadaniu najpotężniejszego na świecie arsenału cyberamunicji jednocześnie jest najbardziej narażony na ewentualne ataki.

Ukraina miała jeszcze jedną przewagę nad USA: świadomość konieczności pilnego działania. Po pięciu latach odpierania ataków ze strony jednego z najpotężniejszych drapieżników świata Ukraińcy nie mieli wątpliwości, że ich być albo nie być zależy od zbudowania potężnych mechanizmów obronnych w cyberprzestrzeni. NotPetya z wielu względów stanowił dla Ukrainy nowy początek; dał szansę na zbudowanie od podstaw nowych procedur i odseparowanie krytycz-

nych systemów państwa od internetu. Kilka tygodni po moim wyjeździe Ukraińcy przeprowadzili wybory prezydenckie wyłącznie w formie tradycyjnej, oddając swe głosy na papierowych kartach w lokalach wyborczych. Bez wyszukanych maszyn do głosowania; każda kartka wyborcza została wypełniona osobiście przez głosującego. Głosy przeliczono ręcznie. Naturalnie, jak zawsze, w całym kraju pojawiły się spekulacje na temat kupowania głosów. Jedno jest natomiast pewne: pomysł przeniesienia Ukraińskich wyborów do internetu dla każdego wydawał się czystym szaleństwem.

Nie pierwszy raz Stany Zjednoczone nie zdołały wyciągnąć z takiej lekcji wniosków dla siebie. Umknęło nam, że potencjalne działania wojenne przeniosły się z ziemi, z morza i z powietrza do cyberprzestrzeni. Kilka miesięcy po moim wyjeździe z Ukrainy okazało się, że to nie rosyjskie ataki na Ukrainie zapadły Amerykanom w pamięć, ale znaczenie tego kraju dla procesu impeachmentu Donalda Trumpa. Jak krótką trzeba mieć pamięć, by zapomnieć, że rosyjskie cyberataki nie skończyły się na kampanii dezinformacji w roku 2016, na wycieku korespondencji mailowej demokratów i wywoływaniu chaosu poprzez podszywanie się pod teksańskich secesjonistów czy aktywistów ruchu Black Lives Matter. Rosjanie sondowali systemy zaplecza wyborów oraz bazy danych wyborców we wszystkich pięćdziesięciu stanach. Być może nie udało im się zhakować ostatecznych wyników głosowania, jednak zdaniem przedstawicieli władz USA wszelkie dotychczasowe działania stanowią trening przed ostatecznym atakiem na amerykańskie wybory w przyszłości.

Donald Trump winą za rosyjską ingerencję w wybory w 2016 roku nieustająco obarczał przypadkowego grubasa, który, nie opuszczając własnego łóżka, infekuje państwowe systemy informatyczne, oraz Chiny. Stojąc w 2018 roku obok rozradowanego Władimira Putina na konferencji prasowej w Helsinkach, Donald Trump nie tylko z lekceważeniem wyrażał się o funkcjonariuszach amerykańskiego wywiadu: „Prezydent Putin zapewnił mnie, że Rosja nie ma z tym nic wspólnego. Przyznam, że i ja nie widzę powodu, by szukać tu winnych". Co więcej, przyjął ofertę Putina, by połączyć siły w ściganiu sprawców zamieszania wokół wyborów 2016 roku. Gdy zbliżały się kolejne wybory, Putin i Trump spotkali się raz jeszcze, tym razem w czerwcu 2019 roku w Osace, gdzie ramię w ramię żartowali jak starzy kumple ze studiów.

Na pytanie dziennikarza, czy ostrzegł Putina, by nie mieszał się do amerykańskich wyborów 2020 roku, Trump z szyderczym uśmieszkiem zwrócił się w stronę rosyjskiego kolegi i, grożąc palcem, oznajmił: „Proszę nie wtrącać się w nasze wybory, panie Prezydencie".

Oto w jakim miejscu znajdujemy się obecnie. Gdy piszę tę książkę, wybory w 2020 roku są nadal przedmiotem sporu, zagraniczni gracze podsycają w kraju atmosferę wewnętrznego chaosu, borykamy się z problemem wycieków z arsenału cyberbroni USA. Rosyjscy hakerzy buszują w naszych szpitalach, agenci Kremla rozpanoszyli się na dobre w amerykańskiej sieci, a zdeterminowani agresorzy każdego dnia przypuszczają miliony ataków na nasze sieci informatyczne. Dodatkowo pandemia przeniosła życie amerykańskiego społeczeństwa jeszcze głębiej w świat internetu. Stoimy bezradni w obliczu naszego cyfrowego Pearl Harbor, przed którym od siedmiu lat ostrzegają mnie eksperci do spraw bezpieczeństwa.

W Kijowie przypominano mi o tym na każdym kroku. Miałam wrażenie, że ledwo powstrzymywali się, by wykrzyknąć mi prosto w twarz: „Teraz wasza kolej!". Światła ostrzegawcze raz jeszcze błysnęły na czerwono. Ostatnie doświadczenia niczego nas nie nauczyły.

Staliśmy się jedynie daleko bardziej narażeni na ataki. Co gorsza, wycelowano w nas działa naszej własnej produkcji. Mówili mi to Ukraińcy. Na pewno wiedzieli o tym nasi wrogowie. Hakerzy nigdy nie mieli wątpliwości.

Oto ich opowieść o końcu świata.

Nowe technologie / Biznes

To najlepsza książka biznesowa roku 2021 według „Financial Times" i McKinsey. To thriller i zarazem przewodnik po zakamarkach cyberprzestrzeni. Prezentuje bogatą galerię szpiegów, hakerów, handlarzy bronią, naukowców, polityków i ludzi biznesu. Pokazuje kulisy działania NSA, GRU czy Mosadu. Wiele miejsca zajmuje w książce cyberbezpieczeństwo w odniesieniu do biznesu i ogromnych strat ponoszonych przez firmy, zwłaszcza banki, na skutek cyberataków.

Reporterka „New York Timesa", Nicole Perlroth, opierając się na wieloletnich relacjach i setkach wywiadów, pozwala zajrzeć przez dziurkę od klucza do tajemnego, wręcz niewidzialnego świata przemysłu cyberbroni, dzięki czemu każdy z nas, żyjący w centrum cyfrowego tsunami, będzie miał szansę zabrać głos, zanim będzie za późno.

Reportaż najwyższej próby... Pasjonująca podróż od pierwszej do ostatniej strony, a zarazem pilne wezwanie do działania, zanim nasz podłączony do sieci świat wymknie się spod kontroli. Zajmuję się cyberbezpieczeństwem od dekady, a mimo to, akapit po akapicie, nie dawało mi spokoju jedno pytanie: W jaki sposób udało jej się na to wpaść? Zastanawiałem się, jak można być aż tak dobrym.

GARRETT M. GRAFF
„Wired", autor bestsellerowej książki „New York Timesa" *Jedyny samolot na niebie*

Porywająca opowieść o tym, jak twórcy groźnej broni cyfrowej stali się jej celem. Perlroth podejmuje złożony temat, dotychczas ukryty za techniczną nomenklaturą, i wyraźnie pokazuje, jak bardzo dotyczy on każdego z nas.

KARA SWISHER
gospodyni serwisu podcastowego „New York Timesa" o nazwie *Sway*

Misterna, szczegółowa, oparta na głębokich źródłach i raportach historia początków i rozwoju rynku [cyberbroni] oraz rozpętanego przezeń globalnego wyścigu cyberzbrojeń. To nie sucha, oparta na faktach kronika zdarzeń. Perlroth oferuje czytelnikowi prozę rodem ze szpiegowskiego thrillera, od samego początku próbując wyrwać nas ze strefy komfortu i samozadowolenia.

JONATHAN TEPPERMAN
recenzja dla „New York Timesa"

Książka dostępna także jako **e-book**.

Patroni:

THINKTANK BRIEF MY COMPANY POLSKA

ISBN: 978-83-8231-111-2

MT21054
Cena 79,90 zł

www.mtbiznes.pl