DAVID E. SANGER

CYBERBROŃ BROŃ DOSKONAŁA

WOJNY, AKTY TERRORYZMU I ZARZĄDZANIE STRACHEM W EPOCE KOMPUTERÓW

password

Helion

Tytuł oryginału: The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age

Tłumaczenie: Tomasz F. Misiorek

ISBN: 978-83-283-7152-1

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/cyberb
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

SPIS TREŚCI

PROLOG

POZDROWIENIA Z ROSJI

GDY DZIEŃ PRZED WIGILIĄ 2015 R. ZGASŁY ŚWIATŁA w zachodniej Ukrainie, Andy Ozment czuł ogarniający go niepokój.

Wielkie ekrany w pokoju narad, do którego wchodziło się z tego samego korytarza co do jego biura, mieszczącego się w nieoznaczonym budynku Departamentu Bezpieczeństwa Wewnętrznego oddzielonego od Białego Domu zaledwie szerokością rzeki Potomac, wskazywały, że nagłe zaciemnienie na odległych krańcach pogrążonej w wojnie byłej radzieckiej republiki spowodowane zostało przez coś groźniejszego niż zimowa burza albo uszkodzona podstacja sieci energetycznej. Zdarzenie to nosiło wszelkie oznaki złożonego cyberataku, przeprowadzonego z miejsca znajdującego się daleko od Ukrainy.

Minęły niecałe dwa lata od czasu, gdy Władimir Władimirowicz Putin zaanektował Krym i ogłosił, że na powrót staje się on częścią Matki Rosji. Czołgi i żołnierze Putina — którzy zamienili mundury na cywilne ubrania i stali się znani jako „małe zielone ludziki" — siali chaos w rosyjskojęzycznych południowo-wschodnich częściach Ukrainy i robili wszystko co w ich mocy, by zdestabilizować nowy prozachodni rząd w Kijowie, stolicy kraju.

Ozment wiedział, że ta chwila, środek okresu świątecznego na Ukrainie, to idealny moment na rosyjski cyberatak daleko od stref walki. Obsada pracująca u dostarczycieli energii ograniczała się do pracowników niezbędnych do utrzymania działania sieci. Dla sekretnej armii Putina złożonej z hakerów-patriotów Ukraina była poligonem doświadczalnym i placem zabaw[1]. To, co się tam stało, jak Ozment powtarzał swoim podwładnym, było preludium do tego, co mogło

stać się w Stanach Zjednoczonych. Jak im często przypominał, w świecie cyberkonfliktu atakujący występowali w pięciu różnych odmianach: „wandali, włamywaczy, zbirów, szpiegów i sabotażystów".

„Nie przejmuję się zbirami, wandalami i włamywaczami" — dodawał szybko. Do firm i odpowiednich agencji rządowych należało pilnowanie wrażliwych obszarów przed zwyczajnymi ciemnymi typkami internetu. Na spokojny sen nie pozwalali mu natomiast szpiedzy, a w szczególności sabotażyści. A sabotażyści, którzy w 2015 r. uderzyli w sieć energetyczną Ukrainy, nie byli amatorami. „To atakujący trzyma w ręku wszystkie atuty" — ostrzegał Ozment. Putin na Ukrainie pokazywał to nader wyraźnie.

Ozment, brodaty informatyk ok. czterdziestki, zdawał się celowo podtrzymywać wrażenie, że odkąd skończył uniwersytet Georgia Tech, nie minęło tak wiele czasu i wolałby wędrować po górach, niż zmagać się ze złośliwym oprogramowaniem. Mieszkał ze swoją norweską żoną w piętrowym domu z cegły w hipsterskiej dzielnicy Waszyngtonu na północ od Kapitolu. Zawsze udawało mu się wyglądać tak, jakby dopiero co wyszedł z jednego z licznych weekendowych targów w swojej okolicy, a nie zszedł z linii frontu cyberwojny toczonej dzień w dzień przez Amerykę. Była to nie lada sztuka, wziąwszy pod uwagę, że dowodził czymś, co w USA było najbliższe zespołowi szybkiego reagowania na cyberataki. Jego zespół w Arlington włączał się do działania jako pierwszy, gdy atakowano banki lub firmy ubezpieczeniowe, zakłady użyteczności publicznej znajdowały wirusy w swoich sieciach i podejrzewały celowe wrogie działania albo niekompetentne agencje federalne (jak Biuro Zarządzania Personelem) odkrywały, że chińscy szpiedzy wykradli miliony ściśle tajnych plików zawierających dane osób starających się o dostęp do poufnych materiałów. Innymi słowy: zespół Ozmenta był cały czas na nogach, jak straż pożarna w okolicy nawiedzanej przez podpalaczy.

Pokój narad Ozmenta — w języku biurokratycznym „Krajowe Centrum Cyberbezpieczeństwa i Komunikacji" — wyglądał jak ze scenografii hollywoodzkiego filmu. Ekrany ciągnęły się na ponad 30 metrów, pokazując wszystko, od ruchu w internecie po działanie elektrowni jądrowych. Przelatywały przez nie paski informacyjne z nowymi danymi. Przy biurkach znajdujących się naprzeciwko ekranów siedzieli przedstawiciele różnych trzyliterowych agencji rządu Stanów Zjednoczonych: FBI, CIA, NSA i DoE (ang. *Department of Energy*).

Na pierwszy rzut oka pokój przypominał podziemny bunkier, który poprzednie pokolenie Amerykanów utrzymywało w gotowości wewnątrz góry w pobliżu

Colorado Springs. Jednak pierwsze wrażenie było mylące. Mężczyźni i kobiety, którzy spędzali zimną wojnę wpatrzeni w wielkie ekrany w Kolorado, wypatrywali czegoś, co było trudne do przeoczenia: sygnału, że rakiety z głowicami nuklearnymi wystartowały w stronę amerykańskich miast i baz atomowych. Jeśli dostrzeli odpalenie pocisków — a było wiele fałszywych alarmów — wiedzieli, że mają tylko minuty na potwierdzenie tego, że USA stały się celem ataku, i ostrzeżenie prezydenta, którego obowiązkiem było zdecydowanie, czy przed dotarciem rakiet do celu przeprowadzić uderzenie odwetowe. Te jasne procedury stanowiły szkielet systemu odstraszania.

Na ekranach Ozmenta natomiast widniał dowód, że w epoce cyfrowej odstraszanie kończy się na klawiaturze. Chaos współczesnego internetu rozlewał się na ekran po ekranie, najczęściej w postaci niezrozumiałej mieszaniny znaków. Pojawiały się niewinne przerwy w działaniu usług i zuchwałe ataki, ale zorientowanie się, skąd pochodzi atak, było prawie niemożliwe. Oszukiwanie systemów przychodziło hakerom w sposób naturalny, a maskowanie ich lokalizacji nie było trudne. Nawet w przypadku dużych ataków mogły minąć tygodnie, a nawet miesiące, zanim amerykańskie agencje wywiadowcze „przypiszą" komuś wrogie działanie, a i wtedy mogło nie być żadnej pewności, że atakujący zostali prawidłowo zidentyfikowani. Krótko mówiąc: zupełnie nie przypominało to okresu zimnej wojny. Analitycy mogli ostrzegać prezydenta o tym, co się dzieje (i zespół Ozmenta robił to często), ale nie byli w stanie uściślić na bieżąco i bez wątpliwości, skąd nadszedł atak lub komu należałoby odpowiedzieć.

Im więcej pojawiało się danych o tym, co działo się tego zimowego dnia na Ukrainie, tym bardziej żołądek Ozmenta skręcał się w supeł. „To był ten rodzaj koszmaru, o którym rozmawialiśmy i staraliśmy się ostrzegać od lat" — wspominał później szef zespołu. Był to tydzień świąteczny, oznaczający rzadką przerwę w codziennym korowodzie kryzysów, i Ozment miał kilka minut na obejrzenie przerażającego nagrania z telefonu komórkowego, przekazywanego sobie wzajemnie przez współpracowników. Filmik został nagrany podczas ataku na Ukrainie na jednego z dostawców energii, Kyivoblenergo, i idealnie ukazywał zdziwienie i chaos wśród operatorów sieci elektrycznej, gdy gorączkowo próbowali odzyskać kontrolę nad swoim systemem komputerowym.

Jak widać było na nagraniu, byli całkowicie bezradni. Nic, co naciskali, nie przynosiło żadnego efektu. Wyglądało to tak, jakby ich klawiatury i myszki zostały odłączone, a nad komputerami władze przejęły nadnaturalne siły. Kursory skakały po ekranach w głównym centrum zarządzania na Ukrainie kierowane

niewidzialną ręką. Atakujący zdalnie systematycznie odcinali obwody, usuwali kopie zapasowe i wyłączali podstacje. Dzielnica po dzielnicy światła gasły. „To było dla nas kompletnym szokiem — wspominał Ozment. — Scenariusz, który spędzał nam sen z powiek, nie był wytworem naszej paranoi. Rozgrywał się przed naszymi oczami".

Nie było to wszystko, co zaplanowali hakerzy. Wprowadzili do systemów tani program — szkodliwe oprogramowanie o nazwie KillDisk — by usunąć zabezpieczenia awaryjne, które pozwoliłyby operatorom na odzyskanie kontroli. Wreszcie zadali ostateczny cios: odłączyli zasilanie awaryjne w dyspozytorni, tak że operatorzy siedzieli nie dość że bezradni, to jeszcze w całkowitej ciemności[2]. Wszyscy pracownicy Kyivoblenergo mogli tylko siedzieć i kląć pod nosem.

Przez dwie dekady (od czasu, zanim jeszcze Ozment rozpoczął swoją karierę w cyberobronie) specjaliści ostrzegali, że hakerzy mogą wyłączyć krajową sieć elektryczną jako pierwszy krok do wyłączenia całego kraju. I przez większą część tego czasu każdy wydawał się pewien, że gdy przyjdzie wielkie uderzenie, wyłączą prąd od Bostonu po Waszyngton albo od San Francisco po Los Angeles. „Baliśmy się tego panicznie przez 20 lat, ale nigdy do tego nie doszło" — wspominał Ozment.

„Aż do teraz".

. . .

DOSZŁO DO TEGO, ALE W O WIELE WIĘKSZEJ SKALI, na sposoby, których Ozment nie potrafił przewidzieć.

Gdy Ozment próbował zrozumieć implikacje cyberataku, do którego dochodziło na drugim końcu świata, czyli na Ukrainie, Rosjanie prowadzili już potrójny atak tuż pod jego nosem. Pierwsza faza obrała za cel amerykańskie elektrownie jądrowe, jak również systemy dystrybucji wody i elektryczności, a polegała na zakażeniu ich złośliwym kodem dającym Rosji możliwość sabotowania zakładów lub wyłączenia ich na życzenie[3]. Druga skupiała się na Krajowym Komitecie Partii Demokratycznej, wczesnej ofierze w serii eskalujących ataków, zleconych (zgodnie z tym, co stwierdził później amerykański wywiad) przez samego Putina. Trzecia natomiast wymierzona została w serce amerykańskiej innowacji: Dolinę Krzemową. Od dekady zarządzający Facebookiem, Apple'em i Google'em byli przekonani, że technologia, która wzbogaciła ich o miliardy dolarów, przyspieszy

też rozwój demokracji na całym świecie. Putin miał zaprzeczyć tym założeniom i pokazać, że potrafi wykorzystać te same narzędzia do złamania demokracji i zwiększenia własnej potęgi.

Razem składało się to na wielowymiarowy atak na amerykańską infrastrukturę i instytucje, atak o niespotykanej skali i niesłychanej zuchwałości. Amerykanie czuli się zaszokowani, ale ruchy Putina nie były wcale zaskakujące. Był to jedynie ostatni etap globalnej bitwy toczonej na niewidzialnych polach walki przez większą część dekady — bitwy, w której Ameryka oddała kilka z pierwszych strzałów.

CYBERPRZESTRZEŃ: POLE GLOBALNEJ WALKI XXI WIEKU!

Od czasu do czasu do mediów przedostają się informacje o wykorzystaniu technologii cyfrowej jako broni. Słyszeliśmy o ekstremalnych scenariuszach grożących fizyczną zagładą świata, ale o wiele powszechniejsze jest wykorzystanie cyberbroni przeciwko celom cywilnym: doprowadzenie do potężnych awarii zakładów przemysłowych, sparaliżowanie miejskich systemów komputerowych albo próby fałszowania wyników wyborów. Cyberbroń to wybór idealny: jest tania, łatwa do ukrycia i trudno udowodnić jej wykorzystanie. Można za jej pomocą wpływać na wydarzenia ogólnoświatowe, ale bez wywoływania otwartej wojny. Wystarczy przecież sfrustrować i spowolnić przeciwnika, podkopać działanie instytucji i wzbudzić w obywatelach gniew lub poczucie zagubienia.

Oto ekscytująca i przerażająca opowieść o wojnach, które toczą się w cyberprzestrzeni. Autor opisuje, jak subtelnie działa cyberbroń i jak bardzo wpływa na realia geopolityczne. Wyjaśnia wydarzenia, które miały miejsce całkiem niedawno i o których większość z nas cośkolwiek słyszała. Dowiadujemy się, jak włamania do systemów komputerowych wpłynęły na politykę, gospodarkę i działania wojenne oraz jak rządy i korporacje odpowiedziały na posunięcia hakerów. Ta książka jest jednak czymś więcej niż zbiorem fascynujących, prawdziwych opowieści. Jest również ostrzeżeniem — pokazuje, jak bardzo jesteśmy bezbronni, gdy ktoś zechce wykorzystać przeciw nam siłę informacji. Zaprezentowane w niej fakty i rzadko przytaczane szczegóły pozwalają uzmysłowić sobie, jak groźna stała się cyberprzestrzeń — świat, bez którego dziś tak trudno się obejść.

W TEJ KSIĄŻCE ZNAJDZIESZ WYŁĄCZNIE FAKTY, MIĘDZY INNYMI:

— tworzenie się nowego ładu geopolitycznego
— cybernetyczne wojny prowadzone w ścisłej tajemnicy
— subtelne odmiany broni cyfrowej
— wykorzystanie najnowszych technologii do mrocznych celów
— cybernetyczne szpiegostwo nowej ery
— niebezpieczeństwa zagrażające również zwykłym obywatelom

DAVID E. SANGER jest korespondentem „New York Timesa" i autorem bestsellerowych tytułów. Specjalizuje się w tematyce bezpieczeństwa narodowego. Był członkiem trzech zespołów, które zdobyły Nagrodę Pulitzera, w tym w 2017 roku za dziennikarstwo międzynarodowe. Regularnie komentuje dla CNN, jest też wykładowcą polityki bezpieczeństwa narodowego w John F. Kennedy School of Government na Uniwersytecie Harvarda.

Otrzeźwiające i aktualne... Wykazując się głęboką wiedzą i klarownością przekazu, od zawsze charakteryzującymi jego teksty, Sanger opisuje niebezpieczną i zwodniczą przemianę cyberprzestrzeni w globalne pole walki XXI wieku — „Washington Post".

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-283-7152-1
9 788328 371521
INFORMATYKA W NAJLEPSZYM WYDANIU
Cena: 49,00 zł