NICOLE PERLROTH

CUM SE VA SFÂRȘI LUMEA

CURSA ÎNARMĂRII CIBERNETICE

CUPRINS

CAPITOLUL 1

Camera Secretelor

Times Square, Manhattan

Eram încă plină de praf când editorii mei mi-au spus, în iulie 2013, să îmi predau dispozitivele, să depun un jurământ de tăcere și să intru în camera secretă a lui Arthur Sulzberger.

Doar cu câteva zile mai devreme conduceam de-a lungul ținutului Maasai Mara într-un jeep decapotabil, încheind o excursie de trei săptămâni în Kenya. Am sperat că dacă voi sta câteva săptămâni în afara atenției mă va ajuta să îmi refac nervii întinși în cei doi ani în care am relatat despre terorismul cibernetic. Sursele mele continuau să insiste că acesta era doar începutul – că lucrurile urmau să se înrăutățească.

Aveam doar treizeci de ani pe vremea aceea, dar deja simțeam povara imensă a subiectului ce îmi fusese desemnat. În 2010, când mi s-a propus să mă alătur celor de la *The New York Times*, scriam articole pentru prima pagină a revistelor din Silicon Valley, despre investitorii care, prin pur noroc sau printr-un simț dezvoltat al afacerilor, investiseră încă de la început în Facebook, Instagram și Uber, iar acum deveniseră foarte conștienți de statutul lor de celebrități.

Conducerea *The New York Times* a remarcat aceste articole și a fost interesată să mă angajeze, doar că pentru un alt tip de subiect. „Sunteți de la *The New York Times*", le-am spus. „Voi scrie articole despre orice domeniu doriți. Cât de rău ar putea fi?" Când mi-au spus că s-au gândit la mine să acopăr domeniul securității cibernetice, eram sigură că glumesc. Nu doar că nu știam nimic despre securitatea cibernetică, dar mă străduisem intens să nu știu nimic despre securitatea cibernetică. Cu siguranță că puteau găsi reporteri despre securitatea cibernetică mai calificați decât mine.

„Am intervievat acei oameni", mi-au zis. „Dar nu am înțeles nimic din ceea ce spuneau."

Doar câteva luni mai târziu participam la o duzină de interviuri de jumătate de oră cu editori seniori la sediul *The New York Times*, încercând să îmi maschez panica. Când interviurile din acea seară s-au încheiat, am traversat strada la cea mai apropiată bodegă, am cumpărat cel mai ieftin vin cu capac din plastic pe care l-am putut găsi și l-am băut pe nerăsuflate direct din pungă. Mi-am spus că măcar într-o zi le voi putea spune nepoților mei că sfântul *The New York Times* m-a invitat odată în clădire.

Dar, spre surprinderea mea, am fost angajată. Iar trei ani mai târziu încă îmi ascundeam panica. În acei trei ani, am făcut reportaje despre hackerii chinezi care atacau termostate, imprimante și aplicații de livrare la domiciliu. Am relatat despre un atac cibernetic iranian care a înlocuit datele celei mai bogate companii petroliere din lume cu imaginea unui steag american arzând. Am urmărit cum hackerii armatei chineze scotoceau prin mii de sisteme informatice americane, căutând orice, de la planurile celui mai recent bombardier invizibil până la formula băuturii Coca-Cola. Am relatat despre seria de atacuri rusești, din ce în ce mai numeroase, asupra companiilor americane din domeniul energiei sau al utilităților. Tot în acest timp, împreună cu echipa de securitate IT a ziarului *The New York Times*, am urmărit hackerul chinez, pe care l-am numit „stagiarul de vară", încercând

să pătrundă în rețelele noastre în fiecare dimineață de la ora 10.00, ora Beijingului, și până la ora 17.00, în căutarea surselor noastre.

În tot acest timp, m-am agățat cu disperare de ideea că aș putea duce o viață normală. Dar cu cât mă aventuram mai adânc în această lume, cu atât mă simțeam mai mult în derivă. Tot timpul apăreau lucruri neprevăzute. Timp de săptămâni, abia dacă apucam să dorm câte puțin; cred că arătam de parcă aș fi fost bolnavă. Orarul după care funcționam m-a costat mai mult decât o relație. Și nu a trecut mult până când a început să apară paranoia. De prea multe ori m-am surprins uitându-mă cu suspiciune la orice era conectat la o priză, îngrijorată fiind că ar putea fi un spion chinez.

Pe la mijlocul anului 2013 eram hotărâtă să mă îndepărtez cât mai mult de orice avea legătură cu computerele. Africa părea cel mai bun loc pentru asta. După trei săptămâni de dormit în cort, de alergat cu girafele și terminând fiecare zi cu contemplarea unui apus, urmărind cum dispare soarele în spatele unei turme de elefanți ce se mișcau lent și, mai târziu, relaxându-mă lângă un foc de tabără în timp ce ghidul meu, Nigel, îmi povestea despre răgetul fiecărui leu, de abia atunci am început să simt balsamul îndepărtării de toate acele probleme.

Dar, când m-am întors în Nairobi, telefonul meu și-a reluat bâzâitul fără sfârșit. Stând în fața unui adăpost pentru elefanți din Karen, Kenya, am inspirat profund încă o dată, iar apoi am parcurs miile de mesaje necitite din căsuța poștală. Unul dintre acestea era mai strident decât celelalte: „Urgent. Sună-mă". Era editorul meu de la *The New York Times*. Deși legătura era slabă, el insista să vorbească în șoaptă, îngropându-și cuvintele în vacarmul din redacție. „Cât de repede poți ajunge la New York?... Nu-ți pot spune la telefon... Trebuie să îți spun personal... Vino aici."

Două zile mai târziu ieșeam dintr-un lift la etajul conducerii din sediul *The New York Times*, încălțată cu o pereche de sandale pe care le cumpărasem de la un războinic Massai. Era în iulie 2013, iar Jill

Abramson și Dean Baquet – directorul executiv al *The New York Times* de la acea vreme și cel care în curând avea să îi ia locul – mă așteptau. Rebecca Corbett, editorul departamentului de investigații al *The New York Times*, și Scott Shane, reporterul nostru veteran în securitate națională, fuseseră chemați și ei. Mai erau acolo încă trei fețe pe care nu le cunoșteam la acea vreme, dar pe care am ajuns să le cunosc foarte bine: James Ball și Ewen MacAskill de la ziarul britanic *The Guardian* și Jeff Larson de la ProPublica*.

James și Ewen au relatat cum, în urmă cu câteva zile, ofițerii de informații britanici au intrat ca o furtună în sediul din Londra al ziarului *The Guardian* și au obligat conducerea ziarului să distrugă hard-diskurile cu informații secrete ale lui Snowden, dar puțin prea târziu, pentru că o copie a acestora apucase deja să fie transmisă ilegal celor de la *The New York Times*. Jill și Dean au spus amândoi că Scott și cu mine vom lucra împreună cu reporterii de la *The Guardian* și ProPublica pentru a scrie două articole referitoare la scurgerile de informații de care era răspunzător Edward Snowden, infamul antreprenor care lucra pentru NSA și care a furat mii de documente secrete din computerele agenției înainte de a fugi în Hong Kong, pentru ca mai târziu să ajungă exilat la Moscova. Snowden îi dăduse toate aceste secrete lui Glenn Greenwald, un autor de editoriale de la *The Guardian*. Dar ni s-a reamintit în acea zi că în Marea Britanie libertatea de exprimare era la fel de respectată ca în Statele Unite. Colaborarea cu un ziar american, în special cu unul care avea cei mai buni avocați specializați în Primul Amendament, precum *The New York Times*, le oferea celor de la *The Guardian* puțină siguranță.

Dar, în primul rând, *The Guardian* avea reguli. Nu trebuia să suflăm nicio vorbă despre proiect nimănui. „Fără pescuit", ceea ce

* Organizație nonprofit cu sediul la New York, care își propune să facă jurnalism de investigație în interes public. (n.red.)

însemna că ni s-a interzis să căutăm în documente cuvinte-cheie care nu au legătură directă cu sarcinile noastre. Fără telefoane și fără internet. A, da, să nu uit, și fără ferestre.

Ultima parte s-a dovedit a fi puțin problematică. Arhitectul italian Renzo Piano proiectase sediul ziarului *The Times* ca pe un model de transparență deplină. Întreaga clădire – fiecare etaj, fiecare sală de conferințe, fiecare birou – este încastrată în sticlă din podea până în tavan, cu excepția unui singur spațiu: debaraua secretă a lui Arthur Sulzberger.

Această ultimă cerere mi s-a părut absurd de paranoică, dar britanicii au insistat. Exista posibilitatea ca NSA, echivalenta sa britanică, Cartierul General al Comunicațiilor Guvernului*, sau oricine altcineva să ne intercepteze conversațiile prin intermediul unor raze laser. Aceiași tehnicieni ai GCHQ care au supravegheat la *The Guardian* distrugerea hard-diskurilor lui Snowden i-au instruit și în acest sens[1].

Și așa am luat pentru prima dată contact cu realitatea post-Snowden.

Zi după zi, în următoarele șase săptămâni, mi-am luat adio de la dispozitivele mele, m-am târât în această ciudată, secretă și securizată locație, înghesuită între Scott, Jeff și britanici, am cercetat cu atenție documentele secrete ale NSA și nu am spus nimănui.

Sinceră să fiu, reacția mea față de informațiile publicate din documentele secrete ale NSA a fost probabil foarte diferită față de cea a majorității americanilor, care au fost șocați să descopere că agenția noastră națională de spionaj într-adevăr spiona. După trei ani în care m-am ocupat fără întrerupere de spionajul chinezesc, o mare parte din mine s-a liniștit văzând că propriile noastre capacități de hacking depășeau cu mult e-mailurile de phishing scrise

---

* Government Communications Headquarters, acronim GCHQ, în engl. în orig. (n.red.)

greșit pe care le foloseau hackerii chinezi pentru a pătrunde în rețelele americane.

Misiunea lui Scott a fost să scrie o relatare cuprinzătoare despre capabilitățile NSA. Misiunea mea a fost mai simplă, dar – având în vedere că nu aveam telefon, nu aveam internet și aveam interdicție să îmi sun orice sursă –, de asemenea, înnebunitor de plictisitoare: trebuia să aflu cât de departe ajunseseră cele mai importante agenții de informații din lume în descifrarea criptării digitale.

După cum s-a dovedit, nu prea departe. După câteva săptămâni de sortare a documentelor a devenit clar că algoritmii de criptare digitală ai lumii rezistau – în cea mai mare parte – destul de bine. Dar era clar, de asemenea, că NSA nu a trebuit să descifreze acești algoritmi de criptare câtă vreme a descoperit atâtea moduri de a pirata ocolindu-i.

În unele cazuri, NSA comunica prin canale neoficiale cu agențiile internaționale care stabileau standardele criptografice adoptate de companiile de securitate și de către clienții acestora[2]. În cel puțin un caz NSA a convins cu succes birocrații canadieni să susțină o formulă greșită pentru generarea de numere aleatorii în schemele de criptare, pe care computerele NSA le putea pirata cu ușurință. Agenția plătea chiar și marile companii americane de securitate, precum RSA, pentru a face din formula sa greșită de generare de numere aleatorii metoda de criptare implicită pentru produsele de securitate utilizate pe scară largă. Când companiile plătite nu au folosit acest truc, partenerii NSA de la CIA s-au infiltrat în fabricile celor mai importanți producători de cipuri de criptare din lume și au introdus defecte de tip backdoor* în cipurile care prelucrau datele. Iar în alte cazuri, agenția s-a infiltrat în serverele interne ale

* Ușă din spate, în engl. în orig., o metodă secretă, hardware sau software, de a ocoli autentificarea pentru a obține acces la informații protejate. (n.red.)

companiilor precum Google sau Yahoo, pentru a fura datele înainte ca acestea să fie criptate.

Snowden a declarat mai târziu că ar fi dezvăluit date ale NSA pentru a atrage atenția publicului asupra a ceea ce el a considerat ca fiind supraveghere nelimitată. Cele mai tulburătoare dintre dezvăluirile sale păreau să fie programul NSA de colectare a metadatelor apelurilor telefonice – un jurnal despre cine a sunat pe cine, când și cât timp au vorbit – și programele de interceptare legală care au obligat companii precum Microsoft și Google să dezvăluie date despre clienții lor. Însă contrar șocului și indignării pe care acele programe le-au provocat la televizor și în cadrul guvernului, devenea evident că americanii nu vedeau ceea ce era cu adevărat important.

Documentele erau înțesate de referințe despre backdoor-urile pe care NSA le introdusese în aproape fiecare unitate de hardware și software de pe piață. Agenția părea să fi achiziționat o bibliotecă vastă de backdoor-uri invizibile pe care le-a infiltrat în aproape fiecare aplicație importantă, platformă social media, server, router, firewall, software antivirus, iPhone, telefon Android, telefon BlackBerry, laptop, computer desktop și sistem de operare.

În lumea pirateriei digitale, acest backdoor invizibil are un nume științifico-fantastic: zero-day* (sau 0 day), pronunțat „oh-day". *Zero-day* este unul dintre acei termeni cibernetici, cum ar fi *infosec*** și *man-in-the-middle attack****, pe care profesioniștii în securitate îi

---

* Ziua zero, în engl. în orig. (n.red.)

** Denumire prescurtată pentru Information Security, Securitatea Informațiilor, în engl. în orig., se referă la protejarea informațiilor prin prevenirea sau reducerea riscului unui acces neautorizat la date sau a utilizării, ștergerii, modificării etc. ilegale a acestora.

*** Man-In-The-Middle Attack, acronim MITMA, în engl. în orig., adică un Atac Cu Un Om La Mijloc, este un atac cibernetic în care atacatorul transmite în secret, modificând comunicațiile dintre cele două părți care cred că mesajele lor sunt transmise direct interlocutorului.

folosesc pentru a face ca totul să pară foarte simplu pentru noi, restul, astfel încât să nu le dăm o importanță prea mare[3].

Pentru cei neîndoctrinați: zero-day oferă superputeri digitale. Sunt ca o mantie care te face invizibil, iar pentru spionii și delincvenții cibernetici, cu cât te poți face mai invizibil, cu atât vei avea mai multă putere. La cel mai elementar nivel, un zero-day este un defect de software sau hardware pentru care nu există niciun remediu. Și-a primit numele pentru că, la fel ca în cazul Pacientului Zero într-o epidemie, atunci când este descoperit un defect zero-day, companiile de software și hardware au zero zile pentru a găsi un remediu astfel încât acest defect să nu poată fi exploatat în scopuri răuvoitoare. Până când furnizorul descoperă defectul, găsește remediul, distribuie soluția utilizatorilor de pe tot globul, iar utilizatorii își rulează actualizările de software – *Dragă cititorule: rulează-ți actualizările de software!* –, sau face o modificare ori diminuează pagubele în alt mod, hardware-ul este vulnerabil, iar toți cei care utilizează sistemul afectat sunt, de asemenea, vulnerabili.

Zero-day este arma cea mai periculoasă din arsenalul unui hacker. Descoperirea unuia este ca și cum ai descoperi parola secretă pentru toate datele din lume. Un zero-day de foarte bună calitate în software-ul unui telefon Apple permite spionilor și hackerilor, care au abilitățile necesare pentru a-l exploata, să pătrundă de la distanță nedetectați în iPhone-uri și să obțină acces la toate detaliile vieții noastre digitale. O serie de șapte zero-day ale Microsoft Windows și ale software-ului industrial Siemens au permis spionilor americani și israelieni să saboteze programul nuclear al Iranului. Spionii chinezi au folosit un singur zero-day al Microsoft pentru a fura unele dintre cele mai bine păstrate coduri-sursă din Silicon Valley.

Găsirea unui defect zero-day seamănă puțin cu utilizarea modului Dumnezeu (puteri depline) într-un joc video. Odată ce hackerii au descoperit comenzile sau au reușit să scrie codul pentru a exploata acest zero-day, ei se vor plimba nedetectați prin

rețelele de computere ale lumii până în ziua în care defectul ascuns este descoperit. Exploatarea defectelor zero-day este cea mai bună ilustrare a zicalei „Informația înseamnă putere dacă știi cum să o folosești".

Exploatând oportunitățile oferite de defectele zero-day, hackerii pot pătrunde în orice sistem – orice companie, agenție guvernamentală sau bancă – care se bazează pe software-ul sau hardware-ul afectat și pot infiltra o secvență de cod pentru a-și atinge obiectivul, fie că este vorba de spionaj, furt financiar sau sabotaj. Nu contează dacă acel sistem este complet corectat. Nu există corecții pentru defectele zero-day, până când acestea nu sunt descoperite. Este ca și cum ai avea o cheie de rezervă pentru o clădire încuiată. Nu contează dacă ești cel mai vigilent administrator IT de pe pământ. Dacă cineva știe un defect zero-day al unui segment de software care rulează pe computerul tău și știe cum să îl exploateze, îl poate folosi pentru a intra în computerele tale, fără știrea ta, făcând din defectul zero-day unul dintre cele mai râvnite instrumente din arsenalul unui spion sau al unui infractor cibernetic.

Timp de decenii, pe măsură ce Apple, Google, Facebook, Microsoft și alții au introdus mai multe chei de criptare în serverele de date și în protocoalele de comunicații, singura modalitate de a intercepta date necriptate a fost să pătrundă în dispozitivul cuiva înainte ca datele utile să fi fost criptate. În acest proces, „exploit-urile pentru vulnerabilitățile zero-day" au devenit diamantele sângerii ale comerțului cu echipamente de securitate, urmărite de statele naționale, antreprenorii care au contracte cu armata și infractorii cibernetici, pe de o parte, și apărătorii securității, pe de altă parte. În funcție de locul în care este descoperită vulnerabilitatea, exploatarea unei vulnerabilități de tip zero-day poate oferi posibilitatea de a spiona fără a fi descoperit de utilizatorii de iPhone din întreaga lume, de a anihila măsurile de siguranță ale unui combinat chimic sau de a prăbuși o aeronavă. În unul dintre exemplele cele mai flagrante,

o eroare de programare, o singură cratimă lipsă, a ghidat Mariner 1 – prima navă spațială americană creată pentru a explora planeta Venus – în afara traiectoriei prevăzute, forțând NASA să-și distrugă nava spațială de o sută cincizeci de milioane de dolari după numai două sute nouăzeci și patru de secunde de la lansare, altfel existând riscul ca aceasta să se prăbușească peste o rută maritimă din Atlanticul de Nord sau, mai rău, deasupra unui oraș foarte populat[4]. În lumea noastră virtuală, întâlnisem aproape peste tot corespondentul erorii de cratimă lipsă, iar acum realizam cât de important devenise pentru cei mai importanți spioni ai națiunii noastre. Conform informațiilor la care am avut acces, lista extinsă a NSA sugera faptul că hackerii puteau penetra și spiona orice dispozitiv, chiar și atunci când nu era conectat la rețea sau chiar dacă nu era pornit. Agenția putea să ocolească majoritatea sistemelor de detectare antiintruziune și să transforme dispozitivele antivirus – chiar software-ul conceput pentru a ține la distanță spionii și infractorii cibernetici – într-un instrument puternic de spionaj. Documentele furate de Snowden fac doar aluzie la aceste instrumente de hacking. Acestea nu conțineau instrumentele în sine, deci codul efectiv și algoritmii utilizați.

Companiile producătoare ale acestor tehnologii nu ofereau agenției erorile care puteau permite accesarea ilegală a sistemelor proprii. Când primele documente ale lui Snowden au fost făcute publice, sursele mele de la cele mai importante companii producătoare de hardware și software ale națiunii – Apple, Google, Microsoft, Facebook – au jurat că, da, s-au conformat cererilor legale privind informațiile personale ale clienților, dar de fapt nu, pentru că nu au dezvăluit niciodată celor de la NSA sau oricărei alte agenții guvernamentale vreo eroare de tip zero-day a oricăreia dintre aplicațiile, produsele sau software-ul lor. S-a dovedit mai târziu că unele companii, precum Yahoo, au făcut aproape orice pentru a se conforma solicitărilor legale ale NSA[5].