PROLOG

ZLOČIN@21STOLETÍ.COM

Při ustavičné honbě za pohodlím a ekonomickým růstem jsme dospěli do situace, kdy jsme nebezpečně závislí na síťových systémech. Tuto závislost jsme si přitom stihli vypěstovat za velmi krátkou dobu: vždyť valné části takzvaných „kritických národních infrastruktur" (v technickém žargonu krátce jen CNI) většiny zemí se dostaly pod nadvládu stále složitějších počítačových systémů během ani ne dvou desetiletí.

Dnes počítače řídí podstatnou část našeho života – ovládají naši komunikaci, automobily, obchodování i kontakt se státní správou, naši práci i volný čas... zkrátka prakticky vše okolo nás. Při jednom soudním přelíčení – a v minulých letech jsem se účastnil hned několika, která se konala kvůli kybernetickým zločinům – britská královská prokuratura požadovala, aby soud uvalil na hackera takzvaný preventivní soudní příkaz, který by vešel v platnost v den hackerova propuštění z vězení a zakazoval by mu přístup k internetu s výjimkou jediné hodiny týdně pod dohledem policejního důstojníka. „Až si můj klient odsedí svůj trest," prohlásil právní zástupce obžalovaného hackera, „sotva bude existovat jediná lidská činnost, která nebude nějakým způsobem zprostředkována internetem. Jak za těchto podmínek má potom můj klient vést normální život?" položil obhájce řečnickou otázku.

Přesně tak, jak? Kdo ze závislejších uživatelů zapomněl někdy doma mobilní telefon a neměl jej u sebe třeba jen na pár hodin, dobře ví, že člověk se cítí náhle nesvůj, má pocit ztráty či nahoty. Zajímavé je, že když nemáte přístroj po ruce nějaké tři dny, pocit neklidu vystřídá vlna osvobození – člověk se vrátí zpět do světa, nepříliš vzdáleného světa, kdy jsme mobilní telefony neměli či je nepotřebovali a organizovali si život bez nich. Většina lidí má však pocit, že bez těchto malých přenosných počítačů vůbec nemůže existovat.

Dobrým příkladem dnešního významu počítačů je obyčejné auto. Když se někdy kolem 40. let 20. století automobily staly standardní výbavou rodiny, jen málokterý řidič rozuměl tomu, co se odehrává pod kapotou. Nicméně ať byla příčina poruchy jakákoli, spousta lidí uměla auto opravit. Ještě více pak bylo těch, kteří dokázali domluvit karburátoru alespoň tak, že se vozidlo dobelhalo domů. A většina lidí určitě uměla přinejmenším vyměnit pneumatiku.

Pokud je problém jen v píchnuté pneumatice, do cíle nejspíše dojedete i dnes. Jenže čím dál vyšší počet poruch je způsoben selháním počítače v elektronické řídicí jednotce – té černé plastikové krabičce, kterou většinou najdete uloženou za motorem. Můžete být třeba zkušený tankový mechanik, ale je-li elektronická řídicí jednotka vadná, s autem prostě nepohnete. Při troše štěstí vám auto opraví nějaký počítačový inženýr, nejspíše však budete muset poškozenou jednotku vyměnit.

Počítačové systémy jsou podstatně složitější a křehčí než spalovací motory. Proto se nemůžeme divit, že jen ta nejužší skupina lidí umí související problémy řešit stylem jdoucím nad rámec známé mantry „zkoušeli jste to restartovat?“.

Dnes se nacházíme v situaci, kdy technologiím, které ve stále větší míře denně řídí naše životy, rozumí pouze tato nepočetná elita – říkejte jim geekové, hackeři, kodéři, sekurokrati, nebo jak chcete. Důležité je, že pro většinu z nás jsou tyto technologické výstřelky zcela nesrozumitelné. Význam této skutečnosti jsem si začal uvědomovat, když jsem pracoval na své předchozí knize *McMafie,* v níž jsem se věnoval globálnímu organizovanému zločinu. V rámci vyšetřování jednoho případu týkajícího se kybernetické kriminality jsem se vydal na cestu do Brazílie. Je to atraktivní země a má spoustu svých krás, mě však do ní přivedl jiný důvod: v té době to moc lidí nevědělo, ale Brazílie je jednou z největších líhní internetových podvodů.

Setkal jsem se tam s kybernetickými zloději, kteří stáli za jedním velmi úspěšným phishingovým podvodem. Phishing (rhybaření) je stále jednou z nejspolehlivějších metod internetové kriminality. Existuje ve dvou jednoduchých podobách. První způsob funguje tak, že oběť otevře spamovou e-mailovou zprávu. Její příloha může obsahovat virus, který po spuštění umožní počítači umístěnému třeba v zemi na opačném konci světa monitorovat veškerou aktivitu na infikovaném stroji, a to včetně zadávaných autorizačních údajů k bankovnímu účtu. Druhý trik

spočívá ve vytvoření e-mailu, který útočník vydává za oficiální zprávu odeslanou bankou nebo jinou institucí; zpráva přitom žádá o potvrzení přesného znění přihlašovacího jména a hesla. Jestliže se adresát chytí do této pasti, jeho údaje může útočník použít k získání přístupu k některým nebo všem webovým účtům. Brazilští hackeři mi předvedli krok za krokem, jak si touto činností zajistili desítky milionů dolarů, které ukradli z bankovních účtů v Brazílii, Španělsku, Portugalsku, Velké Británii a USA.

Navštívil jsem i policisty z oddělení, které se specializuje na odhalování kybernetického zločinu. V té době tito policisté zadrželi další čtyři lidi ze zmíněné zločinecké skupiny (třebaže nikdy neodhalili zbytek týmu, ve kterém působilo minimálně dvakrát tolik osob). Poté jsem dělal rozhovor se šéfem X-Force, což je oddělení tajných operací americké bezpečnostní společnosti ISS. V rozmezí asi dvou týdnů jsem si uvědomil, že pro pachatele s sebou tradiční organizovaný zločin – ač pestrý a rozmanitý – nese daleko větší rizika než kriminalita kybernetická.

Chtějí-li staromódně fungující skupiny organizovaného zločinu, odkázané na technologie a nástroje 20. století, ve svém oboru uspět, musejí překonávat dvě překážky. Nepřítelem číslo jedna jejich byznysu je policie. Efektivnost výkonu práva se liší v závislosti na geografické poloze i na čase. Organizovaný zločin se přizpůsobuje těmto proměnlivým podmínkám a gangy volí jednu z mnoha metod, pomocí nichž se lze s muži zákona a pořádku vypořádat – mohou se pokusit je ovlivnit silou; zkorumpovat; mohou zkorumpovat politiky, jímž je policie podřízena dle zákona; nebo se vyhýbat dopadení.

Pak ale zločinci musí čelit ještě druhému problému: hrozbě, kterou představuje konkurence – i ostatní zlí hoši totiž rozhazují sítě ve stejných vodách. A opět, mohou se pokusit porazit je silou; nabídnout jim spojenectví; nebo se oni poddají jim.

Zločinecký syndikát si však v žádném případě nemůže dovolit tyto dvě překážky ignorovat – taková cesta vede k selhání s často fatálními následky. Klíčem k přežití a prosperitě je schopnost komunikovat s ostatními zločinci i s policií – a samozřejmě vysílat oběma skupinám ty správné signály.

V Brazílii jsem velice rychle zjistil, že zločin 21. století je v tomto směru odlišný.

Nejpodstatnějším rozdílem je, že policisté mají daleko větší problém vystopovat zločince, kteří se dopouštějí trestné činnosti na internetu.

Zákony regulující internet se podstatně liší stát od státu. Tato skutečnost je velmi důležitá, neboť obecně vzato může na webu dojít ke spáchání trestného činu z IP adresy jedné země, zatímco oběť (jednotlivec či korporace) se nachází v druhé zemi a k realizaci činu (či inkasování peněz) dochází ve třetí zemi. Například policejní důstojník z Kolumbie může vystopovat IP adresu, z níž byl veden útok na kolumbijskou banku, a zjistí, že akce vyšla z Kazachstánu. Jenže pak se dozví, že v Kazachstánu tento čin není považován za trestný, takže jeho kolega z kazachstánské metropole Astany nebude mít sebemenší důvod zahájit vyšetřování.

Spousta kybernetických zločinců se vyzná v těchto legislativních rozdílech a umí je i náležitě využívat. „Nikdy nepoužívám americké kreditní nebo debetní karty," řekl mi jeden velmi úspěšný švédský „specialista", „protože tím bych spadal pod jurisdikci Spojených států, ať bych se nacházel kdekoli na planetě. Takže dělám jen evropské a kanadské karty – tohle mi stačí a zároveň jsem i v bezpečí. Nikdy mě nechytí."

Předěl oddělující Spojené státy od Evropy a Kanady je tím nejpodstatnějším, protože tyto regiony se vyznačují největší koncentrací obětí kyberzločinu. Evropa a Kanada mají daleko přísnější zákony chránící svobody jednotlivce, jež lidem zaručují na internetu větší práva. Jednotlivé vlády Spojených států předaly naopak v průběhu let policii mnohem více pravomocí než v Evropě. Díky tomu mají policisté v USA snazší přístup k datům v počítačích soukromých subjektů – a to především ve jménu boje se zločinem a terorismem.

Tyto skutečnosti s sebou nesou vážné a také – alespoň pro tuto chvíli – těžko předvídatelné následky. V kyberprostoru na sebe neustále naráží spousta různých zájmů a motivací: obavy ze zločinu, strach z ustavičného dozoru a ztráty soukromí, sbírání dat jak soukromými, tak i státními institucemi, pak také svoboda slova (viz kauza WikiLeaks), snadný přístup k webovým stránkám (spor o tzv. síťovou neutralitu), sociální sítě coby politický nástroj a národní bezpečnostní zájmy.

Například někdo by mohl tvrdit, že Google porušuje principy americké antimonopolní legislativy, jelikož je všudypřítomný, funguje na všech platformách, nabízí tolik služeb a zpracovává obrovská množství dat; a také že sbíráním osobních dat dává šanci zločincům a ohrožuje tím občanské svobody. Přesto by vám zástupce Googlu mohl s klidnou duší odpovědět, že každičká esence génia a úspěchu této firmy leží právě v jeho všudypřítomnosti, podpoře různých platforem, v počtu služeb

a ve zpracovávání dat a že tím prospívá americkým obchodním a bezpečnostním zájmům. Pokud americká vláda chce, může během několika mála hodin získat pomocí právních procedur přístup k datům Googlu, a protože Google sbírá data z celého světa, Washington tím získává nesmírnou strategickou výhodu. Co by za takovou možnost jen daly ostatní vlády. Aby americká administrativa odhalila tajemství, jež Google drží pod pokličkou, na rozdíl od vlád v Číně, Rusku nebo na Blízkém východě se vůbec nemusí obtěžovat s hackováním jeho sítí. Namísto toho si prostě zažádá o vydání soudního příkazu. Skutečně byste se ve jménu antimonopolní legislativy vzdali takovýchto možností?

Internet je jako jedno velké bublinové pole – vyřešíte jeden problém, který internet sužuje, ovšem v tom hned vedle vybublá na povrch problém nový, zdánlivě stejně nezkrotný.

Pro policii a další orgány činné v trestním řízení je největší překážkou anonymita. I dnes má každý člověk stále jedinečnou možnost používat internet anonymně, ví-li, jak na to – jestliže umí maskovat fyzickou polohu svého počítače.

Maskování polohy se provádí dvěma hlavními způsoby – první kybernetickou zdí je tzv. VPN neboli *virtuální privátní síť*, kde skupina počítačů sdílí jedinou IP adresu. Daná IP adresa patří obvykle jedinému počítači, ale díky VPN se může několik počítačů rozmístěných na naprosto odlišných místech po světě tvářit tak, jako by byly třeba v Botswaně.

Komu k ochraně soukromí nestačí VPN, může se postavit za druhý maskovací val použitím takzvaných proxy serverů. Počítač na Seychelách může použít proxy server umístěný například v Číně nebo Guatemale. Proxy server maskuje pravou IP adresu a neprozradí, že adresa má svůj původ na Seychelách, a rozhodně nevyzradí ani to, že počítač je součástí VPN v Grónsku.

K nastavení VPN a proxy serverů je potřeba mít pokročilé počítačové znalosti, a tak tyto techniky zpravidla používají jen dvě skupiny namočené do kybernetické kriminality – opravdoví hackeři a opravdoví zločinci. Jenže tito „high-end operátoři", kteří reprezentují nový typ závažného organizovaného zločinu, tvoří mezi všemi osobami namočenými do počítačových zločinů jen nepatrnou část.

Když člověk přihlédne k nedostatečným policejním zdrojům, tak tato hrstka aktérů, kteří se pohybují v triviálně malých sumách, je skupinou neškodných zlodějíčků, jejichž hledání prakticky nestojí za námahu. Ani

když se tyto osoby neobtěžují s výstavbou virtuálních privátních sítí, proxy serverů a kupou dalších maskovacích technik, policii mohou ztížit život už jen tím, že budou svou komunikaci šifrovat.

Bezplatný software určený pro šifrování písemné (a dokonce i hlasové a videohlasové) komunikace lze snadno dohledat na webu – jedním z nejznámějších nástrojů tohoto typu je program PGP, což je zkratka sousloví Pretty Good Privacy (Dost dobré soukromí).

Šifrování představuje velmi účinný nástroj, který hraje ve světě kybernetické bezpečnosti důležitou roli. Je to způsob, jak „rozmazat" jazyk pomocí digitálně generovaných klíčů, jejichž permutace jsou z matematického hlediska astronomické, takže zašifrovaný obsah lze přečíst, jen pokud znáte heslo. Zašifrované dokumenty jsou i z dnešního pohledu dobře zabezpečené a šifrování jako takové je ve své podstatě stále spolehlivé, třebaže washingtonský Národní bezpečnostní úřad (NSA), nejmocnější digitální špionážní agentura na světě, neúnavně pracuje na tom, jak používané techniky šifrování prolomit. Bratrstvem kyberzločinců se nesou zvěsti, že Tajná služba USA a tajné služby z Kanady, Británie, Austrálie a Nového Zélandu už umějí prolomit veřejné šifrovací systémy, a to pomocí orwellovského systému Echelon. Ten, soudě alespoň podle různých nepotvrzených zpráv, může sledovat telefonní, e-mailovou a satelitní komunikaci z celého světa.

Politické důsledky digitálního šifrování mají natolik závažný charakter, že vláda Spojených států amerických začala v 90. letech šifrování klasifikovat jako „vojenskou technologii". V jiných zemích může použití šifrování člověka přivést dokonce i do vězení, aniž by přitom policii zajímalo, že zašifrovaný soubor obsahuje něco tak nevinného jako nákupní seznam. V době, kdy vlády a korporace hromadí o svých občanech a klientech stále větší množství osobních informací, je šifrování jedním z mála obranných prostředků, které lidem ještě zůstaly k ochraně soukromí. Šifrování je však také neocenitelným nástroje pro každého člověka namočeného do trestné činnosti páchané na internetu.

Stejně jako tradiční zločinci hledají způsoby, jak identifikovat při rozhovorech přátele, nepřátele, policisty a rivaly, potýkají se kybernetičtí zločinci s permanentním úkolem vytvořit osobám, s nimiž se po internetu baví, určitý typ „osobních dokladů" nutných k identifikaci. V jedné části této knihy se dočtete o metodách, jež kyberpodvodníci vyvinuli k identifikaci, a jak se policejní složky z různých koutů světa naopak

pokoušely hackerům zabránit ve vystopování policistů, agentů a tajných informátorů číhajících na síti.

V 90. letech spočíval nejjednodušší způsob, jak zabránit nevítaným hostům strkat nos do vašich kriminálních aktivit, o nichž jste se bavili na webových stránkách, v zavedení omezeného přístupu. Ke konverzaci se mohli dostat pouze uživatelé se znalostí příslušných hesel a dalších oprávnění. Přesto však bylo otázkou jen několika mála měsíců, než se do těchto systémů vplížily i bezpečnostní složky jako Tajná služba ministerstva vnitřní bezpečnosti USA nebo ruská FSB (nástupce KGB) – přístup získaly buď prostřednictvím agentů, kteří vytrvale předstírali, že jsou kyberzločinci, nebo přes informátory, které přinutily ke spolupráci.

Někteří agenti zahráli své role natolik přesvědčivě, že jiné bezpečnostní složky na ně dokonce poslaly vlastní muže – měly totiž podezření, že v utajení pracující policisté ze sesterských organizací jsou skuteční zločinci.

Deset let trvající snaha policistů a tajných agentů přinesla ovoce – vznikla obrovská databáze kriminálních hackerů: databáze s jejich přezdívkami, skutečnými či předpokládanými místy pobytu, typem aktivit i informacemi o tom, s kým nejčastěji komunikují. Ačkoli tak policisté získali nesčetná množství informací o nejnižší kastě kybernetických zločinců, není vůbec snadné je postavit před soud.

Mužům zákona a pořádku svazuje ruce samotná povaha webu – zejména jeho vzájemná propojenost. Nikdo si totiž nemůže být stoprocentně jist, s kým na síti doopravdy komunikuje. Stojí proti vám tuctový hacker? Nebo si zahráváte s někým, kdo má přátele na vyšších místech? Píšete si se zločincem, nebo s policistou v přestrojení? Nebo s vojenským výzkumníkem, jenž pouze zkoumá význam kriminálních hackovacích technik? Sledujete vy jeho, nebo on vás? Snaží se získat peníze pro sebe, nebo pro Al-Káidu?

„Je to jako hrát sedmirozměrné šachy," poznamenal futurolog Bruno Giussani. „Nikdy nevíte, kdo je v daný okamžik vaším protihráčem."

Když jsem přijel do ústředí Googlu v kalifornském Mountain View, nebyl to sice tentýž pocit, jako když člověk poprvé v životě spatří Tádž Mahal, ale bylo zde něco společného. Jakmile jsem zaparkoval auto na Charleston Avenue před pestrobarevnou značkou oznamující, že jsem v jednom ze zázraků postindustriálního světa, zmocnila se mě vlna bázně.

Rychlost, s jakou se Google dostal do našeho podvědomí – se všemi těmi příznaky, jež k narkotiku patří – je bezprecedentní. Mohou se mu rovnat pouze ostatní největší firmy informačního věku – Apple, Facebook, Microsoft a Amazon. Ale ani jeden z této trojky se nemůže pochlubit takovým vlivem, jakého dosáhl Google – tím, jak nám v životě pomáhá, když jeho obří serverové farmy vyplivují tuny bajtů požadovaných informací, a jak naše životy řídí a monitoruje, když tyto servery chlemtají a ukládají individuální a kolektivní data, profily miliard lidí. Tato data o nás prozrazují daleko víc, než o sobě víme my sami. Není příjemný pocit, když pomyslíte na to, co by se mohlo stát, kdyby tyto informace padly do špatných rukou. A možná už padly...

Jaké byly mé dojmy z návštěvy sídla společnosti? Příjemně působící směs hlavních a vedlejších pastelových barev známých z loga Googlu se nese celým tamním „kampusem". Velké objekty rozptýlené po areálu mají často měkké zaoblené lemy. Na tamní sochy se člověk nemusí nutně jen dívat, ale může na nich i sedět, či si s nimi dokonce hrát. V závislosti na míře vašich obav a paranoii celý komplex připomíná buď rozlehlou mateřskou školku, nebo bizarní vesnici z televizní show z 60. let s názvem *The Prisoner* (Vězeň). Do této vesnice byli posíláni lidé představující ohrožení národní bezpečnosti a nebylo odtud úniku. Mám asi bujnou představivost, ale ať v Googlu potkám uklízečku nebo vyššího manažera, na jejich tváři vidím úsměv, jako kdyby byli v hypnóze. Výraz ve tvářích zaměstnanců jednak zesiluje paranoidní interpretaci podstaty Googlu, jednak na člověka působí dojmem, že to všichni se snahou, aby nebyli považováni za zlo, jaksi přehánějí.* Nemůžu dost dobře říct, zda je to sen, nebo noční můra.

Když se setkávám s člověkem jménem Corey Louie, jenž pracuje v Googlu na pozici manažera důvěry a bezpečnosti, uleví se mi, protože lidé, kteří se věnují problematice bezpečností, nenosí růžové brýle a nemají sklony k mlčenlivosti bez ohledu na to, pro koho pracují. Jeho způsoby jsou vítaným kontrastem googlovských vibrací buddhistické jednoty. Louie je bystrý Američan asijského původu, třicátník, s živým a vřelým chováním. První odborné zkušenosti nezískal mezi do sebe zahleděnými lotofágy v Silicon Valley, ale v daleko drsnějším a mužnějším světě

* Don't be evil" (Nebuďme zlem / Nebuďme za ty špatné) je neformální heslo Googlu, které vymysleli na schůzi dva jeho zaměstnanci.

amerických tajných služeb. Google ho rekrutoval dva a půl roku před mou návštěvou, tedy na konci roku 2006. Před svým odchodem šéfoval v americké Tajné službě jednotce kybernetického zločinu. Není snad nic, co by nevěděl o útocích na sítě (o tzv. průnicích), o podvodech s kreditními kartami, o velmi rozšířených útocích typu DDoS (Distributed Denial of Service, distribuovaném odepření služby), které mohou za pády a nedostupnost webových stránek a sítí, nebo o malwaru, který se v novém tisíciletí rozmnožil jako krysy v kanále. A skvěle se vyzná i v obchodování s čísly karet (tedy, jak se říká v žargonu, v kartování – carding), denním to chlebu kyberzločinu. Při kartování se nakupují a prodávají ukradené nebo hacknuté citlivé informace o platebních kartách, kterých hackerům rukama projdou stovky tisíc a jež jsou následně zneužívány k nákupu zboží nebo k výběru hotovosti z bankomatů.

Mohl snad Google odolat možnosti získat strategickou výhodu, již Corey Louie představoval pro firmu? Nemohl. A mohl snad Louie odolat strategickému kariérnímu přestupu ke Googlu? Jen uvažte: mírné počasí amerického jižního Pacifiku kontra vlhký Washington DC, jeho zimní chlad a pouhopouhý jeden týden provoněný kvetoucími třešněmi; neformální styl oblékání západního pobřeží, nebo škrobené límečky Beltwaye; peníze a pocit, že jste součástí dynamického projektu, nebo americká vládní služba? Tohle nebyl moc vyrovnaný souboj.

Když jedete ze San Franciska po dálnici číslo 101, Google není zdaleka jedinou počítačovou firmou, na niž narazíte. Cestou na jih minete také ústředí Sun Microsystems, Yahoo! nebo třeba McAffee. Čím více firem navštívíte kvůli kybernetické bezpečnosti, tím více potkáte i vládních agentů – narazíte na někdejší pracovníky FBI, NSA, CIA, Protidrogového úřadu či Americké poštovní inspekční služby. Z nepřitažlivého prostředí Washingtonu DC odletěla do Silicon Valley za lepším životem celá hejna bývalých policistů či tajných agentů. Zlákaly je stejné skvělé podmínky, jaké přivedly film do Hollywoodu.

Odliv hlav ze státních agentur do privátního sektoru způsobuje vládám (nejenom té americké) nesporné ztráty. Stát pumpuje peníze do vzdělání kybernetických vyšetřovatelů, ti pak po letech, kdy pod hlavičkou státních úřadů získali potřebné zkušenosti, odcházejí za lepším do příjemnějších krajin. Nicméně tyto investice nejsou tak úplně střelbou do tmy, protože s jejich pomocí vznikají i silné vazby mezi veřejným a soukromým sektorem. Google není jen čistě soukromou firmou; v očích Bílého

domu představuje určitý strategický přínos. Zpráva z DC je dost jasná – zaútočte na Google a útočíte i na Bílý dům. Když někdo jako Corey Louie zvedne telefon a zavolá svým starým známým do tajných služeb, že došlo řekněme k velkému útoku na Gmail, spolupráce mezi veřejným a soukromým sektorem v oblasti internetové bezpečnosti je pak mnohem snazší.

Sice mi do toho nic není, ale vsadím se, že když se Corey přestěhoval na západ, jeho životní standard vzrostl – ale zasloužit si to musel extrémně tvrdou prací. Google je jedním ze dvou největších depozitářů dat na světě – tím druhým je Facebook. A právě z toho tyto firmy těží (inzerenti rádi zaplatí za tajemství o zvycích lidí a tyto informace se ukrývají právě v nashromážděných datech). V důsledku téže skutečnosti pak také obě společnosti představují svatý grál hackerů, ať už pracují na vlastní pěst, ve službách podsvětí, firem nebo znepřátelených států.

Ke konci našeho rozhovoru mi Corey řekl, že jeden jeho kamarád policista investoval spoustu času do vybudování přátelských vztahů s hackery. Spřátelil se s nimi do takové míry, že z něj nakonec udělali správce rozsáhlé webové stránky věnované kyberzločinu. „Dost možná si s tebou rád popovídá," řekl. „Vedl stránku zvanou DarkMarket (Temný trh)." To bylo poprvé, kdy jsem slyšel o stránce takového jména i o zvláštním agentu FBI Keithovi J. Mularském. Byl to začátek zvláštní cesty.

Naplánoval jsem si, že se setkám a promluvím si s co možná největším počtem aktérů, kteří v historii DarkMarketu hráli ústřední roli. Zloději, policajti, dvojití agenti, právníci, hackeři, crackeři a různí další kriminálníci ještě prozaičtějších jmen byli rozptýleni po dvanácti státech světa. Studoval jsem i objemné svazky soudních dokumentů souvisejících s webem DarkMarket a snažil se komunikovat se všemi, kdo v nich figurovali. Další dokumenty a informace jsem získal od bývalých či současných kyberzločinců a policistů. Nepodařilo se mi sice získat přístup ke kompletnímu archivu samotné webové stránky, ale nakonec jsem sehnal jeho podstatnou část. Ten jediný, kdo má kompletní archiv u sebe a kdo dohlížel na veškerou dokumentaci vztahující se k DarkMarketu, je agent Mularski.

Když pomineme nekompletní archiv, některé z předložených důkazů – ač určitě nikoliv bezvýznamných – byly nepřesné; týká se to obzvláště materiálu, který žalobci předkládali při mnoha soudních líčeních. Podle mého názoru nebyly tyto nepřesnosti výsledkem nedbalosti nebo pomstychtivosti. Spíše odrážely vysoce technický a často komplikovaný

charakter důkazů, jež figurovaly v soudních řízeních vedených kvůli počítačové kriminalitě. Soudci a státní zástupci zápasili i se samotným slovníkem této specifické kultury; stejně si připadají i všichni ostatní, když se s internetovou kriminalitou setkají poprvé.

Jádro příběhu se každopádně točí kolem zúčastněných osob a jejich činů. Svědectví se samozřejmě z velké části zakládají na osobních vzpomínkách aktérů, roztroušených po období dlouhém více než deset let. Pod tradičním klamem vzpomínek si všichni z nich přihřívali vlastní polívčičku, některé své aktivity v souvislosti s DarkMarketem vyzdvihovali, jiné zatajovali. V tom jim pomáhala samotná podstata internetové komunikace, kultura, v níž proti lhaní a zatajování snad neexistuje žádná účinná obrana.

Mé pokusy odhadnout, kdy dotyčný lže, přehání nebo fantazíruje a kdy upřímně říká pravdu, byly úspěšné jen částečně. Každý, s kým jsem se bavil, překypoval inteligencí, třebaže některým z nich scházela pevná ruka na morálním kormidle – jinak by se ostatně v neklidných vodách kybernetické kriminality nedokázali vůbec pohybovat. Avšak jak jsem se nořil do podivného světa Temného trhu hlouběji a hlouběji, začal jsem si uvědomovat, že různé verze týchž příběhů v srdci této webové stránky si každopádně protiřečí. Není možné říct, co přesně se mezi aktéry odehrávalo a kdo nakonec pro koho dělal, ale všichni pravdu určitě nemluví.

Internet dal vzniknout nesmírnému množství dat a informací, z nichž je velká část naprosto bezcenná, podstatná část zůstává nadále neprozkoumaná a malé procento je ve své věrolomnosti nebezpečné. Naše sílící závislost na zasíťovaných systémech je však sama o sobě důvodem, proč se snažit pochopit fenomén DarkMarket. Stojí za to sledovat, jak se velice specializované skupiny typu hackerů a tajných agentů pohybují mezi zločinem, průmyslovou špionáží a kybernetickými konflikty, a to i přesto, že důkazy jsou jen částečné, tendenční a roztroušené jak ve virtuálním, tak i reálném světě.