Daniil Turovskij

Stručné dějiny ruských hackerů

PISTORIUS & OLŠANSKÁ

Hackerství se pro naši civilizaci stává stále nebezpečnější hrozbou. S rostoucím významem internetu v organizaci společnosti, komunikacích, hospodářském životě a technologických systémech roste také nebezpečí jeho zneužití či napadení. Svět již zažil a stále zažívá vykrádání bank, vydírání nemocnic, umlčování politických oponentů, útoky na servery hospodářské konkurence, ovlivňování voleb i zablokování dodávek elektřiny v rozsáhlých regionech. Jsme svědky toho, jak se internet stává polem nejen finanční kriminality, ale i prostředkem boje teroristických organizací či vojenských a bezpečnostních struktur některých států. Hackerství rovněž přineslo nevídané možnosti, jak prostřednictvím mobilních telefonů sledovat prakticky kohokoliv. A všechna tato nebezpečí jsou při tom mnohem vážnější, než si většina z nás uvědomuje. I proto vznikla fundovaná kniha Daniila Turovského, jež čtenáři otevírá bránu do světa virtuálních hrozeb. Její autor je novinář, který se dlouhodobě zabývá hackerstvím v Rusku. Opírá se o analýzu dostupných materiálů a řadu vlastních rozhovorů s předními hackery a ve své knize ukazuje vývoj tohoto fenoménu i sociální a politické faktory, které umožnily, že ruští hackeři dnes patří k nejaktivnějším a nejnebezpečnějším. Poukazuje při tom také na praxi ruských silových struktur – armády a FSB –, jež připravují hackerské specialisty, úkolují je a začleňují do nových vojenských a bezpečnostních jednotek či tiše zajišťují beztrestnost „vlasteneckým" kyberzločincům. Turovského *Vpád* je knihou, která je stejně tak objevná, jako i potřebná.

Daniil Ivanovič Turovskij (1990) vystudoval moskevský Institut žurnalistiky a literární tvorby. Pracoval jako redaktor a korespondent různých tištěných i internetových časopisů (*Kommersant*, *Afiša*, *Meduza*, *Lenta.ru*), specializující se na problematiku internetu a hackerství. V roce 2015 napsal také seriál reportáží o Islámském státě, které přetiskoval britský *The Guardian*.


PISTORIUS

Daniil Turovskij

VPÁD

Stručné dějiny ruských hackerů

Z ruštiny přeložil Libor Dvořák

Pistorius & Olšanská
Příbram 2021

Tato kniha byla vydána s laskavou pomocí Ministerstva kultury ČR.

ISBN 978-80-7579-125-2 (PDF)
ISBN 978-80-7579-091-0 (tištěná kniha)

Mým rodičům – za to, že mě naučili zvědavosti

Předmluva

Dějiny ruských hackerů jsou dějinami výrostků z celého bývalého Sovětského svazu. Vyrůstali v inženýrských rodinách, v mládí četli kyberpunk a sci-fi, po tržištích nakupovali klony počítačů IBM – a najednou se ocitli na hackerských fórech, jež jim často vynahrazovala smutný ruský život za okny: s jeho špinavými ulicemi, bídou i vyprázdněnou a děsivě nepředvídatelnou budoucností.

Zatímco v USA se dál a dál nafukovala dotcomová bublina, hackeři v Rusku nastartovali svou vlastní zlatou horečku – kradli americké kreditky, nabourávali se do bankovních účtů a internetových obchodů a mnozí z nich se tak dopracovali až milionů dolarů. Leckdo z nich je v obavách z gangů či státu pečlivě ukrýval a proměňoval v květinářské obchody či pneuservisy, jiní nakupovali vily a drahé sporťáky, další si opatřovali nemovitosti v zahraničí a odjížděli tam, kde byly barvy výraznější než ty, jimž uvykli doma – na Maledivy, na Kypr či do Izraele.

Životopisy těchto lidí nejednou připomínají napínavé akční filmy. Když jsem s nimi mluvil o jejich minulosti, často jsem z toho měl pocit, že veškeré ty vylomeniny nevyváděli jen kvůli penězům, spíš jako by se snažili stát hrdiny filmů a knížek, které tolik milovali v dětství.

V mládí jsem si často četl v časopisu *Hacker*, který každou chvíli radil, jak se někam nabourat, a všechno to dost připomínalo zmodernizovanou *Anarchistovu kuchařku*. Vyrůstal jsem v rodině, kde každý měl svůj počítač a kde se pěstovalo programování: po večerech jsem zkoumal kódy webových stránek a pokoušel se na ně proniknout. Uvažoval jsem o tom, že po maturitě bych se mohl přihlásit ke studiu na fakultě informační bezpečnosti a pak

třeba pracovat u Federální bezpečnostní služby (FSB). Naštěstí mě tyhle úvahy brzy pustily a daleko víc mě začaly zajímat různé texty, historie a nakonec i novinařina.

Polotajné hackerské společenství, do nějž jsem se svého času marně pokoušel proniknout, o sobě však občas opět dávalo vědět. Nejdřív tito lidé přes sociální sítě útočili na známé a požadovali peníze. Později už se vrhali i na mé vlastní účty kvůli mé novinářské práci v Rusku – útočili na ně prorežimní hackeři.

Tohle je kniha o volbě – o cestách, jež si vybrali lidé, kteří se stali součástí hackerské subkultury. Zatímco někteří se dál drželi výhradně romantických představ a na peníze nemysleli (I. část), jiní bohatli (II. část); když pak nadešel čas uspořádat si své vztahy se státem, jedni začali pracovat pro něj, kdežto jiní proti němu (III. a IV. část).

Kniha vychází z textů, které jsem v posledních letech psal pro *Meduzu* (meduza.io), což je jeden z mála opravdu nezávislých ruskojazyčných serverů, ale nejen z nich. Většinu materiálů jsem dával dohromady ve volném čase: zkoumal jsem různá fóra, internetové archivy a knihy, setkával se s hackery nebo, a to častěji, s nimi debatoval prostřednictvím zašifrovaných chatů. Říkám těmto lidem „ruští hackeři", protože rusky mluvící hackerské společenství zůstalo jednotné: Rusové, Ukrajinci, Bělorusové i příslušníci jiných národů bývalého SSSR vyrůstali na stejných fórech, vytvářeli společná uskupení a na své cíle dál útočili společně – dokonce i tehdy, když jejich státy spolu vedly válku.

V jistém smyslu je tedy tato kniha průvodcem po světě ruskojazyčných hackerů od pádu Sovětského svazu až do dneška, encyklopedie protagonistů, či dokonce studie toho, jak ruské úřady vybudovaly jednu z nejbojeschopnějších kybernetických armád světa. Najdete tu mnoho individuálních lidských příběhů, z nichž

si uděláte obrázek, v jakých podmínkách tito hackeři vyrůstali a co určilo jejich další osud.

A konečně je to také vyprávění o tom, jak anonymní jedinci sedící u počítačů dokážou znesvářit celé státy, ničit kritickou infrastrukturu (kupříkladu odpojovat elektrické rozvodné sítě v celých regionech) a zabíjet, aniž by vedli jakoukoli bojovou činnost a aniž by měli sebemenší představu, kdo jsou jejich oběti.

Prolog

První běženec kybernetické války

22. srpna 2015 vousatý obrýlený muž se dvěma batohy vstoupil do budovy Leningradského nádraží v Moskvě. Došel k pokladně a koupil si lístek na nejbližší expres Sapsan, který dojede za čtyři hodiny do Petrohradu.

Jakmile muž dorazil do severní metropole, rozběhl se k nedalekému stanovišti linkových taxíků. V Petrohradu vyrostl, a tak věděl, že mikrobus mířící do Helsinek je nejlevnější a nejméně nápadný způsob, jak se dostat z Ruska do Evropy. Jízdenka stojí 800 rublů a cesta zabere osm hodin, jež náš poutník stráví ve společnosti chudých studentů a překupníků, kteří z Ruska do Finska vezou cigarety a zpátky drogistické zboží.

Po několika hodinách muž překročil rusko-finskou hranici a konečně si s úlevou vydechl. Zatím se jeho plán dařil – pokud ho někdo sledoval, podařilo se ho setřást. Všechno si předem dobře promyslel: cestu vzduchem nezvolil, protože to by ho určitě zajistila letištní kontrola, a lístek na vlak si nekoupil přes internet, ale přímo v nádražní pokladně. Vybavil si svůj předchozí útěk ze zaběhaného života, když před deseti lety projížděl trolejbusem kolem nádraží a najednou se zcela spontánně rozhodl, že se přestěhuje ke své dívce do Moskvy. Na další zastávce vystoupil, koupil si lístek na vlak a tím odjel navždy. S tou dívkou se pak vzali.

V Helsinkách muž nasedl na trajekt do Stockholmu a po příjezdu do Švédska se obrátil na lidskoprávní organizaci s prosbou, aby mu pomohla získat v zemi politický azyl. Odtud ho ovšem poslali zpátky do Finska, podle evropského zákonodárství je třeba o politický azyl žádat v zemi, přes niž člověk na území EU vstoupil.

Po návratu do Helsinek vousáč našel nejbližší wifinu a odeslal e-mail na redakční adresu *Meduzy*, pro niž jsem tehdy pracoval jako zvláštní zpravodaj. Jeho zpáteční adresa zněla *mrtváruka1984*, což poukazovalo jak na slavnou Orwellovu antiutopii, tak i na systém Perimetr, který měl zajistit automatický odvetný jaderný úder a byl v Sovětském svazu vyvinut v časech studené války. Američané si Perimetr přejmenovali na Mrtvou ruku: celý systém byl vybudován tak, aby jaderné hlavice byly odpáleny i v případě, že by všichni, kdo to mohli učinit, byli už mrtví.

V e-mailu se muž představil jako Alexandr Vjarja, jeden z vedoucích pracovníků ruské společnosti *Qrator Labs*, která se věnovala ochraně proti DDoS-útokům. V dopisu vylíčil, jak živě se vysocí ruští státní úředníci a tajné služby zajímají o kybernetické zbraně. On sám byl svědkem toho, jak nasazení těchto zbraní nařídil právě stát.

„Dnes, kdy se situace v Rusku znovu vyostřuje, se obávám, že by mě mohli zapřáhnout do přípravy a organizace těchto útoků, protože jsem do věci zasvěcený. Rozhodl jsem se tedy, že musím veřejnost informovat," psal Vjarja. „Myslím si, že naši občané by měli vědět, na co stát vynakládá peníze v podmínkách krize. A KDO se těmihle špinavými záležitostmi zabývá. Rozhodně to nejsou nějací drobní podvodníčci. A zatímco dřív jsme to všichni jen tušili, teď budete mít důkazy:) Ze země jsem musel vycestovat, aby mě třeba náhodou nepřejelo auto. To rozhodnutí nebylo snadné: dá se říct, že jsem ztratil dobrou práci i rodinu, od které jsem se vydal do neznáma. A to nemluvím o tom, jak mě budou pronásledovat všelijaké novinářské prodejné děvky – například z *Lifenews*."

Odpověděl jsem, že bych se s ním rád sešel a jeho příběh vyslechl co nejdřív. Naše debata se okamžitě přestěhovala do tajného

chatu v Telegramu. V roce 2015 už chráněné chaty v Rusku používal kdekdo, protože bylo jasné, že otevřenou komunikaci můžou číst nebo odposlouchávat ruské tajné služby, i když podle zákona musí k něčemu takovému nejdřív získat povolení soudu.

„Jak rychle se sem dostanete? Hodlám vše oznámit zdejším úřadům a požádat je o pomoc," napsal mi.

„Stačí pozítří?"

„Ajaj!"

„Připadá vám to pozdě?"

„Ačkoli, stejně se musím někde ubytovat."

„Mohl bych to zkusit i zítra."

„Potřeboval bych si najít něco šikovného, na kartě už mi zbývá jen pár krejcarů."

Nakonec si Vjarja našel společný pokoj v jednom z místních hostelů. Helsinky jsou drahé město, ale měl štěstí a za noc platil jen 20 euro. Když už jsem příští ráno nasedal do letadla, dostal jsem od něj další zprávu: „Naprosto nesdělitelná experience – hostel jsem zažil úplně poprvé. Všichni tu chrápou, mluví ze spaní a celou noc se převalují."

Brzy nato jsme se setkali u nákupního centra kousek od nábřeží. Vjarja stál vedle vchodu, neklidně se rozhlížel a očima po mně pátral mezi lidmi přecházejícími tramvajové koleje. Všechny své věci – dva batohy – měl s sebou. Zašli jsme do nejbližšího podniku, objednali si kávu a on mi začal vykládat, co všechno se mu přihodilo.

* * *

Alexandr Vjarja se narodil v polovině 80. let ve společném bytě v Leningradu a vyrůstal bez otce. Když mu bylo dvanáct, zahořel pro počítače – začínal videohrami, posléze se věnoval

programování a „železu“, tedy počítačovému hardwaru. Jeho prvním zaměstnáním byla funkce systémového správce sítě ve společnosti jeho vzdáleného strýce. Sociální sítě se teprve začínaly rodit, ale Vjarja si v nich účty nezřizoval zcela programově: nechtěl po sobě na internetu zanechávat žádné stopy.

Když se přestěhoval do Moskvy, nějaký čas působil jako síťový inženýr v několika hostingových společnostech. Roku 2012 objevil na jednom z profilových fór zajímavou pracovní příležitost a po několika testech ho přijali do společnosti *Qrator*, specializující se na ochranu proti útokům typu DDoS.

Ta v té době byla na trhu ve svém oboru naprostou špičkou: mezi jejími zákazníky byla četná nezávislá média jako *TV Dožď* či listy *Novaja gazeta* a *Vědomosti*, bankovní domy (Alfa, Tinkoff) či internetové obchody (Julmart, Lamoda). Jak Vjarja tvrdil, jejich služeb jednou využil dokonce i internetový obchod prodávající sudy z cedrového dřeva. Nejzajímavější na tom bylo, že právě tento obchod zažil nejtěžší hackerský útok za celou dobu jeho práce u společnosti. „V Rusku je zúčtování s konkurencí za pomoci útoků typu DDoS velmi populární, protože už jednodenní prostoj může znamenat uzavření obchodu,“ vysvětlil mi. Takové útoky jsou velmi levné (kolem tří tisíc rublů denně) a nechráněnou webovou stránku vyřadí z provozu, což vede k významným ekonomickým ztrátám.

Vjarja pracoval v technické podpoře a neustále odpovídal na dotazy klientů. Nejednou se na *Qrator* obraceli i ti, kteří byli nespokojení s tím, že firma chrání i opoziční servery. Na jaře 2012, těsně před Putinovou prezidentskou inaugurací „vlastenečtí“ prorežimní hackeři zaútočili na webové stránky rádia *Echo Moskvy*, listu *Kommersant* a *TV Dožď*. To všechno byli zákazníci *Qratoru*. „Proč chráníte Židy?“ zeptal se Vjarji toho dne jeden z volajících.

Během voleb moskevského primátora v roce 2013 *Qrator* chránil web Alexeje Navalného – hned od okamžiku, kdy tento opoziční politik ohlásil svou kandidaturu a zahájil úspěšnou kampaň. Jednoho dne si Vjarja povšiml, že vedle sídla jeho společnosti stojí dodávka s tmavými okny a anténami na střeše. Od té chvíle se tam auto objevovalo skoro každý den. Když pracovníci *Qratoru* odcházeli na oběd, pokoušeli se do auta nahlédnout a žertovali, že by těm, kdo je odposlouchávají, měli přinést něco na zub.

„Saša je velmi nadaný chlap, ale dost vztahovačný a už mu trochu straší ve věži," řekl mi jeho bývalý šéf Alexandr Ljamin. „Když ve sféře informační bezpečnosti pracujete příliš dlouho, začínáte se měnit a ze všech stran se cítíte ohroženi."

Ať tak či onak, v roce 2015 vedení firmy Vjarju povýšilo na vedoucího provozních služeb. Začal často jezdit do zahraničí, navštěvovat datová centra a instalovat v nich programové vybavení schopné odolávat mimořádné zátěži při případných útocích. V *Qratoru* se takovým serverům říká „centra očisty provozu". Tato zařízení pomáhají obehnat webové stránky zákazníků virtuálním „plotem" s „hraničními přechody", jež jsou pak s to odfiltrovat zdravý provoz od kontaminovaného.

Ve stejné době firma připravovala otevření první zahraniční filiálky v Praze. Všichni její pracovníci už dostali služební víza. V čele této expozitury měl stát právě Vjarja.

3. října 2015 zavolal generálnímu řediteli *Qratoru* Alexandru Ljaminovi zástupce ředitele oddělení infrastrukturních projektů ruského ministerstva spojů Vartan Chačaturov. Ten Ljamina požádal, zda by někdo z jeho odborníků nepomohl ministerským úředníkům vyřešit jeden „choulostivý problém". Kromě Vjarji nebyl v tu chvíli k dispozici nikdo – všichni ostatní se rozjeli po odborných konferencích.

Chačaturov se tedy s Vjarjou spojil a poskytl mu mobilní číslo, na které Vjarja odeslal zprávu. K večeru se mu ozval jistý Vasilij Brovko. Vjarja neměl ponětí, kdo to má být. Brovko mu sdělil, že by spolu během pár dní měli odcestovat do bulharské Sofie a že všechny potřebné formality zařídí jeho asistentka.

Vjarja si tedy Brovka našel na internetu – a chytil se za hlavu. Nejvíc ho přitom zaujalo, že Brovko byl zakladatelem společnosti Apostol, již Alexej Navalnyj na jaře 2013 obvinil, že za pomoci botů napadala sociální sítě Aeroflotu. Poslední dobou tento muž působil ve funkci šéfa oddělení komunikací Rostechu, tedy státní korporace pověřené vývojem a výrobou hi-tech produkce pro civilní i vojenské účely. Tuto instituci řídil Sergej Čemezov, jenž měl velmi blízko k Vladimiru Putinovi.

Vjarja předpokládal, že potřebují pomoc v jeho oboru – tedy vybrat nový systém ochrany před DDoS-útoky. Velmi ho proto překvapilo, že má cestovat do Bulharska, když nejznámější výrobci podobného programového vybavení sídlí v Izraeli a ve Státech.

5. února 2015 nicméně přicestoval do Sofie. Brovkovi zaslal SMS a ten mu odpověděl, že schůzka se uskuteční někdy během odpoledne. Vjarja se tedy prošel po centru města a pak zamířil k místu schůzky, což byla skleněná pompézní budova Grand Hotelu Sofia.

Zanedlouho se objevil i Brovko. V jedné ruce svíral smartphone ruské výroby, kdežto v druhé iPhone. Oba telefony byly v neustálém provozu. Vjarja se s Brovkem pozdravil a prohodil, že Sofie je neuvěřitelně malé město. „Spíš smetiště," utrousil Brovko.

Hned poté se dostavili dva pracovníci místní společnosti *Packets Technologies* (internetová stránka[1] firmy skromně sděluje, že se společnost specializuje na „vývoj pokročilých síťových

technologií“). Brovko Vjarjovi řekl, že teď musejí zajít do sídla společnosti, „podívat se na produkt“ a poté Vjarja řekne, co si o něm myslí.

Společnost sídlila kousek od hotelu. V jednací místnosti firmy spustil jeden z pracovníků *Packets Technologies* prezentaci a během ní o sobě řekl pár slov: působil v izraelské armádě, konzultoval největší internetové firmy v oblasti síťové bezpečnosti a zúčastnil se i *Black Hat* (což je nejdůležitější celosvětová konference o informační bezpečnosti, na kterou přijíždějí jak oficiální odborníci na IT, tak i hackeři).

Poté pracovník bulharské firmy podle Vjarjova tvrzení prohlásil: „A teď vám představím produkt sloužící k provádění DDoS útoků.“ Zmíněný program neměl žádný název. Bulhar dále zdůraznil, že „produkt“ je schopen zajistit DDoS útok na síťové úrovni. Takové útoky „ucpou možnosti serveru parazitními pakety, takže systém nedokáže přijímat žádná další data“.

Produkt měl podobu malé krabičky s programovým vybavením, která se instalovala na jeden z výměnných uzlů. Pro systém bylo vyčleněno zvláštní pásmo s maximálním výkonem 10 gigabitů za sekundu. Odborníci z *Packets Technologies* k řečenému dodali, že systém umožňuje tzv. koktejlové, tedy smíšené útoky, jimž je vůbec nejtěžší čelit. Mimoto se datový tok dá docela jednoduše posílit instalací další „krabičky“. Roku 2010 byl podobný útok o síle 10 gigabitů veden proti serverům *Wikileaks*. Nejmohutnější DDoS útok v dějinách internetu podnikla nizozemská hostingová firma *Cyberbunker* proti společnosti *Spamhaus* – ten měl sílu 300 gigabitů/s,[2] a jak napsaly noviny *The New York Times*, „zpomalil celý internet“.

Když pracovník společnosti ukončil teoretický výklad, spustil VPN-spojení a prohlížeč v Toru, čímž si zajistil anonymitu (vysledovat počátek takového útoku je prakticky nemožné). V prohlížeči

zadal IP-adresu a otevřela se stránka s mimořádně jednoduchým rozhraním. Nahoře byl adresový řádek a pod ním asi deset variant DDoS-útoků. Vedle každé z nich bylo prázdné políčko, které jste mohli označit. Dole knoflík, jímž se dala navolit síla útoku – od 100 megabitů do 10 gigabitů za vteřinu. „Nemusí to jet takříkajíc na plné pecky, samozřejmě pokud oběti útoku stačí méně masivní zásah," vysvětlil Vjarja.

Pracovníci firmy vepsali do vstupního pole adresu serveru ukrajinského ministerstva obrany. Ve vedlejším okně pak otevřeli stránku služby, s jejíž pomocí se dala sledovat funkčnost webových stránek. Pak svůj program spustili na plný výkon. Objevil se i graf ukazující sílu útoku – ta velmi rychle dosáhla 10 gigabitů/s. Indikátor funkčnosti ukázal, že stránka je nepřístupná. Pokusili se ji tedy otevřít v prohlížeči, ale ani to nevyšlo. Během pár minut útok zastavili a stránka znovu začala odpovídat.

Pak se pokusili na stránku ukrajinského ministerstva obrany zaútočit výkonem 100 megabitů/s a ta znovu přestala fungovat.

„Víte co, zkusíme slon.ru," navrhl Brovko, který až do této chvíle mlčel (alespoň tak mi to tlumočil Vjarja). *Slon.ru* (přejmenovaný dnes na *Republic*) je jeden z nejpopulárnějších ruských nezávislých zpravodajských a informačních serverů a právě na ten Bulhaři na požádání zaútočili výkonem 10 gigabitů/s. Stránka se neotevřela a na několik minut spadla. Později mi tehdejší šéfredaktor „slona" Maxim Kašulinskij potvrdil, že 5. února 2015 zaznamenali útok, po kterém jejich stránka na dvě minuty spadla.

„A co když ty stránky jsou chráněné? Prorazíte ochranu?" zeptal se Vjarja a dostal odpověď, že v takovém případě je třeba zjistit skutečnou adresu serveru (protože všechny ochranné systémy nechají útok proběhnout, ale skutečnou adresu serveru zamaskují), jenže na to prý *Packets Technologies* mají svou meto-

diku. Vjarju zajímalo, kolik takový systém stojí, a Brovko mu údajně odpověděl: „Asi tak milion dolarů."

Po této schůzce Vjarja s Brovkem zamířili zpátky do Grand Hotelu Sofia a v baru si objednali kávu. Vjarja si vybavil, že Brovka ze všeho nejvíc zajímalo, jak se dá najít skutečná adresa serveru a na jaké vstupní pole by bylo nejlepší takovýto systém využít. Po jisté chvíli měl pracovník Rostechu říct: „No to víte, potřebujeme někoho, kdo by s tím byl schopen zacházet." Vjarja jen polkl a prohlásil: „Tak to ne, prosím! Uvědomte si laskavě, že nejsem hacker. Něco takového je proti mým zásadám, a navíc je to nezákonné." Nato se Brovko měl Vjarji zeptat: „A víš ty vůbec, jaká organizace tě na tenhle výlet pozvala?" Vjarju hned napadlo, že by to mohla být Federální bezpečnostní služba (FSB), ale nahlas řekl, že napříště je ochoten zabývat se jen čistě technickými záležitostmi celé věci. Přidali si jeden druhého do *Telegramu* a rozešli se.

Vjarja se nijak netajil tím, že tohle ho opravdu šokovalo. Vše ihned sdělil svému šéfovi Ljaminovi a ten mu doporučil, aby se „pokud možno držel stranou". Nazítří, 6. února, se Vjarja vrátil zpátky do Moskvy.

Vjarja mi poskytl záznamy své další korespondence s Brovkem i se svými nadřízenými. Pracovníkovi Rostechu zaslal několik zpráv obsahujících čistě technická doporučení: kupříkladu doporučil, aby pro tento účel použili nizozemské výměnné uzly, které „mají terabitový výkon a nějakých deset gigabitů je nerozhodí". Odpověděl mu stručně: „Díky, podívám se na to."

5. března 2015 Vjarjovi napsala Brovkova asistentka a sdělila mu, že ho prosí o schůzku: „Na Patriarchových rybnících. Ne v konkrétním podniku, bude to jen taková procházka." Po pár hodinách Vjarja odepsal, že takovou věc je třeba projednat s jeho nadřízenými. A to už mu odpověděl sám Brovko:

Nazdar. Přece jsme se domluvili, že se občas setkáme bez vědomí tvých šéfů.
Šlo by to dneska?

Vjarja:
Nazdar.
Šéf prosí všechno řešit přes něj.
Záleží na něm.

Brovko:
Ale!!!
A proč?

Vjarja:
Nemá rád, když ho obchází. Obyčejně mu zavolá Vartan [Chačaturov] a všechno proberou spolu. Já jsem jen podřízený a bez něj to nejde.

Brovko:
Tak mu řekni, že jdeš jenom na kafe.

Vjarja:
Bohužel nemůžu:(

Brovko:
S tím nesouhlasím, ale budiž.
Pošli číslo na šéfa.

Ljaminovi se to vůbec nechtělo líbit. Otevřel v *Telegramu* chat s názvem WTF a pozval do něj Vjarju, Brovka a Chačaturova.

Ljamin:
Zdravím, kolegové.
Kdybych řekl, že mám šílený vztek, tak jsem řekl málo.

Chačaturov:
Ahoj.

Ljamin:
Vždycky ti rád pomůžu, Vartane, a ty to víš. Když ale někdo začne lézt za mými kolegy bez mého vědomí, JSEM PROTI.

Chačaturov:
Popravdě řečeno jsem si myslel, že je to jednorázová akce:)

Ljamin:
Přistoupil jsem na to, že vám pomůžeme se Sofií. Nic víc a nic míň.
Žádnou další „kreativu" jsem neschválil.
[…]
Očekáváme komentář a vysvětlení od Vasilije Brovka.

Chačaturov:
Hlavně klid, kolegové:)

Ljamin:
Já prostě klidně zuřím.
Takhle se gentlemani nechovají.

Brovko:
Nechápu, o čem je tu řeč. Denis [Vjarja neví, kdo to je – pozn. aut.] mi řekl, že můžete poskytnout consulting ve velmi choulostivé otázce. Ale když ne, tak ne.

Chačaturov:
Vasiliji, Denis asi neřekl, že je to dlouhodobější věc, a ne jednorázová výpomoc:)

Brovko:
To je jednorázová výpomoc, stačilo by 15 minut.

Chačaturov:
Ale v takovém případě to není problém, řekl bych, Sašo.

Ljamin:
Nevěděl jsem, že je to čtvrthodina, a dál nevím, k čemu by byla dobrá.

Chačaturov:
Tak to s tebou prostě musíme dojednat.

Ljamin:
V každém případě je to můj zaměstnanec, kterého za jeho práci platím já.
Tak o čem je řeč?
Kontakt na mě máte, tak se obracejte na mě.
Tady nejde o čtvrthodinu. Tady jde o to, že chcete něco po lidech, kteří jsou na mé výplatní listině, a mě klidně obcházíte. To je nepřípustné!

Chačaturov:
No dobře, Sašo, uklidni se prosím. Ber to jako nedorozumění, už jsme to nějak zvládli:)

Ljamin:
Doufám, že jste rozuměli a berete si to k srdci.

Podle Vjarji už se na něj ani Brovko, ani další lidé z Rostechu znovu neobrátili.

* * *

Napsal jsem Vasiliji Brovkovi na jeho číslo v *Telegramu*, z kterého Vjarjovi navrhl, aby se sešli a projednali možnosti kybernetických útoků. Prakticky vzápětí odpověděl, že „v Bulharsku byl, aby s kolegy analyzoval možnosti antikybernetické ochrany, a ne počítačových útoků". A pokračoval: „Obvinění za hranicemi zdravého rozumu a zcela mimo realitu komentovat nehodlám. Rostech je kybernetickým útokům vystaven neustále – od počátku tohoto roku jich na podniky naší organizace mířilo už více než 11 tisíc."

Vjarjův šéf Alexandr Ljamin mne pozval do sídla *Qrator Labs*. Vyklubal se z něho veselý, výřečný vousáč v keckách a pestrobarevném tričku a vzápětí mi potvrdil, že Vjarja na schůzku s Brovkem odcestoval na žádost pana Chačaturova z ministerstva spojů: „Původně se ale nemluvilo o systému DDoS-útoků, nýbrž o generátoru datového provozu, tedy zařízení nezbytném ke kontrole zátěžové odolnosti serverů," řekl Ljamin. „No jistě, nejspíš to byla salva vypálená na slon.ru. Pokusná, kontrolní. Že je to nelegální? Jde přece o šedou zónu…"

Ljamin také vyslovil předpoklad, že jeho firma se Vjarji mohla něčím dotknout, a je možné, že líčením příběhu s Rostechem plnil úkol od Laboratoře Kasperského, což je jejich hlavní konkurent. „Ve Finsku se dolary vždycky můžou hodit," usoudil a poskytl mi odkaz[3] na materiál *Reuters* o tom, že Kasperskij

volá po „kráglování konkurence“. K tomu ovšem také dodal, že Vjarja mu nepřipadá „úplně zdráv“.

Na jaře 2015 pracovníkům *Qratoru* vyřizovali papíry pro práci v zahraničí, konkrétně v České republice. Vjarja s rodinou se z nájemního bytu v Čertanovu přestěhoval do Birjuleva, aby před odjezdem do zahraničí ušetřil nějaké peníze.

Koncem května Vjarja hned vedle sídla firmy objevil známou dodávku s tmavými skly a anténami, která už se tu objevila v době, kdy *Qrator* poskytoval své služby serveru Navalného. O pár dní později zaznamenal stejné auto. Vjarja sám říká, že ho „popadla paranoia“: měl kupříkladu dojem, že v různých částech města potkává stále stejné lidi, pročež se rozhodl do práce jezdit pokaždé jinudy.

Na konci července ve firmě nadřízeným sdělil, že do Česka odjet nemůže – žena je údajně proti. Ljamin ovšem přesto trval na tom, aby pracovníci jeho firmy měli evropské dokumenty. Vjarjovi tedy poradil, aby si povolení k pobytu opatřil ve Finsku, kde měl z otcovy strany příbuzné. V tomto případě ale musel složit zkoušku z finštiny. Vjarja si tedy vzal dovolenou, aby měl čas na patřičnou jazykovou přípravu.

Zároveň mu, jak sám tvrdil, známí sdělovali, že se o něj dál zajímají lidé z Rostechu a tajných služeb, aby ho konečně získali pro práci s kybernetickými zbraněmi – když už je viděl v provozu. Vjarja si byl každopádně jist, že přesně takhle to dopadne – anebo mu někdo „rozkřápne kebuli“.

V srpnu 2015 mu přátelé se styky v tajných službách poradili, aby z Ruska vycestoval. A tak si hned nazítří sbalil to nejnutnější do dvou batohů a odjel do Helsinek.

* * *

Brzy ráno 25. srpna 2015 jsme s Vjarjou dorazili k helsinské policejní stanici, kde měl oficiálně požádat o politický azyl. Byla ještě zavřená a přede dveřmi čekalo pár iráckých uprchlíků. Po krátkém výslechu a sejmutí otisků prstů Vjarju odeslali do jednoho z místních uprchlických táborů, což byla dvoupatrová budova skoro v centru města, v níž se dalo zajít do bezplatné jídelny. Po domě a jeho okolí chodily desítky Iráčanů a Syřanů, kteří neustále telefonovali.

Když se Vjarja ubytoval, seznámil se s jedním čečenským uprchlíkem. Ten mu poradil, aby si hlavně hlídal své vyprané věci, protože se tu hrozně krade. Další den potkal dvojici ze Sibiře, která doma čelila trestnímu stíhání, a hned nato i inteligentního synka jakéhosi egyptského ministra. Po třech dnech z tábora odvezli do nemocnice muže s podezřením na malárii. Čtvrtý den po velkém výslechu, vedeném pracovníky migrační služby, Vjarjovi řekli, že bude nejspíš převezen do uprchlického tábora 600 km severně od Helsinek, kde bude čekat na definitivní rozhodnutí migrační služby.

A přesně tak to taky dopadlo. Poté půldruhého roku putoval z tábora do tábora a byl zván k dalším a dalším pohovorům. Po celé zemi se v zásadě mohl pohybovat zcela volně a navíc mu poskytli finanční příspěvek, který na život sice s bídou, ale stačil.

O jeho případ se přirozeně začalo zajímat ukrajinské velvyslanectví a Vjarja při setkání s diplomaty vylíčil, jak útok na server ministerstva obrany Ukrajiny probíhal. Rostech a ruské vyšetřovací orgány na jeho prohlášení nijak nereagovaly.

* * *

Koncem prosince 2016 vyšla na první straně *The New York Times* poznámka o Vjarjovi, vycházející z materiálů, které jsem

připravil pro *Meduzu* (později noviny za sérii článků o současném Rusku včetně toho mého obdrží Pulitzerovu cenu). On sám je tu označen za „elitního hackera". To Vjarju zarazilo, a tak mi napsal: „Kurva, jaký elitní hacker?! Co to plácají?!" Krátce poté, co článek vyšel, si ho k výslechu už kdoví pokolikáté pozvaly finské tajné služby a hlavní dotaz byl jasný: co ví o ruských hackerech a nedávném útoku na finskou energetickou soustavu.

V létě 2017 Vjarja konečně získal politický azyl ve Finsku. Počátkem září, tedy dva roky po jeho útěku z Ruska, jsme si dohodli schůzku. Nepoznal jsem ho: zhubl o dvacet kilo a působil dojmem člověka, který se konečně zbavil břemene, jež ho tak dlouho trýznilo.

Vjarja mi vylíčil, že půldruhého roku ve finském migračním systému pro něj nebyla žádná procházka růžovým sadem. Dokonce chtěl spáchat sebevraždu, ale přátelé zasáhli včas a odvezli ho do nemocnice, kde strávil několik dalších týdnů. Peněz měl málo, s rodinou také nedokázal navázat spojení a plno času trávil u výslechů – jeho jedinou útěchou bylo rybaření, za kterým na kole vyrážel často na celý den. V uprchlických centrech byli jeho sousedy převážně Iráčané a Syřané, prchající před Islámským státem. Většina z nich brala antidepresiva a mnozí měli různá zranění. Vjarju často považovali za pracovníka tábora.

Nakoupili jsme si pivo a bylinný likér a vypravili jsme se k jednomu jezeru na okraji Helsinek: někde se dočetl, že tu skvěle berou ryby. „Jsem tu už jako doma. Všechno mi tu vyhovuje, včetně klimatu. Jako bych ani nebyl v emigraci, pro mě je to zkrátka nový život." Otevřel plechovou krabičku, pohrabal se v háčcích a za chvilku už nahodil.

* * *

Několik týdnů po schůzce s Vjarjou jsem v jedné moskevské kavárně zaslechl povědomý hlas. Otočil jsem se a uviděl bývalého Vjarjova šéfa Alexandra Ljamina. Zrovna komusi poskytoval rozhovor a nejdřív mě nepoznal: když jsem pozdravil, uhnul pohledem. Když ale odcházel, pozdravil jsem ho ještě jednou: ukázalo se, že když jsem zdravil poprvé, pomyslel si, že třeba mluví moc nahlas a ruší mě v práci.

Pak mi řekl, že je moc rád, že Vjarjovi se přece jen podařilo získat finské papíry. K tomu ještě podotkl, že většina pracovníků jeho společnosti už se přestěhovala do Prahy, odkud se bezpečnost před kybernetickými útoky zajišťuje mnohem pohodlněji. Když už se naše debata chýlila ke konci, zeptal se mě: „Co si myslíš o celé té historii s Michajlovem, FSB a vlastizradou?“ (Krátce předtím byl zatčen vysoce postavený důstojník ruské tajné služby FSB a obviněn z vlastizrady.) Jak se ukázalo, Ljamin o tom poslední dobou hodně přemýšlel.

Vjarjův příběh je jeden z nemnoha případů, kdy se člověk rozhodne otevřeně vypovídat o zájmu ruského státu a tajných služeb o kybernetické zbraně. A možná je Vjarja vůbec jediný, kdo odmítl na vývoji takové zbraně pracovat a dokázal bez vážnějších následků uniknout (pokud samozřejmě nebereme v potaz fakt, že se musel zcela vzdát svého dosavadního života včetně rodiny).

Na podzim 2017 si změnil jméno i příjmení na čistě finské, pak se přestěhoval, změnil číslo mobilu i adresu v *Telegramu*. Teď sní hlavně o tom, že si koupí velký člun, z kterého bude moci lovit lososy, pohybující se ve velké hloubce. Podobné věci dělá i v zaměstnání: práci si našel v jedné nevládní organizaci, která sleduje, jak jedny státy podnikají kybernetické útoky proti jiným státům.

Část první

Kořeny

Kapitola první

Území svobody

V roce 1992 se petrohradský mladík Kirill poprvé ocitl v prostředí trhu Junona na jihozápadním předměstí.[4] Tenhle klasický blešák vznikl už v předešlé dekádě. Kolem obchodu *Junyj těchnik* (Mladý technik) se scházeli tehdejší radioamatéři a přímo na chodník rozkládali své zboží, nabízené na prodej. S příchodem tržních časů tu vzniklo oplocené prostranství s pulty, ale sortiment zůstal podobný či úplně stejný: v podstatě se tu prodávala elektronika a příslušné náhradní díly. Populárním zbožím byly například patnáctiminutové počítačové hry na platformě Atari.

Jako mnozí jiní mladí Petrohraďané si tu i Kirill koupil svůj první počítač a okamžitě u něj začal trávit hodně času. Pár let nato odjel na nějaký čas do USA, kde zrovna začínal být populární internet. V Kalifornii Kirill otevřel svůj první webový prohlížeč. Po návratu do vlasti zjistil, že tu již vzniká domácí digitální underground a rozhodl se, že se s těmito lidmi bude dělit o své americké poznatky – například o tom, co je to WWW, FTP či IRC.

Brzy nato se Kirill seznámil s dalšími ruskými počítačovými a internetovými nadšenci. Oni sami si říkali „scéna", bylo jich asi tak třicet a žili většinou v Moskvě a v Petrohradu. Roku 1995 se poprvé sešli na vlastním festivalu počítačových nadšenců *Enlight*, jehož součástí byla mimo jiné soutěž v hodu pevným diskem. Až doposud se ostatně setkávali především na IRC-kanálech, což mnohým z nich úplně stačilo, takže žádnou osobní komunikaci nepotřebovali.