ČLÁNKY

Aktuální problémy počítačové kriminality včetně její prevence

Actually Problems of the Cybercrime Including its Prevention

Josef Kuchta*

Abstrakt

Článek pojednává o počítačové kriminalitě a zejména o její podstatné části – internetové kriminalitě – z kriminologického pohledu. Přináší některé nové podněty a skutečnosti týkající se zejména změnám názvu a pojmu této kriminality, jednotlivých forem kybernetických útoků, kybernetické bezpečnosti, zvláštnostem pachatelů a možnostem prevence. Jde o podklad pro nové úvahy pro zkoumání této trestné činnosti.

Klíčová slova

počítačová kriminalita; kybernetická kriminalita; jednotlivé útoky; prevence; kybernetická bezpečnost; prevence; trestní právo; kriminologie.

Abstract

The article describes computer and cyber crimes, especially its important part – cyber criminaliuty of the criminological point of view. Its gives some new views, which desscribe new names and terms of this criminality, the new forms of the cyber crimes, cyber security, charakters of the suspicious persons and the possibilities of the prevention. It is the ground for new thinking for the research of this problematic.

Keywords

Computer Crimes; Cyber Crimes; Hacking; Fishing; Keylogging; Cracking; Spoofing; Phreaking; Cardinbg; Skimming; Grooming; Cysberstalking; Prevention; Penal Law; Criminology.

1 Úvod

Elektronické technologie, jejich vznik a bleskový vývoj v průběhu několika málo desetiletí, se staly jedním z nejvýznamnějších fenoménů dnešní doby., neoddělitelnou součástí každodenního života, jíž není možno se prakticky vyhnout. Odvrácenou stránku obrovského přínosu, který představuje pro ekonomický i společenský život, však tvoří i její negativní projevy, projevující se až v tzv. počítačové kriminalitě. Její rozšíření je adekvátní významu těchto technologií, přičemž nepochybně kopíruje jejich další bouřlivý rozvoj. Tzv. počítačová kriminalita je v současné době zařazována vedle organizovaného zločinu

* Doc. JUDr. Josef Kuchta, CSc., Katedra trestního práva, Právnická fakulta Masarykovy univerzity, Brno / Department of Criminal Law, Faculty of Law, Masaryk University, Brno, Czech Republic / E-mail: Josef.Kuchta@law.muni.cz

a distribuce drog mezi nejzávažnější formy trestné činnosti, páchající obrovské škody všeho druhu, a je také formou nejrychleji se rozvíjející. Poněvadž technický vývoj, stejně jako počítačová kriminalita meznají hranic, stala se i předmětem mezistátních jednání a úmluv (např. Úmluva Rady Evropy o počítačové kriminalitě, Rámcové rozhodnutí Rady 2005/222/SVV z 24. února 2005, nahrazené Směrnicí Evropského parlamentu a Rady 2013/40/EÚ), na jehož základě došlo i u nás ke zpřísnění a rozšíření postihu v novém trestním zákoníku. Vznikla také a dále se vyvíjí nová zvláštní skupina pachatelů, vyznačující se výrazně specifickými rysy.[1]

Vzhledem k rozsahu a složitosti problematiky nemohu ve svém krátkém vystoupení komplexně reagovat na všechny nové jevy, spojené s počítačovou kriminalitou, mou ambicí je spíše stručně upozornit na některé nové problémy, které se vyskytly v průběhu posledních let a které poněkud pozměňují rozsah a podobu počítačové kriminality, a případně identifikovat nové trendy, jichž jsme v současné době svědky, resp. odhadnout jejich další vývoj.

Ke změnám v posledních letech došlo a nepochybně bude docházet i do budoucna zejména v následujících oblastech:

- změna terminologického názvosloví – zavádění nových pojmů odrážejících technický vývoj, i samotného vymezení počítačové kriminality,
- změna a vznik nových specifických podob nebezpečných jednání, stejně jako forem provedení klasických trestných činů,
- změny a rozšíření jurisdikce jednotlivých států ve vztahu k této činnosti, změna charakteristik typických pachatelů určitých trestných činů,
- trestní odpovědnost právnických osob,
- změna způsobu a vedení vyšetřování včetně způsobů odhalování a prokazování trestné činnosti,
- nutnost nových legislativních úprav včetně zavádění nových druhů trestů,
- vytváření nových a účinnějších způsobů prevence na nejrůznějších úrovních včetně i celostátní kybernetické bezpečnosti

2 Vymezení pojmu a nové terminologické změny

V současné době nemá pojem počítačové kriminality oficiálně vymezený obsah. Obecněji ji lze vyložit jako trestná jednání, jejichž společným jmenovatelem je, že v nich vystupuje počítač jako nositel hardwarového a softwarového vybavení a dat, a to buď jako předmět útoku nebo jako nástroj pachatele.[2] V poslední době však již lze sledovat vývojové tendence k odklonu od tak širokého obecného pojmu k jednotlivým dílčím proble-

1 VÁLKOVÁ, H. a J. KUCHTA. *Základy kriminologie a trestní politiky*. Praha: C. H. Beck, 2012, s. 602.

2 Např. op. cit. v pozn. 1, s. 603, dále viz např. MATĚJKA, M. *Počítačová kriminalita*. Praha: Computer Press, 2002, s. 5; VLČEK, M. *Počítačová kriminalita*. Praha: Academia, 1989, s. 5 aj.

movým okruhům s akcentem na podstatu problému a méně na formu páchání. Jako synonymum k výše uvedenému pojmu se např. začal používat pojem tzv. kyberkriminality, ohrožující informační a síťovou bezpečnost a vztahující se k obsahu sdělení, zahrnující např. trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů, počítačové podvody, trestné činy související s pornografií, s porušováním autorského práva apod.[3] Podle našeho názoru se však nejedná o synonymum, neboť pojem kybernetická kriminalita se odvozuje nikoli od pojmu kybernetika, ale od pojmu kybernetický prostor, jímž se rozumí systém tvořený tisíci propojených počítačů, severů, routerů, přepínačů, optických kabelů, umožňující této infrastruktuře její funkci. Jde o sběrný pojem pro všechno od internetu a světové sítě až po imaginární prostor, který v něm existuje, skutečný a současně fiktivní prostor, kde probíhá emailová diskuse a chaty.[4] Počítačová kriminalita se může odehrávat i mimo kyberprostor, kybernetická kriminalita nikoliv, je tedy podmnožinou kriminality počítačové. Dalším užívaným pojmem je internetová kriminalita, která se od počítačové kriminality odlišuje zejména tím, že kromě počítače jako objektu nebo nástroje trestné činnosti vyžaduje propojení počítačů lokálními i vzdálenými sítěmi a následně využití internetu. Kyberkriminalita je činností, ve které použití internetu představuje způsob spáchání trestného činu, nebo ve které je internet (kyberprostor) objektem útoku. Kybernetická kriminalita není současně totožná s internetovou kriminalitou, i když do značné míry se s ní překrývá. Nebude tomu tak v případech, kdy kyberprostor bude předmětem útoku, ale při útoku nebude využit internet.

V praxi je pak možno se setkat i s dalšími pojmy vztahujícími se k trestné počítačové činnosti a zdůrazňujícími některé její aspekty. Lze hovořit např. o informační kriminalitě, jejímž cílem jsou informace bez ohledu na to, jakým způsobem jsou zpracovávány a použity (např. u pomluvy), informatická kriminalita, u níž jsou nástrojem nebo cílem útoku nejen počítače, ale i telekomunikace. Vzhledem k probíhající konvergenci médií, kdy v době digitálního zpracování všech druhů informací se přestává rozlišovat, zda jsou obsahem řady bitů zvuk, obraz nebo počítačová data, je možno se setkat i s pojmem e-kriminalita.[5]

Zavedení jednotné definice těchto typů trestné činnosti je úkolem dlouhodobým, popř. snad i téměř neproveditelným. Je ovšem otázkou, zda je vytvoření jednotného pojmu vůbec nutné, neboť tyto definice nemusejí představovat neřešitelný problém pro praxi i právní úpravu. Konkrétní právní předpisy by totiž patrně měly definovat pojmy, se kterými pracují a na něž váží práva a povinnosti subjektů, přičemž by mohly využít výše podaných definic. Např. v Úmluvě o kybernetické kriminalitě se signatářské státy zavázaly trestně stíhat kybernetickou kriminalitu, kterou zde také definují. Jiné trestné

3 Úmluva o kybernetické kriminalitě, Sdělení MZV ČR č. 104/2013 Sb. m.s.

4 ŠÁMAL, P. et al. *Trestní zákoník*. 2. vyd. Praha: C. H. Beck, 2012, s. 2302–2303.

5 SMEJKAL, V. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. *Trestněprávní revue*, 2003, č. 6, s. 161.

činy, spadající např. jen pod obecný pojem počítačové kriminality, nejsou signatáři povinny podle této Úmluvy stíhat.

3 Charakteristika počítačové kriminality a její změny

Počítačová kriminalita i přes svůj difúzní charakter má řadu výrazných charakteristik a rysů, které ji odlišují od kriminality klasické. Existence i intenzita těchto rysů se mění imanentně s technickým a společenským rozvojem. Jde zejména o následující rysy a faktory:

- Vyznačuje se značně vysokou diskrétností a latentností. V řadě případů nelze pachatele ani oběti vystopovat, mnohdy ani samotné oběti nevědí, že byl na nich spáchán např. majetkový trestný čin (např. pomocí počítačového programu byly v bance převáděny částky vzniklé zaokrouhlováním částek na účtech na soukromé konto pachatele). V některých případech dokonce samy oběti mají zájem na utajení trestné činnosti – např. banky v mnoha případech odmítají spolupracovat s orgány činnými v trestním řízení z obav, že by se s nedostatky v jejich zabezpečení i s výší škod mohla seznámit veřejnost, což by mohlo vést ke ztrátě jejich důvěryhodnosti, a s poškozenými se raději vyrovnají mimosoudně. S tím, jak se v posledních letech zmnohonásobil počet operací prováděných za použití počítačů a jejich sítí, nekoresponduje skutečný počet odhalených trestných činů v této oblasti. Samotný počet těchto odhalených činů je velmi nízký, např. v roce 2011 bylo takto spácháno podle statistik 1502, v roce 2014 4348 činů. Lze tedy pozorovat lineární, ale velmi pozvolný nárůst, který dává tušit nesmírnou latenci. Z jednotlivých trestných činů bývají takto nejčastěji páchány trestné činy podvodu (l419 činů v roce 2013, úvěrového podvodu (113). U zbývajících trestných činů jde o počty několika desítek činů podřaditelných pod jednotlivá ustanovení ročně.[6]
- Jejím následkem vznikají značné škody, na jedné straně obtížně kvantifikovatelné, na druhé straně mohou mít až katastrofické rozměry. Tato nebezpečí se zvětšují a stávají se aktuálnějšími zejména v souvislosti s faktem, že počítači a jejich sítěmi mohou být ovládány a řízeny technická zařízení, jejich napadení a zneužití může mít za následek poruchy v zásobování vodou, energiemi v celých oblastech, vytváří se nebezpečí spojená s vyřazením z provozu jaderných elektráren, ovládnutí atomových zařízení včetně atomových zbraní, kosmického výzkumu apod. Přitom tyto trestné činy mohou být spáchány v tisícině sekundy, jejich spáchání nemusí být vůbec postřehnutelné a pachatel nemusí být vůbec přítomen na místě činu.
- Je páchána intelektuálně vyspělými a erudovanými pachateli, jejichž cíle bývají většinou zištné, ale mohou být motivovány i jinak (politicky, ideologicky, nábožensky, bojem za svobodu kyberprostoru apod.).

---

6 Viz blíže statistiky uváděné v LOBOTKA, A. *Globální systémy propojených počítačových sítí a trestní právo*. Disertační práce. MU Brno, 2015, s. 185, 188, 189 a další.

- V důsledku toho způsoby jejich odhalování, dokumentování a dokazování mohou být značně složité a vyžadují skutečné odborníky z oboru, vybavené nejmodernějšími technickými prostředky.
- Lze předpokládat zvyšující se a značný podíl organizovaných pachatelů (např. hnutí tzv. Anonymous, White media na našem území apod.).
- Má často mezinárodní charakter, když následky mohou zasahovat objekty v různých státech, bývá odděleno místo spáchání činu a místo nástupu následků
- Pro boj s ní, který vyžaduje mj. spolupráci většího počtu států, doposud neexistuje dostatek právních, režimových a organizačních prostředků, přitom tato trestná činnost se bude bouřlivě komplikovat a rozšiřovat v důsledku např. přibývajícího počtu počítačů, mobilních telefonů, uživatelů internetu, rozvojem internetového bankovnictví apod.
- Vzhledem k většinovému soukromému podnikání bude její prevence spíše záležitostí příslušných poškozených a vlastníků než orgánů činných v trestním řízení. To samozřejmě nevylučuje, ale i vyžaduje zásahy státu tam, kde by mohly být postiženy zájmy celého státu nebo mezinárodních společenství (např. snaha o zajištění tzv. kybernetické bezpečnosti).[7]

4 Konkrétní typy počítačových útoků

Vyvíjející se počítačová věda a technika postupem času přinášejí kontinuálně stále nové typy počítačových útoků i zdokonalování útoků dosavadních. Snad nejvíce příznačným a nejvíce známým je spam, jenž se dále dělí na nigerijský typ, phishing, ransomware, adware, spyware, počítačové viry, trojské koně, z nových pak logical bombs a pharming crimware.

- Nigerijský spam se snaží příjemce přesvědčit, že má k dispozici velkou sumu peněz, kterou mu může pomoci získat jen příjemce spamu. Podmínkou je odeslání svých osobních údajů nebo uhrazení určité částky odesílateli spamu.
- Phishing popisuje rozesílání podvodných zpráv, nejčastěji e-mailů, které se tváří jako zprávy od správce sítě, banky apod. Cílem je pod smyšlenou záminkou získat od příjemce zprávy jeho citlivé údaje zejména v oblasti bankovnictví.
- Ransomware zabraňuje přístupu k počítači, který je napaden, a zpravidla vyžaduje zaplacení výkupného za opětovné zpřístupnění počítače.
- Adware je program namontovaný do počítače, aniž by o tom uživatel věděl. Bývají obvykle poskytovány zdarma a nainstalované skryté programy potom poskytují údaje o provozu na e-mailu či internetové stránce.
- Spyware a trojský kůň je druh škodlivých programů, jejichž cílem je sledování napadeného počítače a aktivit jeho uživatele (např. od roku 2012 cílí zejména na ambasády a vládní instituce v mnoha státech špionážní spyware jménem Machete).

7 Viz např. op. cit. v pozn. č. 1, s. 606.

- Logical bombs jsou programy tajně vkládané do aplikací nebo do operačních systémů, které za předem stanovených podmínek (např. konkrétního data) provádějí destrukční činnost.
- Pharming crimeware jsou programy, které přesměrovávají uživatele na určité stránky namísto těch, které měl uživatel v plánu navštívit. Na těchto stránkách dochází k instalaci dalšího crimeware. Touto cestou může např. dojít k významnému zvýšení poplatků za připojení internetu prostřednictvím telefonních linek se zvýšeným tarifem.

Dalšími aktuálními hrozbami internetu jsou např. tyto zásahy:

- Hacking – představuje pronikání do systému jinou než standardní cestou, tedy obejitím nebo prolomením bezpečnostní ochrany (firewallu). Původním cílem hackerů bylo systém prozkoumat, popř. odstranit jeho chyby, v poslední době však nastupuje motiv získání peněžní hotovosti.
- Cracking – představuje prolomení ochrany programu proti jeho kopírování nebo neoprávněnému používání.
- Spoofing – označuje změnu totožnosti původce odesílaných zpráv.
- Phreaking – představuje napojení se na cizí telefonní linku. Útočník tak používá telefonní síť nebo kartu bez zaplacení provozovateli.
- Cybersquatting spočívá v registraci doménového jména souvisejícího se jménem nebo obchodní známkou jiné společnosti za účelem následného nabízení domény této společnosti za vysokou finanční částku, případně zneužití domény k dalším nežádoucím jednáním.
- Carding představuje zneužití platební karty různými způsoby, např. nainstalováním kamery nad bankovní automat, vylákáním hesla a čísla karty od vlastníka, ale i strhnutím vyššího peněžního obnosu z klientova čísla, než mělo být zaplaceno (v kamenném obchodě nebo přes internet).
- K novým metodám zneužití platební karty patří nyní i skimming, který se již vyskytl i v České republice – kopírování platebních karet za pomoci zvláštního kopírovacího přístroje, který je umístěn přímo na bankomatu nebo v platebním terminálu.
- Man in the Middle útok – spočívá v narušení šifrované komunikace do které vstupuje třetí osoba. Útočník změní směrovací tabulku zařízení patřící oběti tak, aby byl provoz pro konkretní IP adresu přesměrován přes libovolné síťové cesty včetně počítače pachatele. Před takovým novým útokem varovalo u nás Národní centrum kybernetické bezpečnosti veřejnost teprve v listopadu 2014.
- Pojem hoax (falešná zpráva, mystifikace, podvod, poplašná zpráva, žert) označuje falešnou zprávu která varuje před neexistujícím nebezpečím, přičemž obsahuje nepřesné zkreslující informace či účelově upravené polopravdy. Mezi známé hoaxy patří např. varování před nastrčenými injekčními stříkačkami infikovanými virem HIV, před rakovinotvornými látkami v deodorantech, šamponech apod. Velké množství hoaxů zaplavuje v současné době kyberprostor v souvislosti s problémem migrace.

- Backdoor útok představuje tzv. zadní vrátka vytvořená programátorem pro pozdější převzetí kontroly nad programem. Keylogger je program tajně zaznamenávající znaky zadávané uživatelem, např. hesla s cílem zpřístupnit je útočníkovi. Defacement spočívá v průniku do webových serverů oběti, kde dojde k nahrazení internetových stránek oběti obsahem, který vytvořil pachatel. Na rozdíl od ostatních útoků zde útočník usiluje o co největší medializaci. Psychologická síla tohoto typu útoku spočívá ve vyvolání pocitu ohrožení a nedůvěry ve vlastní informační systémy oběti, a rovněž v prezentaci ideologie či postojů pachatele.
- DDoS (Distributed Denial of Service) neboli distribuované odmítnutí služby představuje útok mnoha koordinovaných útočníků na služby nebo stránky, při kterém dochází k přehlcení požadavky a k pádu nebo nedostupnosti a nefunkčnosti systému pro ostatní uživatele (tzv. spadnutí sítě). Nedostupnosti serveru nebo infrastruktury se dosahuje útokem na šířku pásma (zaplnění kapacity serveru), útokem na zdroje (zaplnění systémových zdrojů stroje, což zabraňuje jeho reakcím na běžné dotazy) nebo využitím chyby software. V poslední době je možno získat dostatečný počet potřebných počítačů komunikací na internetu a domluvou s dalšími lidmi, nejmodernější způsob však představuje tzv. botnet, který udělá z virem napadených počítačů tzv. zombie, kterým lze opakovaně zadat jakýkoliv příkaz (např. opakované zasílání požadavků na tutéž adresu). Botnety je nyní možno pronajmout si za poměrně levné peníze, což představuje značné riziko.[8]

5 Změněné způsoby provádění některých trestných činů

Počítače a zvláště internet přinesly osobité podoby jinak obecných trestných jednání, jejich masové rozšíření, pozměnění způsobu jejich výkonu, umožnění pachatelům jejich efektivnějšího páchání. Často taková jednán í dostávají osobitá pojmenování, jako jsou např. kybergrooming, kyberstalking, kyberšikana, happy slapping, kybermobbing, kyberterorismus a jiné.

- Termín grooming označuje nově pozorované specifické jednání, psychickou manipulaci ze strany groomerů, které má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce, jejímž důsledkem může být zejména některý ze sexuálních trestných činů. Kybergrooming postihuje takové jednání provozované prostřednictvím internetu, mobilních telefonů a sociálních sítí např. na chatech, internetových seznamkách, Skype, facebooku, twitteru a podobných portálech. Problémem při jejich zjišťování a dokazování je zejména anonymita, využití zabezpečovacích systémů a fakt, že v raných stadiích ještě zpravidla nejde o trestný čin, zejména tam, kde není trestná forma přípravy.
- Kyberstalking je možno definovat jako druh stalkingu probíhající v kybernetickém prostoru. Jde tedy o zasílání různých zpráv pomocí chatu, VoiP technologií, emai-

8 Blíže k vysvětlení všech těchto pojmů viz např. Slovník *BezpecnyInternet.cz* (cit. 10. 1. 2016). Dostupné z http://www.bezpecnyinternet.cz/slovnik/default.aspx

lem, sociálních sítí s cílem vyděsit nebo vyhrožovat určitému jednotlivci nebo skupině. E-mail umožňuje pachateli zasílat zprávy různého druhu a přímo tak obtěžovat oběť. Stalker může také vytvořit internetové stránky, které budou obsahovat údaje o pronásledované osobě, ať již pravdivé nebo smyšlené. Může též využívat elektronické diskusní skupiny, tzv. knih návštěv, nástěnek nebo chatů, poměrně často se využívá komerčních služeb na internetu – pachatel může přihlásit oběť k odběru různých služeb, k neustálému zasílání reklam, zpráv, nabídek, např. vyvěšení jménem oběti inzerátu s návrhem k sexuálním praktikám. Stalker obvykle jednotlivé způsoby kombinuje, čímž může dosáhnout multiplikačního účinku. Takové jednání lze zpravidla stíhat jako trestný čin nebezpečného vyhrožování podle § 353 TrZ, resp. podle nové skutkové podstaty stalkingu podle § 354 TrZ.

- U Happy slappingu se jedná o určitý druh šikany, jejímž cílem je nečekaně fyzicky napadnout oběť, přičemž komplic útočníka celý čin nahrává na mobilní telefon nebo kameru a získané video pak umístí na internet zejména k pobavení diváků (,u nás např. i případy vyprovokování učitele žáky). Trestně stíhat lze taková jednání např. podle trestného činu výtržnictví.

V poslední době lze též sledovat vzrůstající intenzitu využívání a zneužívání internetu různými extremistickými hnutími k vlastní propagandě a podpoře filosofií, na nichž jsou založena. Stránky takových hnutí jsou často fyzicky umístěny v lokalitách, které jsou často chráněny široce pojímanou svobodou slova, např. v USA. Opatřením proti danému postupu by mohlo být zablokování IP adres na žádost policejního orgánu, kterému však často není z výše uvedených důvodů vyhověno (dle aktuálního sdělení ministra vnitra ČR byla taková žádost opakovaně zamítnuta americkou stranou např. v případě serveru white-media@info, který v poslední době vstoupil do povědomí veřejnosti např. vykradením a zveřejněním e-mailové pošty předsedy vlády ČR). Obsahem bývají nenávistné a extremistické výzvy, dezinformace, organizační pokyny, zábava, reakce na aktuální dění nebo likvidační seznamy. Taková jednání nejčastěji vyúsťují v trestné činy proti svobodě nebo proti pořádku ve věcech veřejných. K dalším trestným činům páchaným velmi často vedle klasických způsobů využití počítačů a internetu patří např. podněcování a schvalování trestného činu, pomluva a křivé obvinění, šíření, výroba a jiné nakládání s dětskou pornografií, porušování autorských práv, šíření poplašné zprávy, šíření toxikománie, podvody apod. K ryze počítačovým trestným činům patří trestné činy podle ust. § 230 až 232 TrZ, jejichž výskyt v trestní praxi je velmi malý, neboť zde existuje velmi vysoká latence.

6 Pachatelé počítačové kriminality

V současné době, kdy rozvoj a rozšíření počítačů dosahuje masovosti, stoupá zásadně i počet pachatelů, kteří se počítačové trestné činnosti mohou dopustit. Důvodem je obecná dostupnost hardware i software prakticky komukoliv, stejně jako rozvoj počítačové dovednosti prakticky u všeho obyvatelstva. Počítače zasahují do všech oblastí živo-

ta společnosti, což má odraz i ve velkém množství počítačových trestných činů. Z toho vyplývají dvě zásadní teze: pachatelem se za určitých okolností (příležitost dělá zloděje) může stát téměř každý, přičemž nelze patrně vytvořit jeden obecný typ pachatele této trestné činnosti. Lze určit určitou charakteristiku těchto pachatelů, kterou je ovšem třeba pro konkrétní praxi specifikovat a diferencovat podle oblastí činnosti, podle motivace, osobních schopností pachatelů i podle vlivu vnějšího okolí. Lze vyjít z toho, že pachatel bývá často vzdělaný, inteligentní, ovládající potřebné dovednosti, s potřebnou mírou přizpůsobivosti. Nezákonnou činnost neprovádí jen pro zábavu, ale stále častěji i pro zisk. Jeho osobnost nevykazuje zjevné patologické rysy, navenek se nijak neodlišuje od většinové společnosti, rekrutuje se prakticky ze všech jejích vrstev. Obvykle i vzhledem ke svému mládí nemá záznam v trestním rejstříku, trestnou činnost páchá individuálně, často v izolaci, nevzbuzuje při ní pozornost. Často pracuje na místech, kde vzbuzuje důvěru i respekt společnosti. Zisk realizuje po menších částkách, nechce ublížit konkrétní oběti, ale spíše neosobnímu zaměstnavateli, jímž se často cítí být vykořisťován, či společnosti jako celku.

Z rozboru trestných činů dále vyplývá, že pachatelé bývají často jedinci s vyšším vzděláním, ale někdy i geniální samoukové, nadprůměrně vynalézaví právě ve speciální programátorské činnosti, jsou sebevědomí, psychicky silní, někdy ale i s utajovanými komplexy či duševně labilní. Jejich jednání neobsahuje prvky násilí a je vzdáleno tradičním hrubým formám delikvence. Z motivace převažuje touha po zisku, ale motivem může být např. pomsta a získání převahy nad zaměstnavatelem či jinými významnými subjekty (banky, státní orgány), radost z destrukce systému, euforie z pocitu beztrestnosti či neodhalitelnosti, snaha po kompenzaci pocitu křivdy, osobního zneuznání či nedostatečného ohodnocení jejich práce, někdy jen intelektuální výzva. U dobře situovaných osob to může být i touha po riziku a dobrodružství, soutěživost blízká psychologii sportovce apod.[9] Lze tak hovořit o typech průnikářů, neúspěšných kritiků, mstitelů či škodičů, profesionálů atd. Pachatelství zasahuje osoby čím dále širšího věkového spektra, když od původních tradičních představ pachatelů teenagerů se přechází k pachatelům i starším 40 let, kteří získali znalosti již před desítkami let a s rozvojem počítačů si je neustále inovují. Velkou většinu pachatelů tvoří muži, což je vysvětlováno různými důvody, nejpřesvědčivějšími se zdají nezájem žen o technickou dokonalost, jejich menší ambice, nechuť ke zbytečné destrukci, kyberprostor nechápou jako prostor pro loveckou výpravu nebo nedobyté území. [10] Je třeba brát v úvahu i psychologické charakteristiky internetu, a to zejména anonymitu, malá rizika, změněné vnímání pachatele, místní časovou flexibilitu, kdy pachatel v kyberprostoru má možnost delšího času pro promyšlení jednotli-

9 Op. cit. v pozn. 1, s. 607.

10 Blíže k charakteristice osobností pachatelů, zejména tzv. hackerů viz GŘIVNA, T. a R. POLČÁK (eds). *Kyberkriminalita a právo.* Praha: Auditorium, 2008, s. 48–53.

vých útoků, snáze překonává rozpaky, ostych a plachost, a to dokonce do takové míry, že může přistoupit k porušování zákonů.

Nejnověji dělí pachatele Smejkal, a to do pěti kategorií: zaměstnanci poškozené organizace, průnikáři (hackeři), kteří mají spíše anarchistické cíle, příslušníci organizovaného zločinu, profesionálové pracující za peníze, živící se činností jako průniky, odhalování utajovaných informací, špionáž apod., a osoby příliš nepřemýšlející o svém jednání a jeho následcích (děti, mladiství, osoby neznalé práva). V této souvislosti upozorňuje, že psychologickému profilu pachatele by měla být v kriminologických výzkumech věnována pozornost, což se u nás dosud neděje.[11] U konkrétních trestných činů je možno se inspirovat zahraničními výzkumy, např. v případě trestného činu stalkingu byly již vytvořeny určité typologie pachatelů. Holmes např. člení stalkery na pronásledovatele celebrit, ex-partnera, politiků, z vášně, ze zištné motivace, pronásledovatel zhrzený a odmítnutý z vášně.[12] Psychologické charakteristiky stalkerů vypracoval i P.E. Mullen, když je člení na bývalé partnery, uctívače, neobratné nápadníky, ublížené pronásledovatele, sexuální útočníky, poblouzněné milovníky a kyberstalkery.[13]

7 Prevence počítačové kriminality.

Prevence a preventivní opatření musí v první řadě reagovat na změněné podoby páchání této kriminality a postihovat neustálý vývoj informačních technologií. Pro efektivní tlumení počítačové a internetové delikvence je podle našeho názoru prevence důležitější než represívní postihy, neboť zabraňuje vysoké latenci i velmi vysokým škodám. Šetří se tak i kapacity orgánů činných v trestním řízení, neboť odhalování a dokazování těchto trestných činů jsou velmi náročné na finance i čas a často končí neúspěšně a tím i neefektivně. Prevenci je třeba zaměřit v prvé řadě na osoby přicházející do styku s výpočetní technikou, ale i na vnější a vnitřní ochranu této techniky, programů a informací jí zpracovávaných. Ve všech těchto oblastech je nutno vypracovat preventivní strategie jak vůči potencionálním pachatelům, ale i potencionálním obětem, ale i podle typů kriminality (internetové a počítačové v širším slova smyslu), a neustále je inovovat. Preventivních opatření lze uvést celou řadu, pro nedostatek prostoru se zaměříme stručně jen na ty z nich, která považujeme za nejvýznamnější zejména ze strategického hlediska a jejichž cestami by se měla ubírat do budoucna i praxe.

Prevence má působit především výchovně a napomáhat zformování jakési „počítačové kulturnosti a odpovědnosti" a varovat před zneužíváním. Taková výchova má být propojená se zvyšováním i právního vědomí, neboť v této oblasti existuje jen velmi nízké práv-

11 SMEJKAL, V. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 135. Určité zpřesnění charakteristiky pachatelů jednotlivých typů trestné činnosti viz např. op. cit. v pozn. 1, s. 607–609.

12 Viz ČÍRTKOVÁ, L. *Moderní psychologie pro právníky.* Praha: Grada Publishing, 2008, s. 72.

13 Viz KOPECKÝ, K. *Stalking a kyberstalking. Nebezpečné pronásledování.* Olomouc:NET Universi-TY, s. r. o., 2010, s. 4.

ní vědomí spojené s kriminální citlivostí na tyto trestné činy. Naprosto nezastupitelnou úlohu zde má zejména vzdělávání mládeže počínajíc již dětským věkem, neboť právě zde je právní vědomí zcela nedostatečné a neodpovídající značným faktickým vědomostem a dovednostem, které tato generace již mnohdy získala a které využívá v kyberprostoru. Vedle výuky k dovednostem a k základům opatrnosti při práci s počítači seznamováním s nástrahami a riziky by měla být pozornost věnována i právní výchově a faktu, že právní řád je stejně závazný jak v kyberprostoru, tak i v reálném světě. S tím souvisí i vysvětlování, jaké činnosti již spadají pod počítačovou kriminalitu, i seznamování s etickými normami v kyberprostoru. Odpovídající výuka zejména ohledně bezpečného užívání internetu by neměla být zajišťována pouze formou jednorázových projektů, ale měla by být běžnou součástí výuky na školách všech stupňů stejně jako např. dopravní výchova. Preventivním projektům se v tomto směru věnuje zejména Slovenská republika.[14]

Tam, kde je výchova a morální apel neúčinný, je třeba realizovat konkrétní technické způsoby zabraňující přístupu k počítači neoprávněným osobám a zajišťující samotnou ochranu dat před zneužitím. To platí jak pro napadené jak fyzické, tak i právnické osoby, kde se doporučuje např. střežení v pracovní době i mimo ni, užívání kvalitních antivirových programů, zaheslování, případně zašifrování citlivých údajů, stále častěji uplatňovat kontrolu založenou na biometrických charakteristikách (oční signatura, otisky prstů, hlasový nebo grafický projev). Řada preventivních opatření bránících i zneužití internetu nevyžaduje velké náklady, ale lze je odvodit užitím zdravého rozumu. Tak např. každý uživatel internetu by měl pravidelně aktualizovat ochranné mechanismy svého počítače, jako jsou různé antivirové programy, firewaly, hesla (platí i pro tzv. chytré telefony), programy a aplikace instalovat jen z ověřených autorizovaných zdrojů, přihlašovací, bankovní a osobní údaje zadávat v nejnižší možné míře v důvěryhodném prostředí a nikomu je nesdělovat, ve větší míře využívat tzv. elektronické peněženky (např. nabíjecí karty ve formě tzv. Blesk peněženek, které zamezí přístupu ke kontům), nereagovat na podezřelé maily, neotevírat jejich přílohy či je rovnou mazat, pravidelně si měnit hesla, nakupovat jen u osvědčených e-shopů, užívat jen legální software, být obezřetný ve vztahu k aplikacím a hrám nabízeným zdarma, pravidelně si zálohovat důležitá data, nepouštět ke svému počítači nedůvěryhodné osoby, zamezit přístupu dětí na podezřelé internetové stránky, respektovat skutečnost, že každý uživatel internetu zanechává po sobě stopy a neukryje se v anonymitě apod. Děti jako uživatelé internetu by neměly dávat neznámým osobám své telefonní čísla, adresy ani osobní údaje., neznámým osobám nezasílat své intimní fotografie, nedomlouvat si schůzky s neznámými osobami přes internetové sítě jako jsou např. Facebook, nevěřit všem informacím, které na síti naleznou. V zájmu rodičů je, aby své děti s těmito pravidly seznámili dříve než je seznámí a důvěru si získá

14 Stručný i pro nás inspirativní přehled viz např. v DIANIŠKA, G. a kol. *Kriminológia.* Plzeň: Aleš Čeněk, 2009, s. 220–221.

někdo jiný, a kontrolovali jejich dodržování, i když by zde mohly narazit na porušení osobní sféry dětí (patrně tzv. v rámci výkonu rodičovských práv).

Z dalších preventivních opatření je možno uvést zvyšování komfortu služeb nabízených legálními distributory např. autorských děl při jejich současném zlevnění tak, aby byly bez problému dostupné. Nepochybně by bylo vhodné zavést ve spolupráci s nestátními organizacemi (např. BSA) finanční odměny poskytované osobám, které nahlásí počítačovou kriminalitu, pokud dojde k usvědčení pachatele, ale i omezit dostupnost softwarových produktů, které lze užít k trestným činům (např. pachatelé, kteří se vloupali do internetové schránky českého předsedy vlády, použili k tomu speciální programy, které jsou volně k sehnání v zahraničí, byť i za vyšší ceny).[15]

Z legislativních opatření spíše represivního charakteru je možno doporučit rozšíření trestnosti pro právnické osoby na široký okruh trestných činů včetně těch, které souvisejí s internetovou kriminalitou. To by mohlo vést k částečnému přenesení odpovědnosti za obsah sdělení na internetu na providery, stejně jako uložení povinnosti po určitou dobu archivovat data. Na obtíže při odhalování a dokazování trestné činnosti by bylo třeba reagovat upřesněním úpravy trestního řádu týkající se zejména provádění a důkazní hodnoty jednotlivých důkazních prostředků a jednotlivých typů zajišťovacích opatření, když současný právní stav využívající jen judikaturu nelze považovat za dostačující. V oblasti trestání lze navrhnout zavedení nového druhu trestu spočívajícím v zákazu práce na počítači či využívání internetu, bylo by však lze očekávat problémy zejména při kontrole výkonu takových trestů. Nejasná jsou dosud pravidla pro určování jurisdikce jednotlivých států pro stíhání jednotlivých činů počítačové kriminality. Komplexní řešení těchto problémů si ovšem nezbytně vyžaduje mezinárodní spolupráci. Směry této spolupráce je třeba vidět zejména v dohodě o prodloužení doby uchovávání údajů u providerů a u shromažďovatelů dat (u nás činí maximálně 6 měsíců), harmonizaci podmínek pro povolování určitých procesních úkonů jako např. odposlechů a záznamu elektronických komunikací, urgentní vyřizování žádostí o dožádaní v těchto věcech, úprava spolupráce se zahraničními poskytovateli služeb, a to i soukromými (např. Google), na které by bylo možno obracet se s přímými žádostmi, jednotné standardy pro přijímání takto získaných důkazů před národními soudy, jednotná pravidla pro vytěžování úložišť informací – tzv. cloudů, zefektivnit a zejména zrychlit mezinárodní justiční spolupráci, vyřešit otázky konfliktů (zejména pozitivních) státních jurisdikcí.[16] Zatím nejobecnější podklad pro další úvahy tvoří Úmluva o počítačové kriminalitě, přijatá v Budapešti 23. 11. 2001.

Specifika tohoto druhu kriminality si vyžaduje i specializaci orgánů činných v trestním řízení, které se jí zabývají, v České republice však dosud byla na nižším stupni, když existují specializované orgány na úrovni krajských ředitelství a na policejním presidiu

15 *Právo*, 20. 1. 2016, s. 7.

16 V podrobnostech viz např. Mandát ministra spravedlnosti pro jednání neformální Rady pro spravedlnost a vnitřní věci ve dnech 25-26. 1. 2016, Číslo verze 1, vypracováno dne 15. 1. 2016, MS ČR 2016.

(odbor informační kriminality ÚSKPV), k jehož práci byly v poslední době byly vysloveny výhrady a jeho ředitel byl odvolán.[17] Od 1. ledna tohoto roku však zahájil svou činnost nový speciální útvar zaměřený na boj proti kriminalitě, který bude metodicky řídit činnost v rámci ČR a bude spolupracovat s NBÚ a Národním centrem kybernetické bezpečnosti. Současně by měl být technicky zdatným pracovištěm, které bude odhalovat a vyšetřovat případy internetové kriminality.

Na celostátní úrovni pak byly vypracovány zásadní strategické dokumenty preventivních opatření, k nichž je možno si bez problémů získat přístup.[18]

8 Kybernetická bezpečnost České republiky.

Plánované útoky proti informačním technologiím mohou způsobit značné až katastrofální škody jak v soukromém, tak i ve veřejném sektoru, v národním i globálním měřítku. Pokud je útok veden proti prvkům kritické infrastruktury, může být v konečném důsledku ohrožena nejen bezpečnost, ale i samotná existence státu. Útoky se v poslední době přesouvají zejména do oblasti organizované průmyslové špionáže a kybernetického terorismu, jsou stále komplexnější a sofistikovanější, mohou se zaměřit na prvky kritické infrastruktury (energetické systémy, informační systémy veřejné správy, zdravotnické systémy), ohrožena může být obrana státu, atomové hospodářství apod. Je proto třeba proti těmto zvýšeným nebezpečím přijmout mimořádná opatření také v preventivní oblasti.[19]

Každý jednotlivý stát řeší otázku své kybernetické bezpečnosti a potírání kybernetických hrozeb svým vlastním způsobem, protože však kybernetický prostor nemá hranic, měl by ale korespondovat s pohledem mezinárodního společenství. Proto otázkám prevence v této oblasti musí být věnována prvořadá pozornost. V ČR našel tento požadavek odraz teprve v zákoně č. 181/2014 Sb, který nabyl účinnosti 1. ledna 2015. Zákon stojí na dvou zásadách - minimalizaci zásahů do práv soukromoprávních subjektů a individuální odpovědnosti za bezpečnost vlastních informačních systémů - a na třech pilířích (bezpečnostní opatření, hlášení kybernetických bezpečnostních incidentů a protiopatření, tzv. reakce na incidenty.)

Zákon definuje, které osoby jsou povinny hlásit bezpečnostní incidenty v určitých oblastech kterému týmu, a co by měl příslušný tým s takovým hlášením podniknout. Definuje dále významný informační systém (omezeno jen na veřejný sektor) a kritickou informační strukturu, jejichž napadení je třeba hlásit. Na jednotlivé subjekty klade zákon

---

17 *Právo*, 19. 1. 2016, s. 5.

18 Viz Např. Strategie prevence kriminality na léta 2015 až 2015. MVČR (online). 2015. dostupné z www.mvcr.cz/soubor/novejsi-leden2012-jjj-pk-2012-2015-09-11-2011-vlada.doc.aspx, dále viz např. Národní strategie kybernetické bezpečnosti ČR na období let 2015 až 2020. Národní bezpečnostní úřad (online). Dostupné z www.govcert.cz/download/nodeid-1004/

19 Blíže viz např. POLČÁK, M. Kybernetická bezpečnost. *Revue pro právo a technologie*. Brno: Masarykova univerzita, 12/2015, s. 95–151.

povinnost provádět bezpečnostní, technická a organizační opatření, jejich bližší specifikaci je možno nalézt ve vyhlášce 316/2014 Sb. o bezpečnostních opatřeních. Současně došlo k ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a současně národní autoritou pro tuto oblast. Dále byla zřízena Rada pro kybernetickou bezpečnost a Národní centrum kybernetické bezpečnosti jako součásti Národního bezpečnostního úřadu v Brně.[20] Význam této prevence patrně poroste v souvislosti s novodobými hrozbami terorismu zejména v politické, ideologické a náboženské oblasti.

Možnost závažných ohrožení zásadních zájmů vede i k návrhům na omezení práv uživatelů internetu. U nás se zcela nově objevil návrh na prolomení anonymity uživatelů internetu, který by posloužil k identifikaci uživatelů. Inspiruje se nepochybně v praxi a úvahách některých jiných států, které omezují přístup k internetu (Čína, Severní Korea), požaduje registraci uživatelů internetu (Rusko), nebo alespoň zákaz šifrované komunikace a přístupu k některým prohlížečům, např. Darknetu.[21]

9 Další předpokládaný vývoj počítačové kriminality

Další vývoj počítačové kriminality je závislý na mnoha faktorech, zejména na technickém vývoji v dané oblasti, nicméně lze patrně odhadnout některé jeho směry. Patří k nim zejména:

- objektem útoku budou v převážné většině nehmotné informace, nikoliv hardware a hmotné prostředky informačních systému,
- útoky se budou odehrávat zejména na mobilní zařízení a nedostatečně zabezpečená zařízení připojená do sítě zaměstnavatele,
- je třeba předpokládat možnost a větší počet útoků na průmyslové řídící systémy dispečerského řízení a sběru dat v kritické infrastruktuře, přičemž důvodem bude jejich větší rozšíření kombinované s dosud nízkým zabezpečením,
- k útokům budou stále více používány všechny druhy internetové komunikace včetně sociálních sítí,
- individuální vandalismus bude nahrazován cílenými útoky soukromých skupin pachatelů s cílem majetkové trestné činnosti, špionáže i terorismu,
- udrží se množství finančních podvodů spojených s kyberprostorem, stejně jako kriminální jednání zaměstnanců – krádeže dat nebo nedbalostní prozrazení nebo umožnění úniku,
- neustále poroste masívní zneužívání internetu k šíření nepravdivých údajů, a to od útoků na soukromé osoby a podnikatele až k útokům na stát jako takový;

---

20 Blíže k tomu viz LOBOTKA, A. *Globální systémy propojených bezpečnostních sítí a trestní právo.* Disertační práce. Brno: MU 2015, s. 143–149.

21 Chovanec: Na web jen s povolením. *MF Dnes.* 19. 1. 2016, s. 1.

alternativou může být šíření nezákonných ideologií směřujících k poškozování lidských práv

- stále se bude prohlubovat střet mezi anonymitou a ochranou soukromí na internetu a rostoucími požadavky na bezpečnostní kontrolu aktivit v kyberprostoru, zejména pod hlavičkou boje proti terorismu; v souvislosti s tím lze očekávat tlak vládních organizací na zamezení možnosti ochrany identity a obsahu na internetu pod záminkou boje proti organizovanému zločinu a terorismu,
- internet zůstane i nadále vhodným prostředkem pro porušování autorských práv nejen k softwaru, ale především k audiovým a audiovizuálním dílům prostřednictvím různých úložišť a cloudů, ale i práv průmyslových v souvislosti se zhotovováním výrobků pomocí 3D tisku,
- je třeba očekávat útoky na kritickou informační a komunikační infrastrukturu ze strany cizích států, ale i malých skupin osob (asymetrické hrozby).[22]

Velké nebezpečí představuje také do budoucna tzv. internet věcí, kdy na internet budou zapojeny i domácí spotřebiče, každý jednotlivec bude mít tedy více IP adres, které budou komunikovat se sebou navzájem a budou také zvenčí napadnutelné. Veškerá tato nebezpečí vedou odborníky k naléhavým výzvám ke vzniku mezinárodní úmluvy o internetu.[23]

Závěr

Počítačová a internetová kriminalita patří k nejdynamičtěji se vyvíjejícím oblastem kriminality vůbec. Reakce na ni musí být adekvátní, což si již začínají uvědomovat jednotlivé státy i mezinárodní organizace. Dysplastičnosti této kriminality odpovídá i prozatímní postoj k ní, který se vyčerpává ve zkoumání či přijímání opatření zatím nesystematické povahy. Ve svém vystoupení jsem tedy nemohl zachytit všechny její souvislosti, pokusil jsem se jen reagovat a postihnout některé její podstatné rysy jako východiska pro budoucí úpravy.

22 SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 571–572.

23 Až vám hacker na dálku zapálí dům a zapálí ho. Rozhovor s V. Smejkalem. MF dnes, 19. 1. 2016, s. 3.