CyberCrime

Pojem kybernetické trestné činnosti a pojmy související

Kybernetická trestná činnost (Cybercrime)

Užívání výpočetní techniky, informačních systémů a informačních technologií a jejich integrace do téměř všech odvětví lidské činnosti je jevem, který je pro dnešní dobu charakteristický. Lze konstatovat, že v podstatě nejde nalézt takovou oblast lidské činnosti, kde by se přímo nebo zprostředkovaně nevyužívala výpočetní technika, resp. informační systém nebo informační či komunikační technologie. Bohužel, tak jak rostou možnosti užívání těchto vymožeností dnešní doby a vědeckotechnického pokroku, rostou i možnosti a zároveň i četnost jejich zneužívání k páchání trestné činnosti. Různí autoři i různé právní normy používají pro označení těchto aktivit různé pojmy, mezi které patří: informační,18 informatická,19 elektronická kriminalita, softwarová trestná činnost, počítačová trestná činnost (Computer crime), computer-related-crime, počítačová kriminalita, kybernetická trestná činnost, kyberkriminalita aj. U této problematiky přetrvávají rozdíly nejen v označování tohoto jevu, ale rozdílně je chápán též jejich obsahový význam, což mnohdy přispívá k nesprávnému pochopení významu a škodlivosti tohoto druhu trestné činnosti. Na tomto místě je třeba předně konstatovat terminologickou nejednotnost a různorodost v chápání výše uvedených pojmů. To je do značné míry odůvodněné interdisciplinárností přístupu k řešení dané problematiky. Proto bývají v různých odborných pracích i v právních dokumentech často zaměňovány pojmy „počítačový trestný čin“ s „počítačovou kriminalitou“, „kybernetický trestný čin“ s pojmem „kyberkriminalita“ apod., resp. jsou mnohdy užívány jako synonyma. V 90. letech 20. století se pro trestnou činnost páchanou pomocí informační techniky ustálil pojem „počítačová kriminalita“ (Computercrime, Computerkriminalität). Smejkal ve své publikaci definuje, v polovině 90. let 20. století, počítačovou kriminalitu, jako různorodou směsici trestných činů, jejichž společným faktorem je počítač, program a data. Pod pojmem počítačová kriminalita „...je třeba chápat páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení data nevyjímaje, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako movité věci, nebo jako nástroje trestné činnosti.“ 20 Z uvedené definice je patrné, že počítačová kriminalita se vztahovala pouze na počítačové systémy, jakožto na cíle útoku. Označení „počítačová kriminalita“ evokuje představu, že trestný čin musí být spáchán na počítači nebo prostřednictvím počítače, nejčastěji počítače osobního (PC - Personal Computer). Takové chápání je dnes zjednodušující, zároveň i poněkud kvantitativně redukuje množství jevů, které lze pod pojem trestná činnost páchaná prostředky informačních a komunikačních technologií zahrnout. Mnohá technická zařízení v dnešní době, díky implementaci mikroprocesorů spolu s jejich miniaturizací, již dávno převzala funkci osobních počítačů (PC), aniž by byla sama za osobní počítače označována. Jedná se o hybridy plnící rozličné funkce, které dříve plnily speciální přístroje. Soudobá technická zařízení umožňující komunikaci mezi sebou a mezi jejich uživateli a jejichž konstrukce je vedena myšlenkou ALL-IN-ONE (vše v jednom) dosahují mnohem větších výpočetních výkonů, než nejmodernější výpočetní jednotky z první poloviny 90. let. A i tyto prostředky,21 přestože nejsou nazývány počítači, mohou být terčem trestné činnosti či prostředkem k jejímu spáchání. Z těchto důvodů se pojem „počítačová kriminalita“ či „počítačový trestný čin“ v dnešní době již v odborné literatuře téměř nepoužívá. Namísto pojmu „počítač“ je v dnešní době používán spíše výraz „informační a komunikační technologie“ (Information and Communiction Technology – ICT), resp. „trestné činy v ICT“.22

V roce 2000 vydala Rada Evropy definici počítačové kriminality pocházející ze Statutu Komise expertů pro zločin v kyberprostoru: „Trestný čin namířený proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestný čin v tradičním smyslu, při kterém je užito moderních informačních a komunikačních technologií.“ 23 Rámcové rozhodnutí Rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu označuje za „computer-related crime“ takové jednání, které směřuje proti počítači, či jednání, kde je počítač prostředkem ke spáchání trestného činu. Ze znění evropského zatýkacího rozkazu pak vychází i definice kyberkriminality. V mezinárodních úmluvách se pro trestnou činnost páchanou prostředky informačních technologií užívá nejčastěji pojem „kybernetická kriminalita“ a používání tohoto pojmu se z oblasti normativní přeneslo též do slovníku odborné veřejnosti. Pojem kyberkriminalita má obdobný charakter jako pojmy „násilná kriminalita“, „kriminalita mladistvých“, „ekonomická kriminalita“ apod. Takovýmito názvy jsou označovány skupiny trestných činů mající určitý společný faktor, jako např. způsob provedení, osobu pachatele (alespoň druhově) apod. Ve své podstatě přitom může jít o velmi různorodou směsici trestných činů, spojených oním společným faktorem (počítačem, programem, daty).“ 24 Při vymezení obsahu pojmu kybernetická kriminalita si je třeba uvědomit, že spolu s růstem možností využívání informačních a komunikačních prostředků roste i možnost jejich užívání (zneužívání) k páchání trestné činnosti. Proto v podstatě neexistuje jakási

univerzální, obecně přijímaná definice, která by rozsah a hloubku tohoto pojmu plně postihla. Jednu z možných definic počítačové či kybernetické kriminality je možné nalézt i ve Výkladovém slovníku kybernetické bezpečnosti:25 Kybernetická kriminalita - Cyber crime Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti.

Počítačová kriminalita / Kybernetická kriminalita - Computer crime / Cyber crime

Zločin spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený. Z těchto dvou definic je patrná snaha o vymezení všech aspektů kybernetické kriminality, avšak autoři se dopustili určitých nepřesností. Zaprvé využívají oba dva uvedené termíny jako synonymum, avšak v definici počítačová kriminalita pomíjí faktory, že počítač je zároveň cílem i prostředkem útoku. Obdobné problémy spojené s vlastním definováním pojmu kybernetická kriminalita je možné nalézt i jinde. Vzhledem ke snaze o definování pojmu kybernetické kriminality je vhodné využít Úmluvu Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001.26 Tato úmluva však vlastní pojem kyberkriminality nevymezuje. Definuje pouze opatření, která by měla být přijata ratifikující stranou na vnitrostátní úrovni. Tato opatření v oblasti trestního práva hmotného pak vymezují hrubý rámec trestných činů, které jsou považovány za kybernetické trestné činy.27 Toto rámcové vymezení (spolu s dalšími trestnými činy obsaženými v Dodatkovém protokolu Rady Evropy č. 189 k Úmluvě o kybernetické kriminalitě28) poskytuje základní prostor pro jednotnou právní unifikaci trestných činů, které je možné považovat za kybernetické, napříč jednotlivými zeměmi. Vlastní, mnohdy až velmi strohé vymezení daných trestných činů je věci spíše ku prospěchu, neboť nijak neomezuje vnitrostátní (podrobnější či rozpracovanější) implementaci těchto trestných činů, avšak zároveň zaručuje splnění minimálních požadavků (standardů) všemi ratifikujícími stranami. I z důvodu značné nejednotnosti v názorech na to, co vše je a co není kybernetická kriminalita, v následující části této kapitoly vymezím tento pojem, a to jak z hlediska pozitivního, tak negativního. Nejobecněji je možné kybernetickou kriminalitu definovat jako jednání namířené proti počítači, případně počítačové síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu. Neopomenutelnou skutečností pro to, aby bylo možné uplatnit definici kyberkriminality, je fakt, že počítačová síť, respektive kyberprostor je pak prostředím, v němž se tato činnost odehrává. Při definici pojmu kybernetická kriminalita je nutno v prvé řadě vymezit pojem kriminalita vůbec.

V souvislosti s provozem informačních systémů, výpočetní techniky či komunikačních prostředků dochází k celé řadě jednání, která jsou jistě nežádoucí, ale nejsou postižitelná prostředky trestního práva, přestože mohou být pro společnost značně nebezpečná (škodlivá). Taková jednání a priori nemohou být kvalifikována jako počítačová, informační či jakákoliv jiná kriminalita – nejsou totiž kriminalitou vůbec. Při definování pojmu kriminalita (přičemž tuto definici je možno podat z více úhlů pohledu - sociologicky, trestněprávně atd.) se opíráme o definici kriminality jako o souhrn všech jednání, která lze podřadit pod některou skutkovou podstatu, upravenou trestním zákonem.29 Podle tohoto vymezení tedy nejsou kriminalitou taková jednání, která nenaplňují žádnou skutkovou podstatu trestného činu, tedy ani přestupku či jiného správního deliktu. Takové vymezení pojmu kriminalita je poměrně přesné a lze s ním vystačit i v oblasti informační a komunikační techniky. Pro páchání trestných činů v oblasti ICT je však charakteristické, že mnohdy jsou v rámci jejich spáchání používány takové postupy či prostředky, jejichž užití nenaplňuje žádnou skutkovou podstatu trestného činu, avšak jsou nedílnou součástí či předpokladem pro jednání další, které již postižitelné prostředky trestního práva je.30 Navíc tyto netrestné postupy či prostředky představují v procesu odhalování a objasňování trestné činnosti důležité komponenty, jejichž identifikace a pochopení hraje významnou roli při odhalování pachatelů tohoto druhu trestné činnosti.31 Kybernetická kriminalita, resp. kybernetická trestná činnost, představuje jakousi nejširší množinu pro veškerou trestnou činnost, ke které dochází v prostředí informačních a komunikačních technologií. Delikty páchané v rámci této množiny je možno podle různých hledisek dále třídit a označovat různými pojmy. „Internetová kriminalita“, „e-kriminalita“, „kyberterorizmus“ či např. „pirátství“ pak mohou tvořit podmnožiny kybernetické trestné činnosti, přičemž tímto výčtem nedochází k vyčerpání možných podmnožin jednání, které je možné pod pojem kyberkriminalita podřadit. Pod označením kybernetická kriminalita bývají v odborných publikacích nejčastěji označena taková kriminální jednání, při kterých jsou prostředky informačních a komunikačních technologií:

a) užity jako nástroj pro spáchání trestného činu,

b) cílem útoku pachatele, přičemž tento útok je trestným činem.

Takové vymezení kybernetické kriminality však v dnešní době již neobstojí. Zahrnovalo by totiž i takové trestné činy, při kterých sice dojde k použití informačních technologií, avšak nikoliv v kontextu jejich běžného užívání či určení

(např. jde o případy, kdy pachatel ublíží poškozenému na zdraví úderem monitoru či jinou součástí počítače do temene hlavy v úmyslu způsobit ublížení na zdraví; nebo půjde o krádež nákladního automobilu převážejícího počítačové komponenty apod.). Jde o trestné činy, kde je ICT využito mimo svůj rámec určení – např. jako zbraň, jako věc, která má určitou hodnotu vyjádřitelnou penězi, bez ohledu na to, za jakým účelem slouží nebo má sloužit. Při odhalování a objasňování těchto činů se uplatní jiné metodiky vyšetřování (např. metodika vyšetřování krádeží apod.), nikoliv metodika vyšetřování kybernetické kriminality. Aby bylo možno hovořit o kybernetické kriminalitě, musí být informační a komunikační technologie, které byly ke spáchání trestného činu užity nebo které byly cílem takového činu, zasazeny do určitého kontextu. V tomto duchu je tedy ke dvěma výše uvedeným bodům nutno přiřadit ještě jeden bod, obsahující tuto podmínku. Kybernetická kriminalita pak tedy představuje takovou kriminalitu, kde jsou prostředky informačních a komunikačních technologií:

a) užity jako nástroj pro spáchání trestného činu,

b) jsou cílem útoku pachatele, přičemž tento útok je trestným činem, za podmínky, že jsou tyto prostředky užity či zneužity v informačním, systémovém, programovém či komunikačním prostředí (tedy v kyberprostoru).

Takové vymezení kybernetické kriminality je však stále ještě nedostatečné. Za použití takto stanovených kritérií pro určení, zda je či není konkrétní jednání možno považovat za kybernetickou kriminalitu, dojdeme k závěru, že např. hlediska vymezení účastenství ve smyslu § 24 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů,32 je možné spáchat každý úmyslný trestný čin pomocí informačních prostředků (např. osoba přiměje pomocí e-mailových zpráv jiného ke spáchání úmyslného trestného činu vraždy). Obdobně tomu bude i u jiných forem trestné součinnosti (např. podněcování, schvalování trestného činu). Ty lze též spáchat prostřednictvím informačních technologií. Takováto jednání však za kybernetickou kriminalitu označit nelze. Ve svém důsledku by akceptace opačného názoru vedla k jedinému možnému závěru - každý trestný čin, při jehož spáchání pachatel použil jakýmkoliv způsobem informační a komunikační technologie, je kybernetickou kriminalitou. Z tohoto hlediska by se pak těžko hledaly trestné činy, které za kyberkriminalitu považovat nelze. Z uvedeného vyplývá, že kybernetickou kriminalitu nepostačí vymezit pouze pozitivně, ale je nutno ji vymezit i výčtem jednání, která zásadně za kybernetickou kriminalitu považovat nelze. Určitý pokus o takové vymezení je možno nalézt v jednom z dokumentů Odboru bezpečnostní politiky Ministerstva vnitra z roku 2006, který vymezuje trestnou činnost na úseku informačních technologií jako „…páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem s výjimkou majetkové trestné činnosti, nebo jako nástroj trestné činnosti.“ 33 S tímto negativním vymezením je možno souhlasit jen částečně. Mezi trestné činy hlavy V. trestního zákoníku, tedy mezi majetkové trestné činy, jsou totiž zařazeny i skutkové podstaty trestných činů, které slouží přímo k ochraně informačních a komunikačních technologií (respektive počítačových systémů), jejich součástí, dat na nich uložených, což jsou typické příklady kybernetické trestné činnosti. V tomto duchu pak bude možno pod pojem kybernetická kriminalita zařadit trestné činy tří různých kategorií:

1) trestné činy, jejichž individuálním objektem charakterizujícím skutkovou podstatu je přímo ochrana počítačového systému, jeho vybavení a součástí před specifickými druhy útoku resp. oprávněné zájmy osob na nerušené užívání těchto technických prostředků,

2) trestné činy, kde je způsob spáchání prostřednictvím informační a komunikační techniky jedním ze znaků skutkové podstaty,

3) ostatní v úvahu připadající trestné činy, které nespadají do první ani druhé kategorie, avšak které mohou být v konkrétním případě též spáchány prostřednictvím informačních technologií a které odpovídají výše uvedené definici, neboť v rámci jejich odhalování a objasňování se mohou uplatnit obdobné postupy jako při vyšetřování trestných činů z 1. a 2. kategorie (např. obdobně zaměřené znalecké posudky).

Klasifikace forem kyberkriminality

Domnívám se, že pokud se chceme zabývat problematikou kyberkriminality, bylo by vhodné alespoň rámcově vymezit, co vše je možné pod tuto trestnou činnost zahrnout. Na závěr této subkapitoly chci proto čtenáři předložit některé klasifikace kybernetické (či počítačové) kriminality tak, jak je vnímají různé právní normy, různí autoři, či organizace, které se věnují boji s kybernetickou kriminalitou. Na těchto členěních chci demonstrovat i genezi pohledu na problematiku kybernetické kriminality.

1. Klasifikace dle Úmluvy o kyberkriminalitě a dle dodatkového protokolu.

Úmluva o kyberkriminalitě dělí kybernetické trestné činy do čtyř kategorií:

1) trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů (Offences against the confidentiality, integrity and availability of computer data and systems),
2) trestné činy související s počítači (Computer-related offences),
3) trestné činy související s obsahem (Content-related offences),
4) trestné činy související s porušováním autorských práv a práv souvisejících (Offences related to infringements of copyright and related rights).
Dodatkový protokol pak definuje další kybernetické trestné činy:
1) šíření rasistických a xenofobních materiálů pomocí počítačových systémů (Dissemination of racist and xenophobic material through computer systems),
2) rasisticky a xenofobně motivované vyhrožování (Racist and xenophobic motivated threat),
3) rasisticky a xenofobně motivované útoky (Racist and xenophobic motivated insult),
4) popírání, snižování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti (Denial, gross minimisation, approval or justification of genocide or crimes against humanity).

2. Klasifikace Commitee of Experts on Crime in Cyberspace

Dle Statutu Komise expertů Rady Evropy pro zločin v kyberprostoru (Commitee of Experts on Crime in Cyberspace) z roku 2000 lze kyberzločin rozdělit:

1) Dle pozice počítače při páchání trestné činnosti:
◦ cíl (terč) útoku;
◦ prostředek (nástroj) útoku.
2) Podle typu činu:
◦ protiprávní jednání tradiční (např. padělání bankovek aj.)
◦ protiprávní jednání nová (např. phishing, DDoS aj.)34

3. Klasifikace dle eEurope+

Tento dokument členil počítačové zločiny na:

1) Zločiny porušující soukromí
◦ Nelegální sběr, uchovávání, modifikace, zveřejňování a šíření osobních dat.
2) Zločiny se vztahem k obsahu počítače
◦ Dětská pornografie, rasizmus, vyzývání k násilí aj.
3) Ekonomické
◦ Neautorizovaný přístup, sabotáž, hackerství, šíření virů, počítačová špionáž, počítačové padělání a podvody.
4) Zločiny se vztahem k duševnímu vlastnictví35

4. Klasifikace počítačové trestné činnosti dle kriminalistiky

Porada a Konrád36 dělí počítačovou kriminalitu do pěti základních skupin.

1) Neoprávněné zásahy do vstupních dat
◦ změna vstupního dokladu pro zpracování počítačem,
◦ vytvoření dokladu obsahujícího nepravdivé údaje pro následné zpracování dat počítačem,
2) Neoprávněné změny v uložených datech
◦ manipulace s daty, neoprávněný zásah do nich a následný návrat k normálu,
3) Neoprávněné pokyny k počítačovým operacím
◦ přímý pokyn k provedení operace, či instalace softwaru provádějícího operace automaticky,
4) Neoprávněné pronikání do počítačů, počítačového systému a jeho databází
◦ informativní vstup do databáze, bez využití informací,
◦ neoprávněné užívání informací pro vlastní potřeby,
◦ změny, ničení, či nahrazování informací jinými,
◦ nelegální „odposlech“ a záznam provozu elektronické komunikace,
5) Napadení cizího počítače, programového vybavení a souborů a dat v databázích
◦ vytváření programů sloužících k napadení,
◦ zavedení viru do programového vybavení počítače,
◦ vlastní napadení viry, či jinými programy.37

5. Zaměření Europolu na některé druhy kyberkriminality dle závažnosti

Europol respektuje Úmluvu o kyberkriminalitě a vychází z členění trestných činů v ní obsažených. Pro podporu boje s kyberkriminalitou a pomoc členským státům došlo, v rámci Europolu ke vzniku The European Cyber Crime Centre

(EC3).38 Tento tým jasně deklaroval svoje pole působnosti v rámci boje s kybernetickou trestnou činností a vymezil následující tři oblasti (FP – focal point), kterým se věnuje:

1) **FP TERMINAL – Payment fraud**. Skupina, která se věnuje a poskytuje podporu při řešení online podvodů.
2) **FP Cyborg** – High-Tech Crimes. Skupina, která se věnuje a poskytuje podporu při různých kybernetických útocích, jež ovlivňují kritickou infrastrukturu39 a informační systémy. Zejména se jedná o útoky typu: Malware, Ransomware, Hacking, Phishing, Identity Theft aj.
3) **FP Twins – Child Sexual Exploitation**. Skupina, která se věnuje a poskytuje podporu při vyšetřování trestné činnosti, při níž dochází k sexuálnímu zneužívání dětí.

Další možné klasifikace kyberkriminality

Existuje i mnoho jiných způsobů klasifikace, pro ilustraci uvádím další možné dělení kyberkriminality
Na tomto místě si dovolím uvést i klasifikaci, kterou jsem vytvořil na základě vlastních poznatků získaných zejména při interpretaci problematiky kyberkriminality na různých seminářích či konferencích. Je možné konstatovat, že velmi zjednodušeně lze kyberkriminalitu dělit ze tří hledisek:

1) Dle četnosti (povahy) útoků:

a) **porušování práv autorských** (viz kap. 4.10 Internetové (počítačové) pirátství. Jde o jednání, které je v rámci kyberprostoru dominantní a při kterém dochází k porušování intelektuálního vlastnictví. Snaha o potírání tohoto jevu je zjevná zejména za strany soukromých organizací hájících práva autorů.);
b) **ostatní kybernetické útoky** (viz kap. 4 Projevy kyberkriminality. Vyjma kap. 4.10 Internetové (počítačové) pirátství.).

2) Dle postižitelnosti trestním právem:

a) **trestním právem řešené jednání** (viz kap. 5.2.2 Kvalifikace kybernetických útoků dle Úmluvy o kyberkriminalitě, Dodatkového protokolu a dle trestního zákoníku – některé z uvedených jednání subsumovatelných pod skutkovou podstatu trestného činu);
b**) trestním právem neřešené (nepostižitelné) jednání** (některé z uvedených jednání není možné, ani za použití přípustné analogie,41 subsumovat pod zákonné znaky skutkové podstaty trestného činu. Jedná se například o jednání popsaná v kap. 4.5 Spam a kap. 4.12 DoS, DDoS, DRDoS útoky).

3) Dle míry tolerance většinovou společností:

a) společností tolerované jednání (nejvíce je tolerováno již zmiňované Internetové (počítačové) pirátství);
b) společností neakceptované jednání (např. dětská pornografie - viz kap. 4.13 Šíření závadového obsahu aj.).

1.2 Pojmy související s kybernetickou trestnou činností

1.2.1 Kyberprostor (Cyberspace)

„Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat. Jako světla města, ...“
William Gibson: Neuromancer (1984)

Kyberprostor představuje ono pomyslné pískoviště, na kterém se pohybujeme, ale zároveň se jedná o klíčový prvek v definici kybernetické kriminality. Aby bylo možné definovat kyberprostor, je nezbytně nutné vymezit pojem Internet, který právě s kyberprostorem bezprostředně souvisí.42 Světové počátky Internetu, který je nezbytnou materiální podstatou kyberprostoru, se datují do 50. let 20. století.43 V té době došlo k budování a testování sítí propojených počítačů především pro vědeckovýzkumné a vojenské účely. Ačkoli byl Internet vybudován na základech sítí ARPANET a NSFNET,44 v současné době není nikdo vlastníkem Internetu a neexistuje ani centrální autorita či instituce, která by jej řídila. „Přesto existují instituce podílející se významnou měrou na fungování a dalším rozvoji Internetu. Jako první jmenujme Internet Society (ISOC), jenž sdružuje internetové uživatele. ISOC má dvě hlavní složky, Internet Activities Board (IAB) a Internet Engeneering Task Force (IETF). Obě tyto složky spolupracují s nejvýznamnějšími počítačovými firmami na tvorbě standardů potřebných pro další rozvoj Internetu.“ 45

Osobně se však domnívám, že výsostné postavení v rámci sítě Internet má sdružení ICANN46 (Internet Corporation for Assigned Names and Numbers). Do náplně činnosti tohoto sdružení totiž spadá stanovení pravidel pro provoz systému doménových jmen. V současné době se však do popředí stále více dostávají, a větší úlohu hrají ISP.47 Materiální (hmotnou) podstatou Internetu je jeho páteřní síť, která vede signál (data) vzduchem, kabely, či jinými přenosovými médii. Technicky se jedná o celosvětovou distribuovanou počítačovou síť složenou z jednotlivých menších sítí, které jsou navzájem spojeny pomocí protokolů IP a tím je umožněna komunikace, přenos dat, informací a poskytování služeb mezi subjekty navzájem. Tím je vlastně vytvořen dynamický, neustále se měnící a vyvíjející systém vázaný na hardware, avšak zároveň vytvářející těžko definovatelný a prakticky neomezený kyberprostor. Lze říci, že kyberprostor je virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném. Vzniká tak zajímavý paradox, který sice umožňuje existenci nehmotného média (kyberprostoru), schopného se, díky distribuovanosti hmotného média (prvků sítě, jednotlivých počítačových systémů, cloudových úložišť, propojených služeb, atd.), adaptovat a měnit v případě poškození materiálního média, avšak v případě úplného kolapsu materiálního média (respektive všech jeho součástí) dojde k nevratnému poškození, či zániku kyberprostoru jako takového. Kyberprostor je také možné definovat jako prostor kybernetických aktivit či jako prostor vytvořený informačními a komunikačními technologiemi, který vytváří virtuální svět (či prostor) jako paralelu k prostoru reálnému. Pokud jde o legální definici kyberprostoru, je možné využít například znění § 2 písm. a) ZKB, kde je uvedeno, že „kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“ Do obecného povědomí se pojem kyberprostor začíná dostávat po vydání deklarace Johna Barlowa (zakladatele Electronic Frontier Foundation): „A Declaration of the Independence of Cyberspace“: „Vlády Průmyslového světa, vy znavení obři z masa a oceli, přicházím z Kyberprostoru, nového domova Mysli. Jménem budoucnosti vás žádám, abyste nás vy, lidé minulosti, nechali na pokoji. Nejste mezi námi vítáni. Vaše svrchovanost nesahá do míst, kde se scházíme. Nemáme žádnou volenou vládu a nejspíše ani žádnou mít nebudeme, proto k vám promlouvám s autoritou o nic větší než tou, se kterou vždy mluví sama svoboda. Prohlašuji námi budovaný globální společenský prostor za přirozeně nezávislý na tyraniích, do kterých se nás snažíte uvrhnout. Nemáte žádné morální právo nám vládnout a nemáte ani žádné donucovací prostředky, kterých bychom se skutečně museli obávat. Vlády odvozují svou spravedlivou moc od souhlasu podřízeného lidu. O náš souhlas jste nežádali a ani jste žádný nedostali. Nezvali jsme vás. Neznáte nás a neznáte ani náš svět. Kyberprostor neleží uvnitř vašich hranic. Nemyslete si, že ho můžete budovat, jako by to byl nějaký veřejný stavební projekt. Nemůžete. Je to přírodní jev, který roste prostřednictvím našich společných činů. Nezapojili jste se do našeho velkého podmanivého dialogu a nevytvořili jste ani bohatství našich trhů. Neznáte naši kulturu, naše mravy, ani nepsané zákony, které naší společnosti již teď dodávají větší řád, než by mohlo přinést kterékoliv vaše nařízení. Tvrdíte, že mezi námi jsou problémy, které vy musíte vyřešit. Tohle tvrzení využíváte jako záminku, abyste mohli vtrhnout do našeho výsostného prostoru. Spousta těch problémů vůbec neexistuje. Pokud vzniknou skutečné spory, pokud nastanou křivdy, sami je odhalíme a vyřešíme vlastními prostředky. Vytváříme svou vlastní Společenskou smlouvu. Tohle zřízení vznikne podle podmínek našeho světa, ne toho vašeho. Náš svět je jiný. Kyberprostor sestává z transakcí, vztahů a myšlenek vůbec, uspořádaných jako stojatá vlna v síti našich komunikací. Náš svět je zároveň všude a nikde, ale není tam, kde žijí tělesné schránky. Vytváříme svět, kam mohou všichni vstoupit bez výsad a předsudků spjatých s rasou, ekonomickou mocí, vojenskou silou nebo místem narození. Vytváříme svět, ve kterém může kdokoliv a kdekoliv vyjádřit své přesvědčení, jakkoliv ojedinělé, aniž by se musel bát, že bude násilím umlčen nebo donucen se přizpůsobit. Vaše právní koncepty majetku, projevu, totožnosti, pohybu a kontextu se na nás nevztahují. Všechny jsou založené na hmotě, a tady žádná hmota není. Naše identity nemají tělesné schránky, takže na rozdíl od vás nemůžeme zjednat pořádek pomocí fyzického násilí. Věříme, že naše zřízení se vyvine z mravů, osvíceného osobního zájmu a veřejného prospěchu. Naše identity mohou být rozeseté do spousty vašich právních řádů. Všechny naše dílčí kultury budou obecně uznávat jen jediný zákon, Zlaté pravidlo. Doufáme, že naše vlastní řešení problémů budeme moci vybudovat na jeho základě. Jenže nemůžeme přijmout řešení, která se nám snažíte vnutit. Ve Spojených státech jste dnes vytvořili Zákon o reformě telekomunikací, který popírá vaši vlastní Ústavu a uráží ideály Jeffersona, Washingtona, Milla, Madisona, DeToquevilla a Brandeise. Tyto ideály se teď musejí znovu zrodit v nás. Děsíte se svých vlastních dětí, protože jsou domorodci ve světě, kde vy budete vždy jen přistěhovalci.

Protože se jich bojíte, svěřujete svým byrokratickým aparátům rodičovské povinnosti, ke kterým nemáte odvahu postavit se čelem. V našem světě jsou všechny postoje a projevy lidstva, od těch nejpokleslejších až po ty nejvznešenější, součástí jediného nedělitelného celku, globálního dialogu bitů. Není možné oddělit dusivý vzduch od vzduchu, o který se opírají křídla. V Číně, Německu, Francii, Rusku, Singapuru, Itálii a Spojených státech se snažíte zahnat virus svobody budováním strážných věží na hranicích Kyberprostoru. Ty sice nákazu mohou na krátkou chvíli

zadržet, jenže budou k ničemu ve světě, který brzy zaplaví bitonosná média. Váš zastarávající informační průmysl se bude snažit upevnit svou pozici navrhováním zákonů, v Americe i jinde, podle kterých by každé slovo na celém světě bylo jejich majetkem. Tyto zákony prohlásí všechny myšlenky jen za další průmyslový výrobek, o nic ušlechtilejší než surové železo. V našem světě se veškeré výtvory lidské mysli dají neomezeně reprodukovat a šířit s nulovými náklady. Globální výměna myšlenek se teď obejde bez vašich továren. Čím dál více nepřátelské a koloniální praktiky nás staví do stejné pozice, v jaké byli i ti předchozí milovníci svobody a sebeurčení, kteří museli odmítnout autoritu vzdálené neinformované mocnosti. Musíme svá virtuální já prohlásit za nedotknutelná vaší svrchovaností, přestože nadále přijímáme vaši nadvládu nad našimi tělesnými schránkami. Rozprostřeme se po celé Planetě, aby nikdo nemohl uvěznit naše myšlenky. V Kyberprostoru vytvoříme civilizaci Mysli. Nechť je lidštější a spravedlivější než svět, který v minulosti vytvořily vaše vlády. Davos, Švýcarsko 8. února 1996“ 48

Osobně jsem přesvědčen o tom, že i po dvaceti letech od vydání této deklarace je její text více než aktuální. Současná společnost se snaží reagovat na obrovský rozmach informačních a komunikačních technologií, jejich vzájemné prolínání a propojování, vznik nových trendů aj. Tato reakce je však mnohdy primárně postavena na vynucování a restrikci, než na pochopení a výchově uživatelů. Kyberprostor, oproti světu reálnému, je značně specifický a rozhodně je mylné se domnívat, že v něm budou fungovat stejná pravidla, jako ve světě reálném. Obecně je sice možné konstatovat, že na kyberprostor lze aplikovat standardní kritéria,49 která jsou uplatňována v návaznosti na skutečnou fyzickou lokalizaci dat či informací. Druhou možností je vytvoření nových kritérií, pro aplikaci principu místní působnosti (jedná se o virtuální lokalizaci právních vztahů).50 Pro kyberprostor je příznačné, že se do něj propojila značná část společnosti (odhaduje se zapojení přibližně 3,6 miliard obyvatel, přičemž celosvětová populace činí přibližně 7,4 miliard obyvatel).51 Zároveň je třeba konstatovat, že k masovému zapojení společnosti začalo docházet teprve před cca 15–20 lety. Mezi znaky kyberprostoru je možné zařadit jeho decentralizovanost, globálnost, otevřenost, bohatost na informace (a to včetně informací v podobě „informačního smogu“, naprostých nesmyslů, polopravd a lží), interaktivnost a možnost ovlivňování mínění skrze uživatele (avatary52). Podstatným charakterem kyberprostoru je, že primární roli v něm zaujímají technologie a na ně navázané služby. V poslední době se čím dál víc ukazuje, že projev světa virtuálního může a má dopady ve světě reálném.53 Rychlost a zejména dostupnost přenášených dat se stává klíčovým elementem dnešní doby. Uživatel zpravidla nechce a ani nemá snahu zjišťovat, kudy a jakým způsobem dochází k přenosu dat jím do informačních sítí vložených. Nezajímá ho ani, kde se nachází adresát přenášených dat, či kde jsou data uchovávána, tím dochází k odhmotnění obsahu od fyzické struktury informačních sítí. Na jednu stranu je možné sledovat situaci, kdy jsou společenské vztahy v kyberprostoru delokalizovány, 54 což s sebou přináší problémy z hlediska aplikace práva, avšak na stranu druhou tato delokalizace umožňuje uživatelům volně („svobodně“ a bez omezení v podobě hranic) komunikovat, zasílat, uchovávat a měnit data. Kyberprostor je možné si představit jako pomyslný ledovec, kde viditelná část představuje prostor, v němž se běžný uživatel pohybuje při své rutinní práci s ICT.

Obrázek 1: Zobrazení kyberprostoru

Tento ledovec55 lze rozdělit na následující tři části:

1) Surface Web,
2) Deep Web,
3) Dark Web.

Deep a Dark Weby jsou také často souhrnně označovány jako D4rkN3ts – Darknets. Všechny tyto součásti pak společně vytváří skutečný kyberprostor.
Surface Web (také označován jako Visible Web, Clearnet, Indexed Web aj.) je ta součást kyberprostoru, která je dostupná většinové společnosti a lze se v ní „pohybovat" za použití standardních prostředků (např. webových prohlížečů aj.). Tato část kyberprostoru v sobě obsahuje služby (stránky), jako jsou např. Google, Facebook, YouTube, Seznam aj. Surface web pak spadá do správy ICANN a má jasně danou strukturu.57

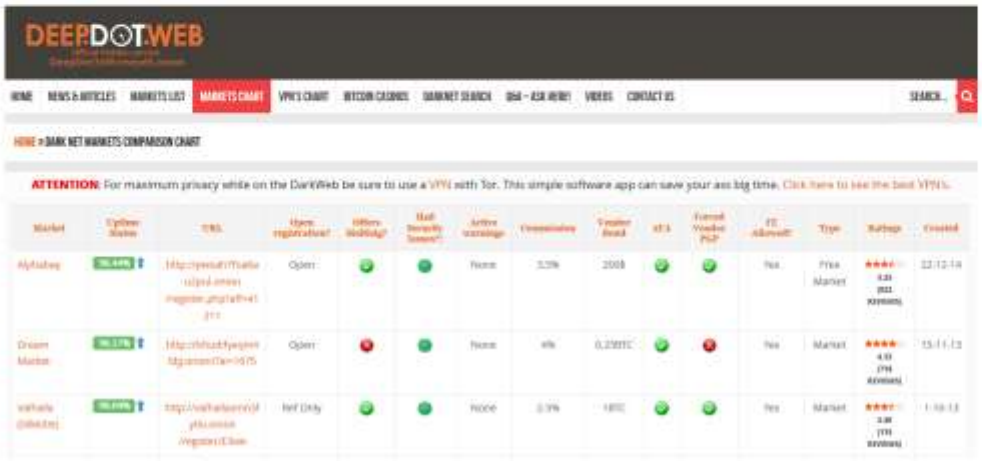
Na tomto místě je vhodné zmínit se i o intranetu, respektive o privátních či poloprivátních částech kyberprostoru. Intranet je typicky využíván jako firemní či podniková, počítačová síť (tj. umožňující komunikaci mezi subjekty navzájem, jakož i umožňující přenos dat a informací), avšak tato síť, či její prvek není veřejně dostupný. Tím částečně dochází k vytváření Deep Webu, jakožto jedné ze součástí kyberprostoru. Je třeba si uvědomit, že Darknets nejsou separátní fyzickou sítí, ale že se jedná o aplikační vrstvu v rámci existujících sítí a služeb. Rozdíl spočívá především v indexaci obsahu. Surface web představuje onu indexovanou část kyberprostoru, avšak tato indexace činí přibližně pouhé 4 % z celkového objemu kyberprostoru. Oněch 96 % obsahu pak připadá právě na Darknets. Jsem přesvědčen o tom, že je třeba vymýtit tvrzení, která přirovnávají Darknet k prostředí, v němž se nemáte pohybovat. Stejně jako budete ve světě reálném vykázáni z určité oblasti, protože tam například probíhá demolice, tak je vhodné respektovat určitá doporučení a omezení i ve světě virtuálním. Pro pohyb v kyberprostoru je třeba pochopit základní principy, na nichž funguje připojení vašeho počítačového systému do tohoto prostředí58 a stejně tak je třeba znát podstatu a pravidla poskytovaných či nabízených služeb. Například vytvořením své soukromé VPN59 mezi dvěma specifickými počítačovými systémy již vstupujete do prostředí Darknetu. Avšak bez tohoto připojení se v mnoha společnostech nejste schopni připojit k pracovnímu počítači, nebo nemůžete navštívit své oblíbené sociální sítě například z území Čínské lidové republiky. Vždy pak vyvstane otázka: Je to hrozba? Pro řadu uživatelů budou Darknets vždy představovat hrozbu a nelze u nich změnit názor na to, že jde pouze o prostředí, kde se prodávají drogy, zbraně a dětská pornografie. Pro druhou skupinu lidí pak Darknets představují „…internet pod Internetem, jehož základní ideou je neregulované a necenzurované prostředí…" 60 a nástroj Tor Browser, běžný nástroj umožňující nesvobodným svobodnou komunikaci. Než něco odsoudíme, je vhodné se seznámit s podstatou fungování konkrétní věci. Při plném respektování minimálních základních pravidel Darknets nepředstavují takovou hrozbu, jak mnohá média prezentují.61 Řadu nástrojů a prostředků, pomocí nichž můžu páchat kybernetickou či jinou trestnou činnost, mohu zcela legálně získat i v rámci Surface Webu například na stránkách www.alibaba.com. Jen pro zajímavost si zkuste zadat do vyhledávače na této stránce výraz card skimmer. Nemíním nikoho navádět k páchání trestné činnosti, jen se snažím poukázat na to, že pokud se někdo rozhodne spáchat trestný čin, pak si prostředek k jeho spáchání může obstarat kdekoliv. Na druhou stranu je třeba objektivně přiznat, že v oblasti Dark Webu je možné snadněji narazit na všechny výše zmiňované negativní jevy, jako je prodej drog, dětská pornografie aj. Princip fungování Darknetu je zpravidla postaven na připojení se na bázi Friend-to-friend (F2F) / Peer-to-peer (P2P). Mezi nejznámější „anonymní sítě", či anonymizéry patří: Freenet62 a TOR project.63 Asi nejznámějším příkladem tržiště v rámci Darknetu, byl Silk Road (http://silkroad6ownowfk. onion, zakladatel: Ross Ulbricht, screen stránky Silk Road je uveden na obrázku č. 2 - Tržiště Silk Road), který zahájil svoji činnost v roce 2011 a uzavřen byl v říjnu 2013 v rámci akce FBI. Podstatou Silk Roadu byla snaha o zachování anonymity jak prodávajícího, tak kupujícího. Transakce byly hrazeny prostřednictvím virtuální měny (v tomto případě Bitcoin64) a účty, jež si jednotliví uživatelé zakládali, byly fiktivní. Rozmach Silk Roadu byl spojen především s prodejem drog a s teritoriálním umístěním většiny uživatelů (USA – distribuce zakoupených drog pak zpravidla nenarážela na problémy teritoriality a s nimi spojené procedury, jako je celní kontrola zboží převáženého mezi jednotlivými suverénními státy). Nicméně kromě drog bylo možné na tomto tržišti získat například kradený software; ukradené přihlašovací údaje k e-mailovým adresám, sociálním účtům; falešné či kradené občanské a řidičské průkazy, pasy; kreditní karty; zbraně; padělané zboží všeho druhu aj. Různé zdroje uvádí,65 že obrat stránky (po dobu jejího fungování) činil okolo 9 519 664 Bitcoinů a bylo zde 957 079 registrovaných uživatelů.

Obrázek 2: Tržiště Silk Road

V rámci služby Silk Road byl vždy určitý poplatek z každé transakce připsán na účet Rosse Ulbrichta. Ulbricht byl obviněn z praní špinavých peněz, obchodování s drogami, protivládní konspiraci a hackerství. FBI zajistilo Bitcoiny (26 000 BTC) v hodnotě přibližně 4 milionů dolarů a byly zajištěny finanční prostředky Rosse Ulbrichta pocházející z této trestné činnosti. Po uzavření Silk Road založili stejní administrátoři, ještě v roce 2013, tržiště Silk Road 2.0. Toto tržiště bylo uzavřeno v rámci společné akce Europolu a FBI dne 17. 10. 2014 (viz Obrázek 3). Dle vyjádření vyšetřovatelů66 docházelo v rámci tržiště Silk Road 2.0 k transakcím s měsíčním obratem přibližně 8 milionů dolarů, přičemž drogy činily až 70 % prodávaného zboží.

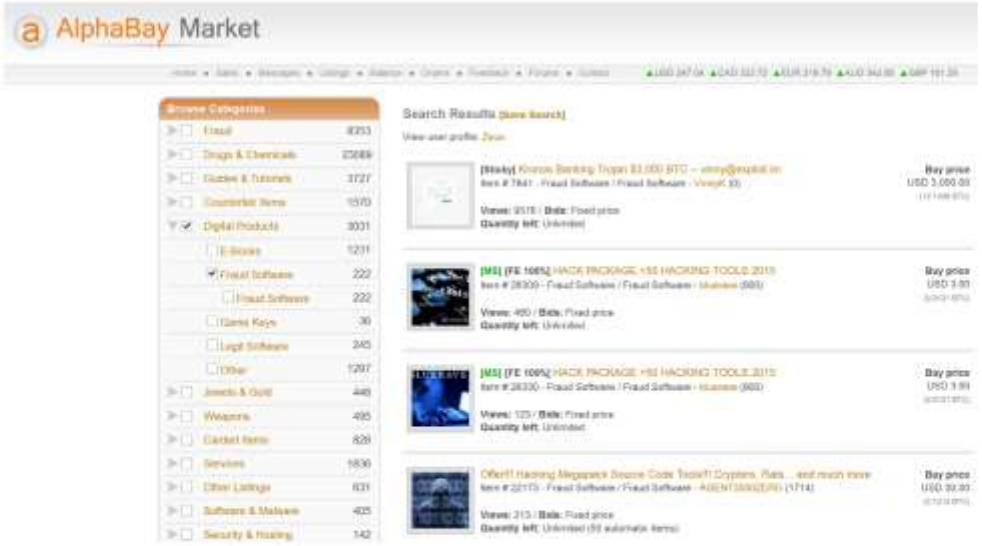
Obrázek 3: Printscreen zobrazující uzavření tržiště Silk Road 2.0

Praxe však ukazuje, že pokud ve virtuálním prostředí jednu službu zakáži nebo jinak znepřístupním, pak na její místo téměř okamžitě nastoupí služby nové, obdobné, mnohdy lépe zabezpečené. Jako příklad je možné uvést seznam tržišť, které fungují v Darknetu, a který naleznete na https://www.deepdotweb.com/dark-net-market-comparison-chart/.



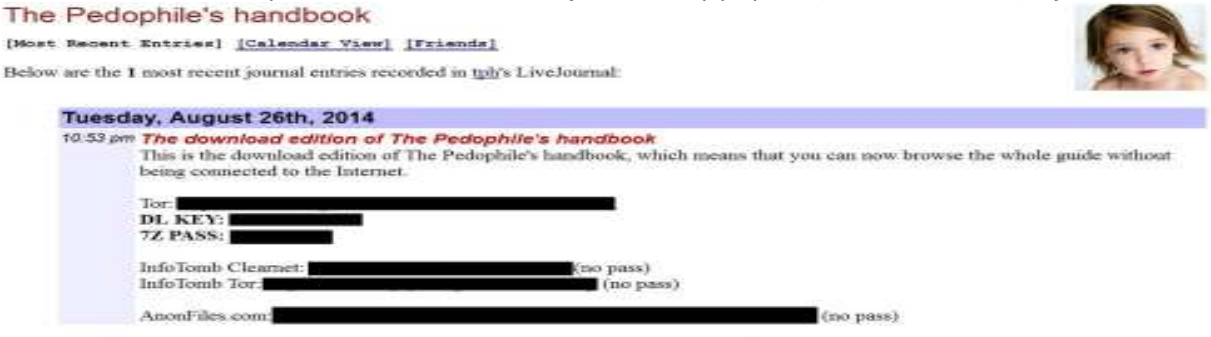
Obrázek 4: Seznam tržišť, které fungují v Darknetu

V současnosti je jedním z oblíbených tržišť tržiště Alphabay. V porovnání se Silk Road 1.0 a 2.0 je třeba konstatovat, že zde dochází k nabízení téměř identického zboží.

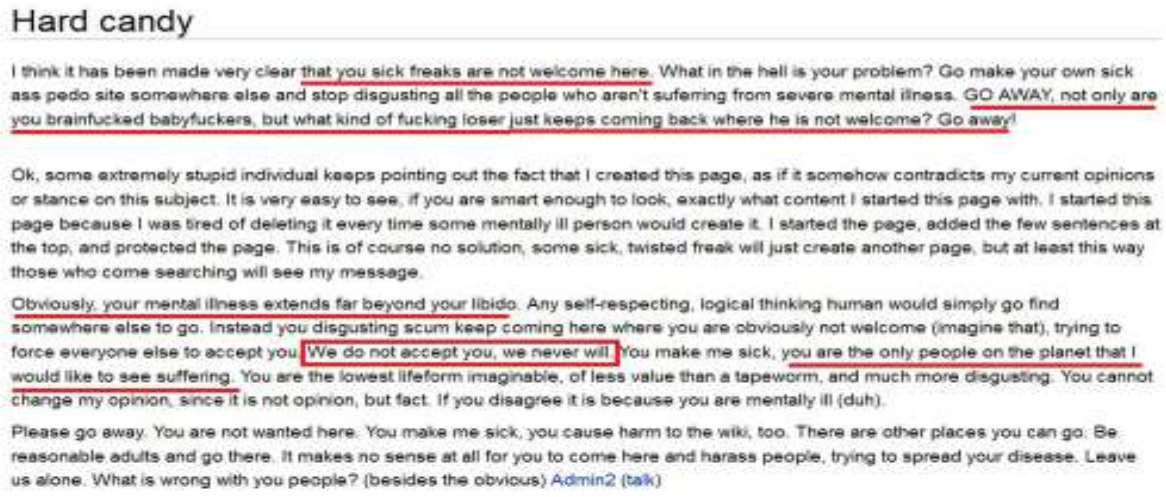


Obrázek 5: Nabídka malware na tržišti AlphaBay Market

Nicméně i v oblasti Dark Webu a aktivit zde prováděných je možné pozorovat určitý posun. Například v roce 2015 bylo možné na Hidden Wiki (http://kpvz7ki2v5agwt35.onion) nalézt návod i stránky na stažení The Pedophile's handbook (viz Obrázek 6). Nicméně správce Hidden Wiki se v současnosti jasně a velmi striktně distancuje od podobných aktivit (viz Obrázek 7 - Vyjádření správce The Hidden Wiki k vyhledávání dětské pornografie). Netvrdím, že tímto činem vymizí tisíce pedofilů či jiných osob, které se chtějí dopouštět trestné činnosti, z Dark Webu, avšak je možné pozorovat snahu uživatelů a správců o regulaci obsahu i v prostředí, kde de facto žádná regulace fungovat nemusí. Je mi jasné, že pod Dark Webem může vzniknout Dark Dark Web, či Pitch Black Web, ale i v tomto prostředí záleží na uživateli, správci a dalších osobách, jaké aktivity připustí (budou tolerovat) a jaké už ne.



Obrázek 6: The Pedophile's handbook



Hard candy

I think it has been made very clear that you sick freaks are not welcome here. What in the hell is your problem? Go make your own sick ass pedo site somewhere else and stop disgusting all the people who aren't suferring from severe mental illness. GO AWAY, not only are you brainfucked babyfuckers, but what kind of fucking loser just keeps coming back where he is not welcome? Go away!

Ok, some extremely stupid individual keeps pointing out the fact that I created this page, as if it somehow contradicts my current opinions or stance on this subject. It is very easy to see, if you are smart enough to look, exactly what content I started this page with. I started this page because I was tired of deleting it every time some mentally ill person would create it. I started the page, added the few sentences at the top, and protected the page. This is of course no solution, some sick, twisted freak will just create another page, but at least this way those who come searching will see my message.

Obviously, your mental illness extends far beyond your libido. Any self-respecting, logical thinking human would simply go find somewhere else to go. Instead you disgusting scum keep coming here where you are obviously not welcome (imagine that), trying to force everyone else to accept you. We do not accept you, we never will. You make me sick, you are the only people on the planet that I would like to see suffering. You are the lowest lifeform imaginable, of less value than a tapeworm, and much more disgusting. You cannot change my opinion, since it is not opinion, but fact. If you disagree it is because you are mentally ill (duh).

Please go away. You are not wanted here. You make me sick, you cause harm to the wiki, too. There are other places you can go. Be reasonable adults and go there. It makes no sense at all for you to come here and harass people, trying to spread your disease. Leave us alone. What is wrong with you people? (besides the obvious) Admin2 (talk)

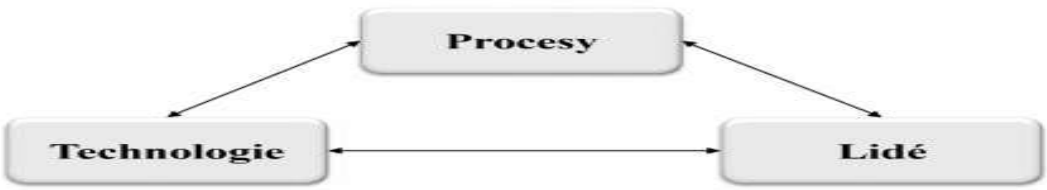
Obrázek 7: Vyjádření správce The Hidden Wiki k vyhledávání dětské pornografie

Na závěr chci říci, že je možné být anonymní, ovšem pouze za podmínky, že máte dostatečné znalosti ICT, Internetu, jste důslední a máte dostatek času a často i zdrojů. Avšak jako lidé často chybujeme a neuvědomujeme si, že anonymizace jednoho připojení není synonymem pro anonymizaci sítě. Je možné anonymizovat například připojení počítačového systému do počítačové sítě, avšak například využívané služby uchovávají a předávají informace o aktivitách uživatele a počítačovém systému jako takovém.67 Domnívám se, že je mnohem lepší pochopit, poznat a porozumět, než pouze zakazovat či nepovolovat. Veškeré tyto aktivity pouze zákonitě vzbudí touhu po zakázaném a neznámém. Cestou k poznání je podle mě pochopení alespoň základních principů, na nichž funguje svět ICT.

1.2.2 Kybernetický útok (Cyber attack)

Prosise a Mandiva charakterizují tzv. „počítačovou bezpečnostní událost“ (kterou lze chápat jako počítačový útok či počítačový trestný čin), jako nezákonnou, nepovolenou, neautorizovanou, nepřijatelnou akci, která zahrnuje počítačový systém či počítačovou síť. Tato akce může být zaměřena například na krádež osobních údajů, spam či jiné obtěžování, zpronevěru, šíření či držení dětské pornografie aj.69 Jirásek a kol. definují kybernetický útok, jako: „Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“ 70 Takovéto vymezení kybernetického útoku by bylo značně zužující a nepostihující všechny negativní aktivity uživatelů kyberprostoru, 71 zejména z toho důvodu, že kumulativně slučuje podmínky poškození IT a získání informací. Kybernetickým útokem přitom může být i jednání v podobě sociálního inženýrství,72 kde je jediným cílem získat informace, či naopak útok DoS, či DDoS,73 kde může být jediným cílem potlačení (tedy nikoliv poškození) funkčnosti jednoho či více počítačových systémů, případně poskytovaných služeb. Na základě výše uvedeného je tedy možné kybernetický útok74 definovat jako jakékoli protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby. 75 Tato jednání nemusí mít vždy podobu trestného činu, podstatné je, že narušují běžný způsob života poškozeného. Kybernetický útok může být dokonán, stejně jako může být ve stádiu přípravy či pokusu.76 Kybernetický trestný čin musí být zároveň kybernetickým útokem, avšak ne každý kybernetický útok musí být trestným činem. Řadu kybernetických útoků je, i díky absenci trestněprávní normy, možné subsumovat pod jednání, které bude mít povahu správněprávního, či občanskoprávního deliktu, případně se nemusí jednat o jednání, které je postižitelné jakoukoli právní normou (může jít např. pouze o nemorální či nechtěné jednání).

Úspěšnost kybernetického útoku typicky spočívá v porušení některého z prvků, které tvoří kybernetickou bezpečnost (lidé, procesy a technologie). Tyto prvky je třeba uplatňovat, případně modifikovat v průběhu celého jejich životního cyklu. Zejména jde o prevenci, detekci a rekci na útok.77 Bezpečnost IT, informací a dat je také přímo závislá na repektování principů „C“ „I“ „A“.78



Obrázek 8: Prvky kybernetické bezpečnosti

Pokud chceme definovat pojem kybernetický útok, je vhodné využít i definice, které vyplývají ze zákona o kybernetické bezpečnosti. Tento zákon totiž definuje v § 7 pojmy kybernetická bezpečnostní událost a kybernetický bezpečnostní incident. Kybernetickou bezpečnostní událostí je „událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.“ De facto jde o událost bez zatím reálného negativního následku pro daný komunikační nebo informační systém, ve své podstatě se jedná pouze o hrozbu, která však musí být reálná. Kybernetickým bezpečnostním incidentem je „narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.“ Kybernetický bezpečnostní incident tak představuje samotné narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací, tj. narušení informačního nebo komunikačního systému s negativním dopadem.

1.2.3 Počítač (Počítačový systém)

Pojmy počítač a počítačový systém jsou na tomto místě uváděny a vysvětlovány záměrně, neboť i když může být na první pohled patrné, že se jedná o notoriety, trestní zákoník tyto pojmy užívá79 a jejich vymezení z pohledu práva nemusí být vždy jednoznačné. Existuje celá řada definic pojmu počítač.

1) Za počítač je možné označit zařízení, které se vyznačuje následujícími rysy: zařízení obsahuje centrální procesorovou jednotku, schopnou řídit se programovým kódem a schopnou ovládat přidružené periferie a další části počítače; dále zařízení obsahuje médium pro ukládání dat (paměť, disk aj.). Mezi nepovinné prvky počítače se pak řadí zařízení pro vstup dat (klávesnice, myš aj.), zobrazovací zařízení (nejčastěji se jedná o monitor, ale může se jednat i o projektor či jiné zobrazovací zařízení) a jiné periferie.80

2) Počítačem je funkční jednotka schopná provádět rozsáhlé výpočty, včetně mnoha aritmetických a logických operací, bez zásahu člověka.81

3) Počítačem je každá funkční jednotka schopná provádět výpočty a operace bez lidského zásahu a podle určitého programu, zařízení na zpracování, uchovávání a využívání dat, která převádí na číselné kódy.82

4) Jde o soubor technického vybavení (hardware) schopného vyplňovat posloupnost předem stanovených příkazů. Tyto příkazy jsou ve formě programu nebo sady programů (software).

5) „V nejobecnějším smyslu lze za počítač považovat přístroj, který může být naprogramován za účelem samostatné realizace aritmetických a logických operací.“ 83

6) „Elektronické zařízení, které je schopné přijímat informace (data) v určité formě a provádět sekvenci operací v souladu s předem nastavenou, ale variabilní sadou procesních instrukcí (program) za účelem vytvoření výsledku ve formě informací nebo signálů.“ 84

Veškerá činnost počítače musí být předem naprogramována. Počítač je prostřednictvím paměťových médií schopen uchovávat informace, které do něj mohou být vkládány, zpracovávány a transformovány, nebo je počítač může zpětně poskytovat ve vnímatelné podobě (na zobrazovacím zařízení, jako zvukové signály, případně jako určité činnosti při řízení výrobních procesů). Pojem počítačový systém je pojmem, který je využíván trestním zákoníkem a který byl do našeho právního řádu včleněn na základě ratifikace Úmluvy o kyberkriminalitě. V čl. 1 písm. a) této Úmluvy je definován počítačový systém jako „jakékoli zařízení nebo skupina propojených nebo přidružených zařízení, z nichž jedno nebo více provádí automatické zpracování dat podle programu.“ Počítačový systém je tedy funkční jednotkou, která je složena z jednoho nebo více počítačů a přidruženého software, využívající paměťové médium pro všechny, nebo část programů a dat nezbytných pro vykonání programů. Počítačový systém může být samostatnou funkční jednotkou (pracující samostatně - např. osobní počítač, notebook, smartphone aj.), nebo může jít o soubor několika vzájemně propojených počítačových systémů (např. počítačová síť).85 Příkladem počítačového systému je osobní počítač (včetně připojených periferií), bankomat (ATM), mobilní telefon, PDA, tablet, herní konzole (např. Sony Playstation, PSP, Wii, Xbox 360) aj. Mezi počítačové systémy je však možné například zařadit i televize či jiné domácí spotřebiče umožňující spouštění aplikací, včetně připojení na Internet, či systémy v automobilech, poskytující obdobné funkce. V současné době, zjednodušeně řečeno, je za počítačový systém možné považovat téměř každé zařízení, které splňuje podmínky Internet of Things (IoT). 86 Relativně komplexním počítačovým systémem je Internet jako takový. Lze konstatovat, že počítačový systém je souhrnem technických a programových prostředků, jejichž variabilita je značná a uvedený výčet je pouze orientační a zdaleka nepostihující všechny možnosti. Vývojem techniky se tak i rozsah zařízení, které spadají do definice počítačového systému, značně posouvá.87

1.2.3.1 Hardware

Hardware (z angl. významu: „technické vybavení“). Pojem hardware vyjadřuje souhrn hmotných technických prostředků umožňujících nebo rozšiřujících provozování počítačového systému.88 Jde o veškeré fyzické zařízení,

které je třeba pro funkci systémů zpracování informací. Je to v podstatě počítač sám. Negativním vyjádřením lze uvést, že hardware je vše, co není programovým vybavením (software). Hardware je možné rozčlenit na dvě skupiny:

1) Vnitřní vybavení počítače. Jedná se o součásti hardwaru, bez kterých by nebyla možná vlastní činnost počítače. Těmito nezbytnými komponentami jsou: základní deska s obvody, paměť, procesor, napájecí zdroj. Mezi současné standardní vnitřní vybavení počítače však dále patří harddisk, grafická karta (umožňující vizualizaci činnosti počítače), mechaniky paměťových médií (FDD, CD, DVD, CD-RW, DVD-RW, Blu-Ray, čtečky karet), porty/ řadiče (ATA-PATA/SATA, PCI, USB, FireWire, E-SATA aj.), síťové komponenty (umožňující komunikaci v rámci sítí), zvukové a televizní karty aj.
2) Periferie (peripheral, či peripheral device).89 Jedná se o zařízení, která ve své podstatě nejsou nezbytně nutná k samotnému provozu počítače (pouze rozšiřuje možnosti jeho využití). „V širším slova smyslu se za periferii považuje cokoli kromě základní desky počítače s jeho procesorem (periferií tedy je: paměť, disk, disketová mechanika, porty, klávesnice, monitor), v užším slova smyslu pak až zařízení připojovaná k počítači externě a skutečně nepotřebná k obvyklému provozu i ovládání počítače.“ 90 Nejběžněji je periferie chápána právě v užším slova smyslu, tak jak je zde uvedeno. V tomto pojetí se jedná o zařízení, které se různými metodami (kabely, infračervený přenos, technologie Bluetooth, WiFi aj.) připojuje k počítači. Periferií je například klávesnice, myš, monitor, tablet, externí paměťová zařízení, tiskárna, datový projektor, optické senzory, scanner, plotr, externí modem, joystick aj.

Za předmět sloužící k ovládání počítačového systému je možné považovat některé z výše uvedených periferií (např. klávesnice, myš, tablet aj.).

Procesor (Central Processing Unit – CPU) je nezbytnou součástí každého počítače. Tato základní elektronická součást počítače je schopna provádět strojové instrukce. Dochází v ní ke kontrole a provedení všech zadaných operací. 91
Hlavními součástmi procesoru jsou: aritmeticko-logická jednotka (ALU - tato jednotka provádí vlastní výpočetní operace), registry (lze rozlišovat registry obecné a řídící) a řadič. Řadič řídí činnost procesoru, neboť zprostředkovává načítání strojových instrukcí z paměti, jejich dekódování, provedení a následné uložení výsledků. Pokud má obvod v sobě více procesorových jednotek, pak je označován jako vícejádrový procesor (přičemž uváděn je počet fyzických a virtuálních jader). Současné počítače v sobě kromě hlavní procesorové jednotky mají zabudovány zpravidla další „podpůrné“ procesorové jednotky, které s hlavní procesorovou jednotkou spolupracují. Tyto jednotky slouží např. pro provádění výpočtů pro grafické výstupy (GPU), zajištění WiFi, Bluetooth komunikace, příjem GPS aj.
Paměťové nebo záznamové médium (případně datový nosič či nosič informací) je externí nebo interní prostředek k zápisu a uchovávání dat. Kromě popsaných pevných disků jsou to nejčastěji diskety, kompaktní disky s různou hustotou zápisu (CD, DVD, Blu-Ray), paměťové karty (SD, MMC, CF karty, SDHC aj.), elektronické paměti typu USB (flashdisky) apod. Paměťovým médiem jsou však i operační paměti. Operační paměť (vnitřní či hlavní paměť. Anglicky: main memory, internal memory, primary storage) je nezbytnou součástí počítače, neboť umožňuje čtení i zápis dat, nad nimiž programy vykonávají operace. Operační paměť je s procesorem spojena pomocí rychlé sběrnice a procesor má okamžitý, či přímý přístup k této paměti,92 respektive k přímo požadované buňce operační paměti. Operační paměť je rozdělena do paměťových míst (buněk), které mají definovanou velikost (typicky 1, 2, 4 či 8 bytů). Toto rozdělení se nazývá fyzický adresový prostor (FAP) a slouží k:

- přidělování paměťových regionů na požádání procesů,
- uvolňování paměťových regionů na požádání procesů,
- udržování informací o obsazení adresového prostoru,
- zabezpečení ochrany paměti (zabránění přístupu procesu k paměti mimo jeho přidělený region).

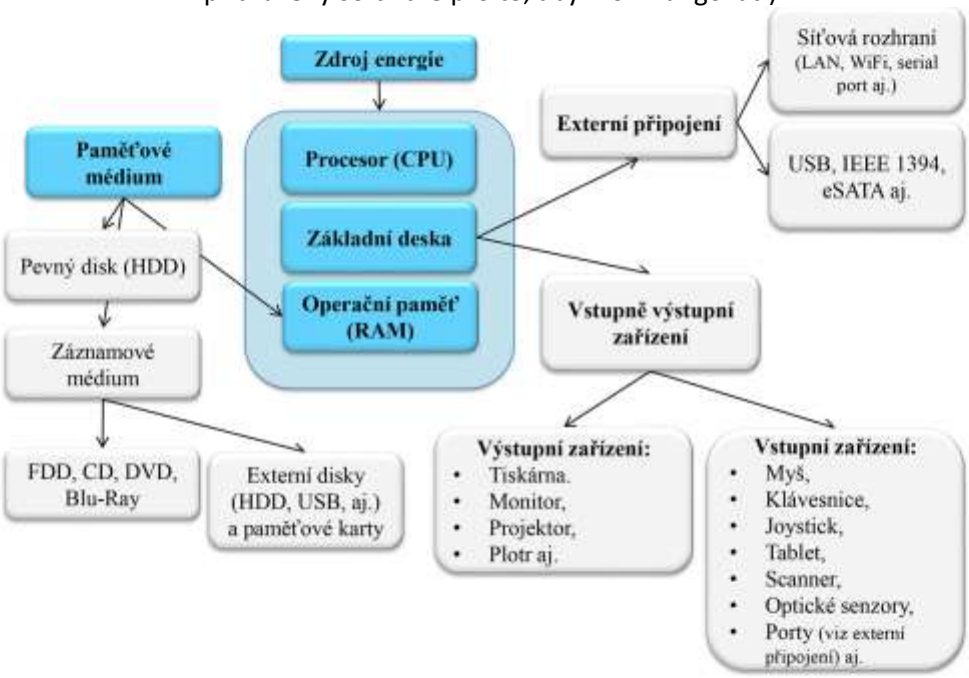
V současných počítačích je operační paměť v podobě RAM (Random Access Memory). Jedná se o polovodičovou paměť, která je typicky volatilní (dochází ke ztrátě uložených dat v případě odpojení od zdroje napájení) a dynamická. Mimo paměti RAM se v počítači nachází i paměť

ROM (Read Only Memory), která umožňuje pouze čtení, nikoliv však zápis dat. Tato paměť typicky slouží pro uchování základního řídícího software počítače (BIOS: Basic Input Output System. Tato paměť je součástí polovodičové desky – základní desky), či pro uchování firmware aj. Paměť ROM je energeticky nezávislá.
Základní deska (mainboard, motherboard) propojuje jednotlivé součásti počítače do fungujícího celku. Přes základní desku dochází k napájení jednotlivých komponent. Základní deska obsahuje integrované obvody zabudované v čipové sadě (chipset). Fyzicky se může jednat o jeden či dva čipy, přičemž čipová sada rozhoduje o tom, jaký procesor a operační paměť lze k základní desce připojit.

Harddisk (pevný disk) je paměťové médium zabudované v počítači sloužící k ukládání a uchování dat a programů, instalaci a načtení systému. Povrch disku je rozdělen do sektorů, které mají přesně definované umístění a obsahují příslušná data. Alokační tabulka disku (jedná se nejčastěji o tabulku FAT či NTSF, která je na pevně daném místě disku) určuje, v jakém sektoru disku se data nacházejí. Toto určení má význam zejména z hlediska znaleckého zkoumání paměťových médií. V současnosti se kapacita jednotlivých pevných disků pohybuje v rozmezí několika desítek či stovek MB až po několik TB. Pevné disky mohou být propojeny i v tzv. diskovém poli nejčastěji prostřednictvím SCSI (Small Computers System Interface), či SATA, PATA aj.

Server je výkonný počítačový systém, užívaný nejčastěji v počítačové síti jako zdroj dat a programů pro koncové počítače, tzv. klienty nebo pracovní stanice. Pracovní stanice mohou všechny současně pracovat s daty na serveru, přičemž využívají jeho diskové kapacity a programy uložené na jeho discích. Serverů může být zapojeno v síti i několik a každý z nich může plnit specifickou funkci (např. tiskový server, databázový server, terminal server, firewall aj.).

Pokud bychom chtěli graficky znázornit současný počítačový systém, pak by jedním z vhodných zobrazení mohlo být to následující (Modré93 bloky jsou povinné a bez nich nemůže počítačový systém fungovat. Šedé bloky pak představují periferii v užším či širším slova smyslu. Zároveň je třeba konstatovat, že počítačový systém musí využívat přidružený software pro to, aby mohl fungovat.):



Obrázek 9: Grafické zobrazení počítačového systému a jeho částí

1.3 Počítačové sítě a jejich fungování

Tato subkapitola definuje pojem počítačové sítě a další základní pojmy a některá technická specifika související s počítačovými sítěmi a Internetem. Uvedená minimální charakteristika je zcela nezbytná pro pochopení fungování počítačových systémů v rámci počítačových sítí. Alespoň obecná znalost v této subkapitole uvedeného schématu připojení k počítačové síti a jeho jednotlivých komponent je důležitá pro úspěšné pochopení fungování IT světa, možnosti vytvoření a nastavení si vlastních pravidel, jakož i odhalování kybernetických útoků a trestné činnosti páchané prostřednictvím ICT.

1.3.1 Počítačová síť (Computer network)

Existuje celá řada definic pojmu počítačová síť, pro představu čtenáře některé z nich uvádím. Jednu z možných definic počítačové sítě je možné nalézt ve Výkladovém slovníku kybernetické bezpečnosti, kde autoři uvádějí, že se jedná o „soubor počítačů spolu s komunikační infrastrukturou (komunikační linky, technické vybavení, programové vybavení a konfigurační údaje), jejímž prostřednictvím si (počítače) mohou vzájemně posílat a sdílet data.“ 114 Další definici je možné nalézt v dnes již neplatné normě ČSN ISO/IEC 2382-1 která definovala počítačovou síť jako „síť uzlů, které se při datové komunikaci propojují.“ 115 „Jedná se o množství vzájemně propojených počítačů, strojů, nebo operací.“ 116 Počítačovou síť si je možné asi nejjednodušeji představit jakožto soubor (množinu) počítačových systémů, které jsou navzájem propojeny a mezi nimiž dochází k výměně dat či informací. Počítačové sítě je možné dělit z celé řady hledisek. Uvedu tři možná dělení, která mají význam pro tuto publikaci:

1) **Dělení dle rozlehlosti sítí.** Podle rozlehlosti, respektive rozsahu sítí se sítě rozdělují na čtyři základní skupiny, přičemž v současnosti jsou nejvýznamnější sítě uvedené pod písmeny b) a d):

a) **PAN** (Personal Area Network – Osobní síť). Jedná se o malou privátní síť, která zpravidla slouží pro potřeby jednotlivce či domácnosti. V rámci této sítě dochází typicky k propojení jednotlivých počítačových systémů (mobilní telefon, PDA, laptop aj.) typicky za pomoci Bluetooth, IrDA, WiFi, ZigBee.117 PAN sítě se v současnosti značně rozšiřují a zapojují do své struktury čím dál více zařízení. Příkladem fungování PAN sítě je komunikace jednotlivých technologií v domácnosti například s mobilním telefonem či počítačem, a to v rámci propojení těchto systémů do Internetu věcí (IoT) či Internetu všeho (IoE).118

b) **LAN** (Local Area Network – Lokální počítačová síť). Typicky je tento pojem využíván pro označení lokální, či místní sítě, což je síť, v rámci které dochází k propojení uzlů119 v rámci jedné či více budov. Nezáleží na způsobu propojení jednotlivých uzlů. Toto propojení může být realizováno metalickými, optickými či bezdrátovými sítěmi. Tato síť mívá typicky vyšší přenosovou rychlost a menší vzdálenost mezi jednotlivými uzly. Lokální sítí může být např. kompletní síť (subsítě) univerzity, organizace, ale zároveň se může jednat o malou síť, která je vybudována v rámci domácnosti (například jde o propojení více počítačových systémů: počítače, tiskárny, Smart TV, datové úložiště aj. přes switch či router).

c) **MAN** (Metropolitan Area Network – Metropolitní síť). Jedná se o síť, která propojuje LAN sítě v městské zástavbě. Síť MAN spojuje jednotlivé uzly v řádech jednotek až desítek kilometrů. Někteří autoři řadí tuto síť do sítí WAN.

d) **WAN** (Wide Area Network – Vzdálená počítačová síť). Pojem WAN označuje počítačovou síť propojující geograficky vzdálené oblasti. Typicky jsou do sítě WAN propojovány jednotlivé LAN a MAN sítě. Z geografického hlediska je možné definovat WAN sítě, jako sítě s rozsahem například v teritoriu státu, kontinentu i jako sítě celosvětové.

2) Dělení dle postavení síťových uzlů.

a) **Peer-to-peer** (P2P – „rovný s rovným“, či klient-klient) je počítačovou sítí, kde mezi sebou přímo komunikují jednotliví uživatelé, respektive jednotlivé počítačové systémy. Tento typ sítě nelze centrálně spravovat. Tyto sítě jsou například používány pro sdílení souborů, systémových prostředků aj.

b**) Klient-server** je typem sítě, kde je jeden či více počítačových systémů (server) nadřazen počítačovému systému či systémům (klient/klienti). Klient-server označuje vztah „nadřízenosti a podřízenosti“ mezi dvěma počítačovými programy. Klient typicky žádá o služby server. Na modelu klient-server jsou založeny služby typu e-mail, web, přístup k databázi aj.

3) Dělení dle vlastnictví sítí.

a) **Privátní síť** je počítačovou sítí, která využívá privátní IP120 adresy. Privátní adresy jsou používány v rámci sítě LAN (domácí, podnikové aj.). Pokud privátní síť potřebuje připojení k Internetu (přes přidělené veřejné IP adresy), musí používat překlad síťových adres (NAT), nebo proxy server. Privátní sítě se využívají zejména z důvodu nedostatečného množství veřejných IP adres ve verzi IPv4.

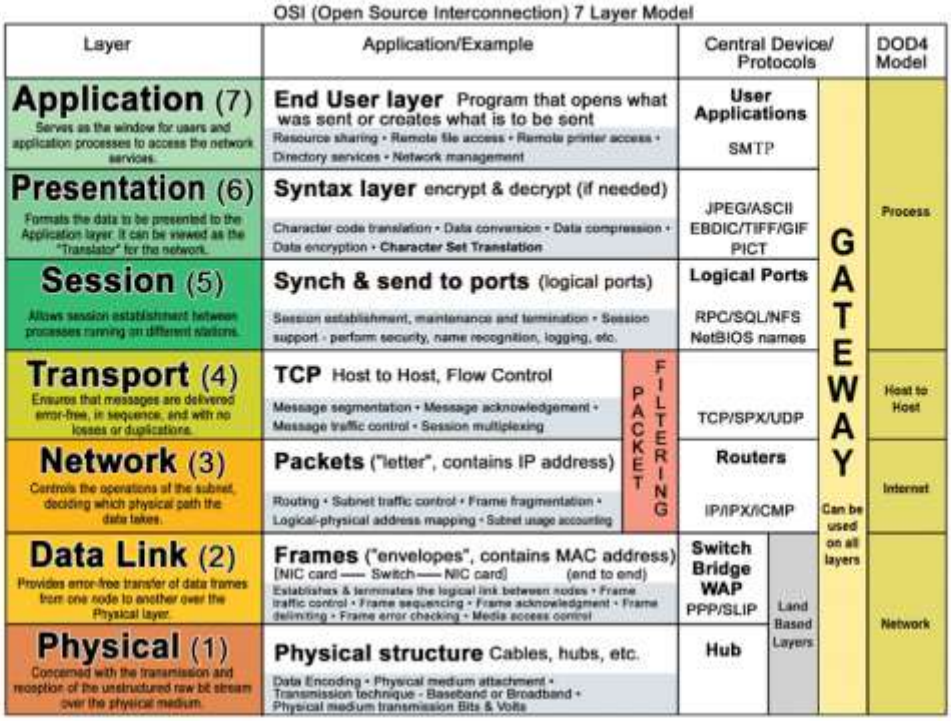
b) **Veřejná síť** je otevřena „nejširší veřejnosti, které nabízí své služby spočívající v přenosu dat. Uživatelem takovéto sítě se skutečně může stát kdokoli, kdo o to má zájem a je ochoten za to zaplatit, resp. přistoupit na podmínky toho, kdo takovouto síť provozuje. Provozovatelem přitom bývá takový subjekt, který svou datovou sám nepoužívá - vlastní ji a provozuje především proto, aby její služby mohl poskytovat na komerční bázi jiným subjektům.“ 121

c) **Virtuální privátní síť** (VPN – Virtual Private Network). VPN je mechanismus (nebo metoda) umožňující propojení počítačových systémů prostřednictvím nedůvěryhodné (např. veřejné) počítačové sítě tak, že propojené počítačové systémy mezi sebou budou moci komunikovat, jako by byly propojeny v rámci důvěryhodné (uzavřené privátní) sítě. Tyto počítačové systémy ověřují svoji totožnost (např. pomocí certifikátů, hesla aj.) a po vzájemné autentizaci je komunikace mezi těmito privátně propojenými počítači šifrována.

Komplexní a globální počítačovou sítí pak je Internet, který je také označován jako „Síť sítí“. Technicky se jedná o decentralizovanou, celosvětovou distribuovanou počítačovou síť složenou z jednotlivých menších sítí navzájem spojených pomocí protokolů TCP/IP.

Protokoly počítačových sítí a Internetu podle modelu ISO/OSI

K tomu, aby bylo možno přenášet data mezi jednotlivými počítačovými systémy, byl definován model ISO/OSI jako referenční komunikační model. Tento model rozděluje komunikaci do sedmi vzájemně propojených vrstev. Tento model je zařazen do ISO/IEC 7498-1:1994 [v ČR: ČSN EN ISO/IEC 7498-1 (369614). Informační technologie – Propojení otevřených systémů – Základní referenční model – Základní model (ISO 7498-1:1994).].



Další možné grafické znázornění v sobě zahrnuje i příklady aktivit v rámci jednotlivých vrstev, či využívané protokoly:

OSI Model				
Data Unit (protokolová datová jednotka)		Layer (Vrstva)		Function (Funkce)
Host Layers	Data	7	Aplikační	Definuje způsob, jakým komunikují se sítí aplikace, například databázové systémy, elektronická pošta nebo programy pro emulaci terminálů. Používá služby nižších vrstev, a díky tomu je izolována od problémů síťových technických prostředků. Je softwarová.
	Data	6	Prezentační	Specifikuje způsob, jakým jsou data formátována, prezentována, transformována a kódována. Řeší například háčky a čárky, CRC, kompresi a dekompresi, šifrování dat. Je softwarová.
	Data	5	Relační	Koordinuje komunikace a udržuje relaci tak dlouho, dokud je potřebná. Dále zajišťuje zabezpečovací, přihlašovací a správní funkce. Je softwarová.
	Segments (Segmenty)	4	Transportní	Vlastní přenos dat. Definuje protokoly pro strukturované zprávy a zabezpečuje bezchybnost přenosu (provádí některé chybové kontroly). Řeší například rozdělení souboru na pakety a potvrzování. Je softwarová.
Network Layers	Packets (pakety)	3	Síťová	Definice protokolů pro směrování dat. Adresování a směrování dat v síti od zdroje k cíli. Definuje protokoly pro směrování dat, jejichž prostřednictvím je zajištěn přenos dat do požadovaného cílového uzlu. Je hardwarová, ale když směrování řeší PC s dvěma síťovými kartami je softwarová.
	Frames (rámce)	2	Linková	Zajišťuje integritu toku dat z jednoho uzlu sítě na druhý. V rámci této činnosti je prováděna synchronizace bloků dat a řízení jejich toku. Je hardwarová.
	Bits (bity)	1	Fyzická	Definuje prostředky pro komunikaci s přenosovým médiem a s technickými prostředky rozhraní. Dále definuje fyzické, elektrické, mechanické a funkční parametry týkající se fyzického propojení jednotlivých zařízení. Je hardwarová.

Dalším síťovým modelem vytvořeným pro sítě internetového typu je TCP/IP. 125 Graficky by bylo možné TCP/IP model znázornit následovně:

TCP/IP	OSI
Aplikační	Aplikační
	Prezentační
	Relační
Transportní	Transportní
Síťová	Síťová
Vrstva síťového rozhraní	Linková
	Fyzická

Technické vymezení sítě tak, jak bylo uvedeno výše, však právem běžně používáno není. Z hlediska práva, zejména trestního, je třeba na závěr kapitoly o počítačových sítích vymezit i pojem „veřejně přístupná počítačová síť“ [viz § 117 písm. a) TZK]. Trestní zákoník v tomto ustanovení uvádí, že trestný čin je spáchán veřejně, pokud je spáchán „obsahem tiskoviny nebo rozšiřovaného spisu, filmem, rozhlasem, televizí,veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.“ Šámal k tomuto pojmu uvádí, že se jedná o „funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především internet a jiné podobné informační systémy (např. francouzský Minitel apod.). Z technického hlediska je veřejně přístupná počítačová síť soustavou serverů, datových komunikací a k nim připojených počítačů. Z organizačního hlediska jde o provozovatele jednotlivých sítí a podsítí, zprostředkovatele připojení i uživatele a další subjekty.“ 127 K pojmu spáchání činu veřejně přístupnou počítačovou sítí se dále blíže vyjadřuje Tpjn 300/2012 (stanovisko trestního kolegia Nejvyššího soudu České republiky z 30. 1. 2013) – Rt 20/2013:128 Toto kolegium „obecně uznává, že za veřejně přístupnou počítačovou síť se v obecných rysech považuje funkční propojení do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především Internet a jiné podobné komunikační systémy. Internet je informační a komunikační systém, který má kromě jiného i povahu prostředku, jehož prostřednictvím lze veřejně šířit informace.

Je tedy patrné, že internet je počítačovou sítí, která figuruje jako přenosové médium umožňující využívání určitých služeb, z nichž nejvýznamnější je přenos informací. K tomu je možno dodat, že na základě výše uvedených skutečností je internet veřejně přístupnou sítí, neboť zaregistrovat se na něm a využívat jeho služby může obecně každý. Podmínka veřejně přístupné sítě je splněna bez dalšího v případě, pokud by komunikace byla vedena formou veřejně přístupných webových stránek, na kterých by např. byly závadné materiály vyvěšeny. K takovým stránkám, pokud nejsou zakódovány či opatřeny heslem, má přístup každý či může se stát uživatelem při splnění určitých podmínek. Webové stránky jsou tedy obecně přístupné blíže neurčenému a neomezenému okruhu uživatelů.“

1.3.2 Internet Protocol a IP adresa

Internet Protocol (IP) zajišťuje vysílání datagramů na základě síťových IP adres uvedených v jejich hlavičce. Datagram je samostatná datová jednotka, která obsahuje všechny potřebné údaje o adresátovi i odesílateli a pořadové číslo datagramu ve zprávě. Jednotlivé datagramy jedné zprávy putují sítí nezávisle na sobě, mohou putovat jinou cestou a pořadí jejich doručení nemusí odpovídat pořadí ve zprávě. Vlastní doručení datagramu není zaručeno, spolehlivost přenosu datagramu musí zajistit vyšší vrstvy (TCP, aplikace aj.). Podstatnou informací je, že pokud chce počítačový systém komunikovat v rámci jakékoli sítě, musí mít přidělenou IP adresu, 129 která je v rámci dané koncové sítě jedinečná. IP adresy mohou být přidělovány staticky (počítačovému systému je „napevno“ manuálně přidělena IP adresa) či dynamicky, kdy mu je (při každém připojení nového počítačového systému k počítačové síti) na základě MAC adresy přidělena automaticky IP adresa nová. IP adresa není standardně anonymní a počítačový systém ji využívá při komunikaci s jinými počítačovými systémy jakožto jeden z identifikátorů. V současnosti existují dvě verze Internetového protokolu:

1) Internet Protocol version 4 (IPv4). Jedná se o první, masově rozšířenou a v současnosti stále nejrozšířenější verzi Internet protokolu. IPv4 používá 32bitové adresy, které jsou zapsány dekadicky po jednotlivých oktetech (osmicích bitů). Veřejná adresa130 v rámci IPv4 je tvořena čtveřicí čísel, vždy od sebe oddělených tečkou, přičemž hodnota každého z nich nepřesahuje 255. IP adresa tedy může mít podobu například takovéhoto číselného řetězce:

195.113.149.160, či 64.233.168.99 apod. Číselný řetězec IP adresy: 302.233.8.158, či 64.233.168.299 v tomto provedení je nesmyslný a není se možné jeho prostřednictvím přihlásit do sítě Internet.

Protokol IPv4 poskytuje teoretický adresní prostor v rozsahu 232 (což je 4 294 967 296 adres). Prakticky je však využitelnost menší, protože kvůli přidělování adresových bloků je část adres nevyužitých.

Internet Engineering Task Force131 rozhodla o zachování následujících rozsahů IPv4 adres pro privátní sítě:

Označení RFC 1918	Rozsah IPv4 adres	Počet adres	Největší CIDR blok (maska podsítě)	Pro síťové rozhraní
24bitový blok	10.0.0.0–10.255.255.255	16 777 216	10.0.0.0/8 (255.0.0.0)	24 bitů
20bitový blok	172.16.0.0–172.31.255.255	1 048 576	172.16.0.0/12 (255.240.0.0)	20 bitů
16bitový blok	192.168.0.0–192.168.255.255	65 536	192.168.0.0/16 (255.255.0.0)	16 bitů

Z důvodu nedostatku veřejných IP adres ve verzi IPv4 došlo k zavedení protokolu IPv6. Tyto dva protokoly v této době fungují současně, avšak je předpokládáno postupné nahrazení protokolu IPv4.

2) Internet Protocol version 6 (IPv6). IPv6 je novým protokolem, který by měl vyřešit problémy související s nedostatkem veřejných IP adres. IP adresa verze 6 má délku 128 bitů, které jsou zapsány hexadecimálně (např. 2001:0:5ef5:79fd:386a:e7:4dee:fb51). U IPv6 je odstraněna potřeba použití překladu síťových adres. IPv6 obsahuje celkem 2 128 adres.

Adresní architekturu IPv6 definuje RFC4291. Adresní prostor je rozdělen následovně:

prefix	význam
::/128	neurčená
::1/128	smyčka (loopback)
ff00::/8	skupinové
fe80::/10	individuální lokální linkové
ostatní	individuální globální

Protokol IPv6 zavádí tři typy adres:

◦ **Individuální** (unicast), která identifikují právě jedno síťové rozhraní.

◦ **Skupinové** (multicast), která označuje skupinu síťových rozhraní, jejímž členům se mají data dopravit. Skupinově adresovaný datagram se doručuje všem členům skupiny.

◦ **Výběrové** (anycast), která označují také skupinu síťových rozhraní, data se však doručují jen jejímu nejbližšímu členovi.

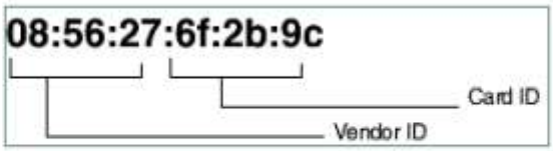
Z pohledu práva je třeba uvést, že IP adresa je schopna více méně (viz užití NAT,132 TOR aj.) jednoznačně identifikovat síťové rozhraní v počítačové síti, nikoliv ale přímo konkrétní osobu. IP adresa je schopna identifikovat počítačový systém „po celou dobu" jeho připojení k počítačové síti (skrze všechna jednotlivá připojení). „V tomto ohledu lze hovořit o tom, že IP adresa sama o sobě představuje neperfektní identifikátor směřující pouze k místu připojení, případně k síti více počítačů či jednomu konkrétnímu počítači. Samotná IP adresa tak z principu neslouží k identifikaci konkrétní osoby, ale směřuje toliko k místu, kde je realizována nějaká činnost, přičemž není samo o sobě známo, zda jde o činnost strojovou (tj. počítače), nebo činnost konkrétní osoby." 133 U předmětného počítačového systému mohla sedět osoba provádějící konkrétní aktivity, avšak mohla tam sedět i osoba jiná, nebo se mohlo jednat o vlastní (či naprogramovanou) činnost počítačového systému. Prokázání skutečnosti, kdo byl v daný okamžik uživatelem počítačového systému, je významné zejména pro trestní řízení

K otázce, zda je IP adresa osobním údajem, se vyjádřil i Nejvyšší správní soud, který v jednom ze svých rozsudků134 (mimo jiné i s odvoláním na Soudní dvůr EU) uvedl: „Při posuzování povahy IP adresy je možno podpůrně odkázat rovněž na judikaturu Soudního dvora EU. Ten ve svém rozhodnutí ze dne 29. 1. 2008, sp. zn. C-275/06, Productores de Música de Espana (Promusicae) vs. Telefónica de Espana SAU (rozhodnutí je dostupné z http://curia.europa.eu), považoval IP adresu v kontextu daného případu (Promusicae požadovala po Telefonice odhalení identit osob, kterým poskytovala připojení k Internetu a u nichž byla známá jejich IP adresa a datum a čas připojení) za osobní údaj ve smyslu předpisů na ochranu osobních údajů. Pro účely nyní posuzované věci lze z uvedeného závěru vyvodit, že jestliže může IP adresa za určitých okolností představovat osobní údaj, tedy údaj, na jehož základě lze identifikovat (přímo či nepřímo) nějakou konkrétní osobu, pak může sloužit také jako důkaz v přestupkovém řízení, byť jako důkaz nepřímého charakteru.

MAC Adresa

MAC adresa (Media Access Control) je jedinečný identifikátor síťového zařízení, který používají různé protokoly druhé (spojové) vrstvy OSI. MAC adresa je přiřazována síťové kartě bezprostředně při její výrobě, proto je také někdy označována za fyzickou adresu. Přidělená MAC adresa je vždy celosvětově jedinečná (unikátní), avšak je ji možné

podvrhnout.136 MAC adresa je rozdělena na dvě poloviny, přičemž první z nich definuje výrobce síťové karty a druhá polovina je pak jedinečným identifikátorem karty, který jí přidělil výrobce (viz Obrázek 11137).



Obrázek 11: MAC adresa a její součásti

Ethernetová MAC adresa se skládá ze 48 bitů a podle standardu by se měla zapisovat jako tři skupiny čtyř hexadecimálních čísel (např. 08:56:27:6f:2b:9c). Mnohem častěji se ale píše jako šestice dvojciferných hexadecimálních čísel oddělených pomlčkami nebo dvojtečkami (např. 00-B0-D0-86-BB-F7).

MAC adresa se zobrazuje pouze k nejbližšímu síťovému zařízení (např. router u poskytovatele připojení k Internetu) a slouží tedy k identifikaci počítačových systémů pouze v jedné, značně omezené části počítačové sítě.

1.4 ISP (Internet Service Provider)

Na závěr kapitoly, která se věnuje vymezení některých pojmů bezprostředně se vztahujícím ke kyberkriminalitě, IT/ICT, kyberprostoru a aktivitám v něm uskutečňovaným, považuji za nezbytné vydefinovat pojem Internet Service Provider (ISP).138 Internet Service Provider je nezbytnou součástí fungování světa informačních a komunikačních technologií, zejména pak Internetu a s ním spojenými službami. Internet Service Provider se svou vlastní činností bezprostředně podílí na jeho budování, obměně. Internet Service Provideři poskytují jednotlivé služby v rámci Internetu. V nedávné minulosti se primárně jednalo o služby, které byly spojeny s poskytnutím internetového připojení, a zkratka ISP označovala pouze subjekty, které zajišťovaly koncovým uživatelům (fyzickým či právnickým osobám) „konektivitu“.139 V minulosti byla většina ISP zároveň telefonními společnostmi nebo si od nich fyzickou infrastrukturu pronajímali. V současnosti však pojem ISP nezahrnuje pouze ty subjekty, které zajišťují fyzickou konektivitu, ale i subjekty, které poskytují další služby v prostředí Internetu. V současnosti je možné konstatovat, že začínají převažovat ISP poskytující jiné služby než konektivitu (cloudová úložiště, e-mail, sociální sítě aj.) nad ISP, kteří poskytují konektivitu, byť ti první jsou na druhých závislí. V České republice není v legislativě používán pojem ISP, ale pojem poskytovatel služby informační společnosti.140

Poskytovatel služby informační společnosti

Jedná se o subjekty, jejichž prostřednictvím mohou koncoví uživatelé vstupovat do počítačových sítí a využívat zde nabízené služby. Směrnice Evropského parlamentu a Rady č. 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů ve znění směrnice č. 98/48/ES nedefinuje pojem poskytovatele služeb informační společnosti, ale pouze pojem samotné informační společnosti. 141 Pojem služba informační společnosti je vymezen v čl. 1 odst. 2 směrnice č. 98/34/ES následovně:

3 Anonymita uživatele

Žít v digitální době s představou či pocitem, že mé jednání je anonymní či skryté před zraky jiných uživatelů, 275 je dle mého názoru naivní. S nástupem doby digitální se neobjevují pouze její pozitivní, ale i negativní aspekty.276 Jedním z těchto negativ je i ta skutečnost, že se čím dál méně zajímáme o podstatu fungování služeb poskytovaných v kyberprostoru.

Náš svět, který stále častěji chápeme jako „svět informací“ či „svět Internetu“, je pevně spojen s informačními a komunikačními technologiemi, které zasahují do života jedince velmi výrazným způsobem. Tyto technologie usnadňují přístup k informacím a zjednodušují či zrychlují vzájemnou komunikaci mezi jednotlivými uživateli atd. Na straně druhé je však třeba si uvědomit, že jakékoli uveřejnění informací z našeho soukromí na Internetu je rizikem, kterého může v kyberprostoru kdokoliv zneužít. Veškeré aplikace, ať už jsou využívány v jakémkoli počítačovém systému, webové služby277 a zejména sociální sítě, 278 shromažďují o svých uživatelích značné množství informací, které majoritně nepotřebují ke svému fungování, ale které jednak umožňují dotyčnému ISP poskytovat službu „zadarmo“, a jednak „cílit“ či modifikovat jím nabízené služby. Mezi informace, které standardně nejsou nezbytně nutné k přímé funkčnosti jednotlivých služeb, patří například informace mající povahu osobních (jméno, příjmení, e-mailová adresa, telefonní číslo, bydliště aj.), citlivých279 (např. informace o využívaném operačním systému počítače, verzích jednotlivých aplikací, soubory cookies aj.), lokalizačních údajů (souřadnice GPS, informace o WiFi, GPRS aj.), provozních údajů aj.

Uvedené informace mohou být využity značně různorodě. Poskytovatel služby může dle těchto informací nabízet např. doplňkové služby či reklamu na základě požadavků, zájmů či zálib uživatelů. Policie je díky nim schopna vytvořit rámec denní činnosti osoby, která se například ztratila či byla unesena, a tím urychlit vlastní činnost při pátrání po této osobě. Zároveň však tyto informace mohou být velmi jednoduše zneužity pachateli trestné činnosti, ať již pro navázání kontaktu s obětí, či k naplánování činu samotného. Poskytnutím (byť i nedobrovolným či nevědomým) těchto údajů umožňuje uživatel dané služby získat jiným osobám důležité informace o svém životě (např. informace o svém chování v průběhu dne, navštěvovaných místech, aktivitách a osobách, se kterými je v kontaktu).281 V tento okamžik se sami stáváme informací či komoditou, se kterou může někdo jiný obchodovat. Různé dostupné statistiky282 uvádějí, že v současnosti je celková populace přibližně 7,4 miliard lidí. Z tohoto počtu zhruba 3,6 miliardy lidí jsou aktivními uživateli Internetu a více než 2,1 miliardy lidí jsou aktivní uživatelé sociálních sítí. Mobilní zařízení vlastní více než 3,6 miliardy uživatelů a k sociálním sítím se přes tato zařízení připojuje více než 1,7 miliardy uživatelů. Sociálním sítím vévodí Facebook s více než 1,59 miliardami uživatelů: 283 V této části publikace se pokusím upozornit na možné bezpečnostní hrozby, které jsme si zvykli de facto přijímat či nevnímat a u kterých si většina jedinců či organizací vůbec neuvědomuje možné nebezpečí.

3.1 Digitální stopa

Uvedené hrozby, či spíše rizika, spočívají velmi často v zanechávání digitálních stop v kyberprostoru. Digitální stopy, na základě toho, zda mohou, či nemohou být ovlivněny uživatelem, je obecně možné rozdělit na stopy ovlivnitelné a neovlivnitelné.

Dělení digitálních stop:

- **Digitální stopa neovlivnitelná**
  - Informace z počítačového systému;
  - připojení k počítačovým sítím, zejména Internetu;
  - využívání poskytovaných služeb aj.
- **Digitální stopa ovlivnitelná**
  - vědomé využití služeb;
  - dobrovolné zveřejnění informace
    - blogy, fóra,
    - sociální sítě,
    - e-mail,
    - datová úložiště,
    - cloudové služby aj.

V následující části se budu věnovat některým aspektům jednotlivých digitálních stop a informacím v nich obsažených. Smyslem je upozornit uživatele na to, že jeho jednání v prostředí informačních a komunikačních systémů není tak anonymní, jak si možná myslí. Ve světě ICT platí jedno pravidlo: pokud kdykoliv cokoliv nahrajete, přenesete, zprostředkujete, vložíte do kyberprostoru, zůstane to tam „navždy“. Vždy bude existovat kopie (vzniklá na základě funkcionality počítačového systému či kopie uložená některým jiným uživatelem) vašich dat. A i když tato data následně odstraníte (či je odstraní někdo jiný), k jejich skutečnému, trvalému a nezvratnému odstranění nedojde. Je proto vhodné věnovat pozornost své digitální stopě a informacím či datům, jež za sebou v prostředí kyberprostoru zanecháváme.

3.1.1 Digitální stopa neovlivnitelná

Neovlivnitelné stopy nejčastěji vznikají na základě interakce jednoho počítačového systému s počítačovým systémem jiným nebo na základě funkčnosti počítačového systému (a přidruženého software). Příkladem těchto stop mohou být informace z operačního sytému (např. hlášení o chybách systému Windows či systémové informace), nebo další informace a data, jež jsou ukládány na základě funkčnosti tohoto systému, aniž by muselo dojít k jejich předání (např. počítačový systém nebyl nikdy připojen k žádné síti či jinému počítačovému systému).284 Tvrdit zcela nekompromisně, že nelze tyto stopy ovlivnit, by nebylo zcela korektní. V případě, že je uživatel dostatečně zkušený, je schopen celou řadu „neovlivnitelných“ digitálních stop pozměnit, maskovat nebo potlačit (např. prostým anonymním režimem webového prohlížeče, který vypne cookies). Nicméně pohyb uživatele po Internetu se dá sledovat nejrůznějšími způsoby

IP adresa

Připojení počítačového systému k Internetu je typickým příkladem relativně neovlivnitelné stopy využívající IP adresu či MAC adresu, které jsou předávány spolu s dalšími informacemi ISP. V kapitole 1.3.2 Internet Protocol a IP adresa bylo uvedeno, že IP adresa není standardně anonymní a počítačový systém ji využívá při komunikaci s jinými počítačovými systémy jakožto jeden z identifikátorů. IP adresy jsou přidělovány hierarchicky, přičemž dominantní roli zde má ICANN, 285 který rozdělil reálný svět na regiony, nad nimiž vykonávají správu regionální internetoví

registrátoři (RIR - Regional Internet Registry). Tito registrátoři dostali od ICANN přidělen určitý rozsah IP adres, které přidělují LIRům v rámci svého regionu. Regionální registrátoři jsou rozděleni do následujících pěti teritorií:

1) „Euro-asijská“ oblast - RIPE NCC: https://www.ripe.net/
2) „Asijsko pacifická“ oblast – APNIC: https://www.apnic.net/
3) „Severo-americká“ oblast – ARIN: https://www.arin.net/
4) „Jiho-americká“ oblast – LACNIC: http://www.lacnic.net/
5) „Africká“ oblast – AFRINIC: http://www.afrinic.net/

Obrázek 17: Rozdělení světa mezi RIR

Regionální registrátoři286 provozují na svých stránkách službu Whois, což je označení pro databázi, v níž jsou evidovány údaje o držitelích IP adres. Tyto databáze obsahují celou řadu informací, na jejichž základě je možné identifikovat např. rozsah používaných veřejných IP adres, kontaktní údaje, abuse kontakt,287 hierarchicky nadřazeného poskytovatele připojení aj. K vlastnímu zjištění „vlastníka“ (operátora, poskytovatele) konkrétní IP adresy je mnohdy možné využít právě těchto volně dostupných databází.2

```
Responsible organisation: Policejni akademie CR v Praze
Abuse contact info: abuse@polac.cz

inetnum:        195.113.149.160 - 195.113.149.175
netname:        POLAC-TCZ
descr:          Policejni akademie CR
descr:          Prague 4
country:        CZ
org:            ORG-PACV1-RIPE
admin-c:        PACV1-RIPE
tech-c:         PACV1-RIPE
status:         ASSIGNED PA
mnt-by:         TENCZ-MNT
remarks:        Please report network abuse -> abuse@polac.cz
created:        2014-09-02T14:06:09Z
last-modified:  2014-09-02T14:06:09Z
source:         RIPE

route:          195.113.0.0/16
descr:          CESNET-TCZ
origin:         AS2852
mnt-by:         AS2852-MNT
remarks:        Please report abuse -> abuse@cesnet.cz
created:        1970-01-01T00:00:00Z
last-modified:  2006-06-26T14:36:38Z
source:         RIPE
```

Obrázek 18: Výpis informací z databáze RIR

Regionální registrátoři dále rozdělují přidělené IP rozsahy mezi lokální internetové registrátory (LIR - Local Internet Registry). Lokálním registrátorem je zpravidla ISP (v ČR poskytovatel služeb informační společnosti, konkrétně pak poskytovatel připojení, ať veřejný, či neveřejný). Tento registrátor pak může dále svůj rozsah IP adres poskytnout například části své organizace či jiným subjektům. Na zkráceném výběru z databáze RIR je zobrazen LIR (v tomto

případě CESNET, z.s.p.o. využívající rozsah IP adres: 195.113.0.0/16) a organizace, jíž CESNET přidělil část veřejných adres [Policejní akademie ČR s rozsahem IP adres 195.113.149.160–195.113.149.175. Policejní akademie pak opět může rozdělit tyto adresy mezi další části organizace (např. fakulty, laboratoře, či jiné sub sítě, jež spravuje)]. Dle IP adresy a přesného času je možné na základě hierarchického přidělování adres určit konkrétní počítačový systém. 289 Informace o připojení koncového počítačového systému (zdroje) k cílovému počítačovému systému (např. připojení počítače k Internetu a zobrazení si požadované webové stránky) jsou uchovávány jednotlivými ISP v rámci celé cesty mezi zdrojem a cílem.

Díky přísným pravidlům definujícím hospodaření s IP adresami a veřejně přístupnými databázemi RIRů, které obsahují informace o držitelích jednotlivých adresových bloků, je možné velmi rychle zjistit, do které sítě patří určitá IP adresa a kdo danou síť provozuje. Provozovatel dané sítě pak díky logování informací ze síťového provozu dokáže identifikovat, kdo (respektive jaký počítačový systém) v konkrétním čase používal konkrétní IP adresu. Toto určení je velmi důležitým zdrojem informací při řešení bezpečnostních incidentů (kybernetických útoků) a při pátrání jejich po zdroji (původci).

E-mail

E-mail jakožto jedna z nejčastěji využívaných služeb v prostředí Internetu rozhodně není anonymní službou. Zpráva, která je odeslána od zdroje k cíli (adresátovi), v sobě typicky nese celou řadu informací, které mohou identifikovat jednak poskytovatele služby (e-mailu), tak i poskytovatele připojení zařízení, z nějž byl e-mail odeslán. Tyto informace nejsou zobrazeny v těle zprávy (tedy textu, který odesíláme konkrétní osobě), ale ve zdrojovém kódu (hlavičce) zprávy. Z toho zdrojového kódu je například možné zjistit cestu přes servery, skutečného odesílatele, zdrojové jméno počítače, název počítače, čas odeslání zprávy (včetně časové zóny) používaný operační systém, mailového klienta aj. Níže je uvedený příklad hlavičky přeposlaného290 podvodného e-mailu s vyznačením potenciálně zajímavých informací.

Obrázek 19: Zobrazení informací z hlavičky e-mailové zprávy

Web browser

Webový prohlížeč je další aplikací, která standardně předává informace o uživateli a jeho počítačovém systému, počítačovému systému (serveru) navštívené stránky. Tento server pak v rámci dotazu od klienta zjistí například referer (což je stránka, ze které uživatel přichází), používaný webový prohlížeč a operační systém (včetně přesné verze), cookies, flash cookies, historie, cache aj. Kromě IP adresy jsou to právě mimo jiné i soubory cookies, 291 jež pomáhají vytvořit „otisk“ („fingerprint“) uživatelova počítačového systému (počítače, smartphonu aj.). Tento otisk umožňuje určit konkrétní počítačový systém, 292 a to i v případě, že uživatel používá jiný webový prohlížeč, či promaže cookies, přihlašuje se z jiné IP adresy, atd. Jeden z mnoha v současnosti požívaných způsobů tvorby

„fingerprintingu“ je canvas fingerprinting. 293 Canvas fingerprinting funguje tak, že navštívený webserver nařídí webovému prohlížeči uživatele „nakreslit skrytý obrázek“. Tento obrázek je unikátní pro ten který webový prohlížeč a počítačový systém. Nakreslený obrázek je pak převeden do ID kódu, který je na webovém serveru uchován pro případ, že by jej uživatel navštívil znovu.

Obrázek 20: Ukázka Canvas Fingerprintingu

Kromě fingerprintingu je u webového prohlížeče dále zajímavé sledovat předávání informací třetím stranám (jak subjektům, tak službám, které informace o uživateli mohou dále využít). Toto předávání se standardně děje na základě smluvních podmínek uzavřených s ISP. Každý koncový uživatel může například využít aplikaci Light Beam,295 která zobrazí všechny stránky, se kterými na webu uživatel (mnohdy nevědomky) komunikuje (dochází k předávání dat třetím stranám). Předávání informací o uživatelích třetím stranám rozhodně není něco výjimečného. Naopak v digitálním světě se jedná o samozřejmost a „nezbytný předpoklad“ pro fungování řady ISP.

Určení počítačového systému na základě informací z jeho komponent

Jedním z unikátních, avšak za určitých okolností změnitelných, identifikátorů počítačového systému, je MAC adresa, která je pevně svázána se síťovou kartou počítačového systému.300 Síťová karta není však jedinou hardwarovou komponentou, která je schopna předávat unikátní identifikátor počítačového systému jinému počítačovému systému. Vědci z Princenton University zjistili, že počítačový systém je možné identifikovat například i na základě informací o baterii tohoto systému, přičemž webové prohlížeče jsou nezbytnou součástí předávání těchto informací.301 V praxi je užíván postup, který využívá možnosti HTML5. Součástí tohoto standardu je totiž funkce, která umožňuje webovým stránkám (resp. web serveru) zjistit stav baterie počítačového systému, který na ně přistupuje (předávány jsou informace o tom, kolik procent baterie zbývá, za jak dlouho se přibližně vybije nebo nabije). Představa vlastníků web serverů je taková, že uživateli, kterému se vybíjí baterie, bude zobrazena úsporná verze webové stránky. Dva skripty, které popsali právě vědci z Princeton University, data o baterii už skutečně využívají, zároveň sbírají další informace - například IP adresu nebo otisk z canvas fingerprinting. Takové kombinace už mohou poskytnout velmi přesnou identifikaci počítačového systému.

Digitální stopa ovlivnitelná

Digitální stopa ovlivnitelná představuje veškeré informace, které o sobě uživatel sám dobrovolně předá jiné osobě (ať fyzické či právnické, nebo i např. ISP). Pod pojmem předání si je třeba představit celou řadu činností, které mohou spočívat například v odeslání e-mailu, přidání příspěvku do diskuse, fóra, zveřejnění jakýchkoli médií (foto, video, audio aj.) v rámci sociálních sítí, atd. Dále pod tento pojem spadají i registrace a využívání všech představitelných služeb v rámci kyberprostoru [např. operační systémy, e-maily (včetně freemailu), sociální sítě, seznamky, P2P sítě, chaty, blogy, BBS, webové stránky, cloudové služby, datová úložiště aj.]. Digitální stopy ovlivnitelné jsou stopami, nad kterými může mít uživatel relativní kontrolu a je pouze na něm, jaké informace o sobě hodlá zpřístupnit jiným. Je však třeba upozornit na již uvedenou premisu: jakákoli data či informace vložené do kyberprostoru již v kyberprostoru zůstanou. Teoreticky by bylo možné definovat i kategorii hypoteticky ovlivnitelných stop, což je svým způsobem oxymóron, nicméně tato kategorie zahrnuje jisté skutečnosti, na které může mít uživatel teoreticky vliv, tedy je schopen je ovlivnit, ale běžně to nedělá, neboť by de facto značně omezil možnosti svého fungování v digitálním světě. Mezi tyto stopy by pak bylo možné zařadit například používání služeb největších ISP (Microsoft, Apple, Google, Facebook aj.), u nichž je využívání služby podmíněno odsouhlasením smluvních podmínek (EULA), které umožňují těmto ISP získávat značné množství informací.303 Dále je pak do těchto stop možné zahrnout i stopy, jež vznikly např. korelací neovlivnitelných a ovlivnitelných stop; informace, jež o nás zveřejní jiní uživatelé; data, jež jsou zrcadlena; EXIF data.

3.2 Smluvní podmínky (EULA)

V následující části této kapitoly se pokusím popsat, jaké informace jsou standardně o uživatelích sbírány největšími ISP. 305 Specificky jsem si vybral společnost Google Inc., neboť se domnívám, že existuje minimum uživatelů, jež by nikdy nevyužili některý z produktů (např. OS Android, vyhledávací nástroj na www.google.com, Gmail, Google

Chrome aj.) této společnosti.306 Mým cílem v žádném případě není „útok“ na společnost Google Inc. či jiné společnosti (včetně jejich produktů). Smyslem je prezentovat možná bezpečnostní rizika, která jsou spojena s využíváním některých poskytovaných služeb a s akceptací smluvních podmínek (EULA - End Users Licence Agreement), na něž je využívání uvedených služeb vázáno. Smluvní podmínky, umožňující využití služby daného poskytovatele služby nejsou ve své podstatě ničím jiným než zpravidla jednostranně vymezeným definováním práv a povinností ze strany poskytovatele služby (ISP). Uživatel však není nikterak omezován na svých právech, neboť má možnost volby v podobě nevyužití takto jednostranně stanovených smluvních podmínek. V případě souhlasu s využíváním takovýchto služeb je možné obecně konstatovat, že dojde primárně k aplikaci soukromoprávních norem. Otázkou je, zda si uživatel skutečně uvědomuje, jaké smluvní podmínky odsouhlasil, kdy se pro něj stávají závaznými a jaký možný (legální) zásah do jeho základních lidských práv a svobod takto vyslovený souhlas představuje. Další neopomenutelnou skutečností pak je, že takto poskytovaná služba může ovlivnit práva a oprávněné zájmy (např. bezpečnost IT, důvěryhodnost dat aj.) třetích osob (např. zaměstnavatele; osob, kterým je e-mail adresován aj.), které k využívání předmětné služby explicitně souhlas nevyjádřily. Teoreticky je možné konstatovat, že soukromoprávní smlouvu s touto společností za celé období existence této společnosti uzavřely téměř 3 miliardy uživatelů. 307 Smutným faktem zůstává ta skutečnost, že velmi malé procento uživatelů je ochotno číst smluvní podmínky, vztahující se k té které poskytované službě.

Výňatky ze smluvních podmínek společnosti Google Inc.

Google explicitně uvádí, že pokud kterýkoli uživatel začne využívat jakékoli služby společnosti Google, souhlasí s platnými smluvními podmínkami. Dále jasně definuje vztah uživatele a sebe, jakožto poskytovatele služby, v případě, že je uživatel povinen akceptovat další smluvní podmínky. Tento vztah je vyjádřen následujícím způsobem: „Nabídka našich služeb je široká, a na některé se proto mohou vztahovat dodatečné podmínky nebo požadavky (včetně omezení věku). Dodatečné podmínky budou k dispozici spolu s příslušnými službami. Pokud tyto služby použijete, stávají se dodatečné smluvní podmínky součástí smluvních ujednání mezi oběma stranami.“ Již v úvodu smluvních podmínek Google stanoví, že: „Obsah310 můžeme kontrolovat, abychom určili, zda je legální a splňuje naše zásady, a pokud se domníváme, že naše zásady nebo právní předpisy porušuje, můžeme obsah odstranit nebo zamezit jeho zobrazování. Berte prosím na vědomí, že výše uvedené neznamená, že obsah prověřujeme.“ Z hlediska bezpečnosti je dle mého názoru zásadní částí smluvních podmínek sekce, která pojednává o Ochraně osobních údajů a autorských práv. 311 V této části Google definuje, jaké informace o uživatelích shromažďuje a jak s nimi nakládá. Z pohledu bezpečnosti a „pocitu anonymity“ jsou následující informace klíčové. Domnívám se, že deklarace toho, že následující informace jsou shromažďovány „proto, abychom mohli všem našim uživatelům poskytovat lepší služby – od určení jednoduchých věcí, jako je jazyk, kterým mluvíte, až po věci složitější, například reklamy, které pro vás budou nejužitečnější, lidé o které se na webu nejvíce zajímáte, nebo která videa na YouTube by se vám mohla líbit“ je možná chvályhodná, avšak minimálně zarážející. Přirovnání k již zmíněnému Minority Reportu v podobě cílení reklamy je po takovémto prohlášení více než nasnadě. Mimoto se mi opět vybaví Manfred Spitzer a Digitální demence, neboť po čase to již nejsem já, kdo rozhoduje, na co se budu dívat či co budu vyhledávat (resp. mi nemusí být a nejsou nabízeny všechny relevantní odpovědi).

Google shromažďuje informace o uživateli v zásadě dvěma způsoby:

1) Informace, které uživatel sám sdělí. Typicky se jedná o: ◦ jméno, e-mailovou adresu, telefonní číslo nebo platební kartu.

2) Informace získávané při používání služeb Google. Jsou shromažďovány informace o službách, které jsou uživatelem používány, včetně způsobu, jakým jsou používány („například když se podíváte na video na YouTube, navštívíte webové stránky, které využívají naše reklamní služby, nebo sledujete naše reklamy a obsah nebo na ně reagujete“). Dle Google se jedná

o: ◦ Informace o zařízení (např. model hardwaru, verze operačního systému, jedinečné identifikátory zařízení 312 a údaje o mobilní síti včetně telefonního čísla). Google je oprávněn přiřadit k vašemu uživatelskému účtu na Google identifikátory vašeho zařízení nebo vaše telefonní číslo.

◦ Informace z protokolu:

▪ podrobnosti o tom, jakým způsobem uživatel využil službu Google,

▪ **informace z protokolu telefonování** (např. telefonní číslo, číslo volajícího, čísla přesměrování, čas a datum hovorů, trvání hovorů, údaje o směrování zpráv SMS a typy hovorů),

adresa internetového protokolu, ▪ informace o událostech zařízení (např. selhání, činnost systému, nastavení hardwaru, typ prohlížeče, jazyk prohlížeče, datum a čas vašeho požadavku nebo odkazující adresa URL,

▪ **soubory cookie**, které mohou být jedinečnými identifikátory vašeho prohlížeče nebo účtu Google. ◦ Informace o poloze. Google je oprávněn shromažďovat a dále zpracovávat informace o skutečné poloze svého uživatele. Polohu

může Google určovat pomocí různých technologií, jako jsou IP adresa, systém GPS a další senzory, které společnosti Google mohou poskytovat například údaje o zařízeních v okolí, přístupových bodech sítě Wi-Fi a vysílačích mobilních sítí.

◦ **Jedinečná čísla aplikací. Typicky se jedná o licenční číslo a typ (verzi) příslušného nainstalovaného softwarového produktu. Ze smluvních podmínek nevyplývá**, že by se jedinečná čísla aplikací zaznamenávala pouze ze zařízení, jejichž primárním operačním systémem je systém Android. Lze tedy dojít k závěru, že pokud dochází k využívání služeb Google, pak jsou sbírány i informace o jedinečných číslech aplikací i z jiných operačních systémů (iOS, Linux, Windows aj.).

◦ **Místní úložiště. Dle smluvních podmínek může Google**: „shromažďovat a uchovávat informace (včetně osobních údajů) v místním úložišti vašeho zařízení." I v tomto případě lze dojít ke stejnému závěru, jako tomu bylo u jedinečných čísel aplikací. Problémem je dle mého názoru i ta skutečnost, že nikde v obecných smluvních podmínkách není přesně vymezeno,313 jaké umístění a především jaké zabezpečení bude službou Google využito, a tím pádem je teoreticky možné využívat úložiště jako celek. Lze získávat informace o souborech (např. jejich názvy, lokaci, a ad absurdum i hash, který bude následně porovnán např. s databází jiné služby, kde se ukládají data – např. DropBox, OneDrive aj.). Hrozbou pro uživatele pak je dle mého názoru i možnost zneužití takto uložených dat útočníkem. Informace (které se typicky nabalují na cookies aj.) uložené v uživatelově místním úložišti se mohou stát i zajímavým cílem pro útočníka, neboť právě z těchto informací je možné zjistit např. vzorce chování uživatele.

◦ **Soubory cookie a podobné technologie**. „Když navštívíte nějakou službu Google, používáme my i naši partneři různé technologie ke shromažďování a ukládání informací. To může mimo jiné zahrnovat používání souborů cookie nebo podobných technologií k identifikaci vašeho prohlížeče nebo zařízení. Pomocí těchto technologií shromažďujeme a ukládáme informace i v případě, kdy využíváte služby, které nabízíme našim partnerům, jako jsou reklamní služby nebo funkce Google, které se mohou zobrazit na jiných webech."

4 Projevy kyberkriminality

Kyberkriminalita se typicky projevuje prostřednictvím tzv. kybernetických útoků,360 nicméně k úspěšnému uskutečnění řady útoků je třeba využít i ryze netechnické aspekty. Při definování toho, co vše je a co už není kyberkriminalitou, je vhodné využít definici uvedenou v kap. 1.1 Kybernetická trestná činnost (Cybercrime). Určitá protiprávní jednání v kyberprostoru či jednání související s kyberkriminalitou je možné podřadit pod příslušná ustanovení platného trestního zákoníku, existují však určité typy jednání, jejichž označení za trestné činy může být podstatně obtížnější, či dokonce nemožné (v řadě případů se spíše jedná o pouze nemorální jednání).

Velmi často je kyberkriminalita považována za nový druh kriminality, nicméně značná část kyberkriminality využívá či přenáší notoricky známé druhy protiprávního jednání (např. podvody, porušování práv autorských, krádeže, šikanu aj.) do prostředí digitálního, ve kterém je lze páchat „lépe, rychleji, efektivněji" než ve světě reálném. Mezi ryze kybernetické útoky by pak bylo možné zařadit např. hacking, DoS a DDoS útoky, botnety aj.

Pro svět virtuální je příznačné, že většina uživatelů v něj má dle mého názoru až nepochopitelnou, téměř bezmeznou důvěru.361 Přičemž je třeba konstatovat, že svět virtuální se pro nás stává čím dál tím významnějším. Osobně mám pocit, že v případě využívání poskytovaných služeb na Internetu mnoho lidí přestane přemýšlet o možných rizicích či hrozbách. Primárně jsou uchváceni zdánlivě nekonečnými možnostmi „nových technologií"; jak jinak je pak možné vysvětlit si absenci základních obranných principů a mechanismů ve světě virtuálním, když ve světě reálném bychom se chovali zcela jinak. Jindy mi naopak uživatelé kyberprostoru svým chováním v něm připomínají „Podivný případ Dr. Jekylla a pana Hyda" [orig. Strange Case of Dr. Jekyll and Mr. Hyde - Robert Louise Stevenson (1886)]. Zdánlivě slušní lidé ve světě reálném, se v „pseudoanonymním" prostředí kyberprostoru projevují bez jakýchkoli legálních nebo morálních zábran. Je tak možné narazit například na případ soudce, jenž si stahuje „dětskou pornografii"362, uživatele, kteří v reálném světě nikdy nic neukradli, ale ve světě virtuálním nemají problém krást,363 či porušovat jiná práva chráněná zákonem té které země.

K prognózám vývoje kyberkriminality se v minulosti vyjadřovala celá řada předních odborníků, z nichž si dovolím citovat zejména Schneiera, který v roce 2002 predikoval, že dalším velkým bezpečnostním trendem v Internetu bude zločin. „Nepůjde o případy virů, trojských koní a DDoS útoků pro zábavu nebo možnost se vychloubat se svými schopnostmi. Půjde o skutečný zločin. V Internetu.

Zločinci mají sklon zaostávat za vývojem technologií o pět, deset let, ale nakonec si uvědomí jejich možnosti. Tak jako Willie Sutton začal přepadat banky „protože tam byly peníze", tak moderní zločinci začnou útočit přes počítačové sítě. Stále více hodnot (finančních prostředků) je online, než v penězích reálných." 364 V roce 2007 představil

Jirovský statistiku FBI, která porovnávala běžné „bankovní přepadení“ (loupež) s jednáním, které má povahu phishingového útoku.

Goodman v roce 2012 ve vztahu k informačním a komunikačním technologiím uvádí, že „schopnost jedince ovlivnit masy, právě díky těmto technologiím, roste exponenciálně. Exponenciálně roste jak v oblasti ‚dobrého, tak zlého účelu‘“. Názorně tento růst prezentuje na vývoji zločinu loupeže, ke kterému v minulosti původně stačil nůž či pistole a de facto docházelo k loupežnému přepadení mezi jednotlivci či malými skupinami. „K zásadní „inovaci“ došlo v okamžiku loupežného přepadení celého vlaku, ve kterém cestovalo 200 lidí.“ Internet umožňuje ještě výraznější rozsah útoku jedné osoby. Okradení velkého množství uživatelů dobře demonstruje případ Sony Playstation s přibližně 100 miliony poškozených osob. „Kdy v historii lidstva mohl jedinec okrást 100 milionů lidí? Ale nejde jen o krádeže…“ 366 V témže roce vystoupil s proslovem na RSA Cyber Security Conference (San Francisco, CA) ředitel FBI Robert S. Mueller, který mimo jiné ve své řeči uvedl: „Jsem přesvědčen o tom, že existují pouze dva druhy společností: takové, do kterých se již hackeři nabourali, a ty, do nichž se teprve nabourají. A i tyto dvě skupiny se velmi rychle spojují v kategorii jedinou: společnosti, do jejichž systémů hackeři pronikli, a společnosti do nichž proniknou znovu.

V současnosti dochází ke stále většímu a masivnějšímu propojování různých počítačových systému do kyberprostoru, což de facto generuje přímou úměru spočívající v následujícím tvrzení: „čím více je připojených zařízení, tím větší je jejich zranitelnost a tím větší bude počet útoků.“ Jedno z grafických znázornění probíhajících útoků je možné nalézt na stránkách: http://map.norsecorp.com/#/; https://cybermap.kaspersky.com/; https://map.lookingglasscyber.com/ aj.

Domnívám se, že není možné pochybovat o tom, že kyberkriminalita je na vzestupu a představuje celosvětový problém. Různé statistiky uvádějí částečně rozdílné škody způsobené právě kyberkriminalitou, nic to však nemění na tom, že všechny do těchto škod započítávají škody primární (např. nefunkčnost počítačového systému, jeho části, nabízené služby, výpadek infrastruktury aj.) a škody sekundární (např. obnova systémů, záchrana dat, znovu připojování koncových uživatelů aj.). Europol ve své zprávě z roku 2014368 uvádí, že kyberkriminalita stojí globální ekonomiky přibližně 300 miliard $ ročně. Komunita útočníků se od masového rozšíření Internetu značně změnila. Primárně už se nejedná o individuality, které páchaly protiprávní jednání pro zábavu či překonávání překážek. V současnosti se zpravidla jedná o profesionály, kteří svoji činnost dělají s cílem profitovat a nezřídka jsou zapojeni do organizovaných skupin.

Tento posun je pochopitelný a neodmyslitelně spojený se třemi aspekty:

1) Závislost společnosti na Internetu (resp. nabízených službách, technologiích aj.),
2) Kyberkriminalita se stala výnosným globálním businessem [již první kybernetické útoky ukázaly možnosti zisku finančních prostředků, ať již přímo (odčerpáním financí), či zprostředkovaně (např. platbou za poškození služby jiné osoby)].
3) Minimální gramotnost uživatelů, kteří značně využívají informační a komunikační technologie (uživatel je typickým příkladem toho nejslabšího článku řetězu).

S rozvojem všemožných služeb postavených na principu as-a-service369 vznikla i v prostředí kyberkriminality řada platforem (typicky undergroundových, darknet fór), kde jsou nabízeny služby, které je možné označit za Crime-as-a-service (cybercrime-as-a-service). Dochází tedy ke vzniku „malware či underground economy“, která poskytuje téměř jakémukoli uživateli prostředky ke spáchání kybernetických trestných činů. V rámci služby souhrnně označované crime-as-a-service jsou standardně nabízeny následující služby:

- Research-as-a-service,370
- Crimeware-as-a-service,371
- Infrastructure-as-a-service,372
- Hacking-as-a-service,373
- Data-as-a-service,374
- Spam-as-a-service,375
- Ransomware-as-a-service376 aj.

Výčet jednotlivých služeb není konečný a je možné konstatovat, že v rámci služby crime-as-a-service si lze objednat jakoukoli myslitelnou službu nebo komoditu, kterou lze v kyberprostoru využít či získat. Rozmach těchto negativních aktivit je přímo spojen i s fenoménem Internetu věcí (IoT), který propojuje zařízení (počítačové systémy) s Internetem, a představuje tak další výraznou hrozbu, která primárně spočívá v nerespektování některého ze základních principů bezpečnosti.

Řada výrobců či distributorů počítačových systémů, které je možné zařadit pod pojem IoT, neřeší otázku bezpečnosti (jejich cílem je co nejdříve na trh uvést a prodat co nejvíce zařízení, jež je možné označit za počítačový systém), čehož útočníci využívají.

Náklady spojené s vývojem v oblasti bezpečnosti jsou zpravidla nejnákladnější součástí vývoje, nicméně je to oblast, které je třeba se věnovat i s ohledem na již známé hrozby. Mezi ně například patří: nezabezpečený komunikační kanál u kardiostimulátoru;378 auto či letadlo, jež lze ovládat na dálku;379 chytrá domácnost či její součásti (lednice, kotel, zabezpečovací systém, televize aj.), jež lze ovládat na dálku380 aj. „Jak asi dopadne svět, když máme už tento rok využívat 6,4 miliardy zařízení spadajících do IoT. Za další čtyři roky by to mělo být 20,8 miliardy zařízení. Řada z těchto zařízení navíc bude mít oproti běžnému životnímu cyklu mobilních telefonů, tabletů či laptopů podstatně delší životnost. Jak bude výrobce automobilů schopen chránit bezpečnost modelu z roku 2020 o deset let později? Nebo ledničky, která vám doma může stát i dobrých patnáct let? Jak dlouho trvalo, než se Microsoft naučil, jak aktualizovat vlastní operační systém?

Schneier ve vztahu k datům uvádí, že útočníci s nimi mohou dělat v podstatě tři základní věci: krást je (narušení principu Confidentiality – důvěrnosti), měnit je (narušení principu Integrity – celistvosti) nebo zabraňovat vlastníkům v přístupu k nim (narušení principu Availability – dostupnosti). Schneier uvádí, že s nástupem IoT se právě poslední dva druhy útoků stanou extrémně účinné.382 V následující části představím některé útoky, ke kterým v prostředí kyberprostoru dochází. Nelze vymezit všechny útoky, ať již z důvodu rozsahu této publikace, či z důvodu nemožnosti popisu všech možných alternativních jednání subsumovatelných pod pojem kyberkriminalita. Pokud to bude možné, bude u konkrétního projevu kyberkriminality uvedena i případná trestněprávní kvalifikace takovéhoto jednání.

4.1 Sociální inženýrství (Sociotechnika)

Pouze dvě věci jsou nekonečné: vesmír a lidská hloupost. Ačkoli tím prvním si nejsem jist.” Albert Einstein

Sociální inženýrství nelze za každých okolností považovat přímo za kybernetický útok, nicméně je předpokladem pro to, aby byla řada kybernetických útoků úspěšná. Pokud bychom chtěli definovat pojem sociální inženýrství, bylo by možné říci, že jde o ovlivňování, přesvědčování či manipulaci s lidmi s cílem je donutit provést určitou akci, či od nich získat informace, které by jinak neposkytli. Smyslem je v oběti navodit dojem, že situace, v níž se nachází, je jiná, než ve skutečnosti je. Zjednodušeněji by se dalo říci, že se jedná o „umění klamu“, přičemž Mitnick rozlišuje dvě specializace v povolání umělce-manipulátora. „Ten kdo mámí z lidí peníze je obyčejný podvodník, zatímco ten kdo využívá manipulace a přesvědčování vůči firmám – obvykle se záměrem získání informací – je sociotechnik.“ 3

Jsem přesvědčen, že toto tvrzení Mitnicka z roku 2003 by v současném digitálním světě neobstálo, neboť řada útočníků využívá techniky sociálního inženýrství pro to, aby získala právě informace či data a dále je využila například v rámci služby crime-as-a-service. Dále jsou tyto techniky využívány nejen vůči firmám, ale i vůči jednotlivcům. Vlastní útok primárně nemusí mít podobu podvodu, ale následně mohou být tyto informace prodány či zneužity k závažnějšímu útoku. Hlavní myšlenkou sociálního inženýrství je nevyužívat různé ryze technické přístupy či nástroje například k prolomení hesla, když mnohem jednodušší je uvést oběť v omyl, ve kterém sama dobrovolně toto heslo prozradí. Nejslabším článkem bezpečnostního systému je a vždy bude člověk (uživatel). Jelikož na světě nemůže existovat počítačový systém, který by alespoň v nějaké fázi nebyl závislý na člověku (ať již jde o zprovoznění, nastavení, či údržbu počítačového systému), je nejjednodušší cestou získat potřebné informace právě od člověka.

Právě jednoduchost útoku zacíleného na nejslabší článek celého systému z něj zpravidla činí tu nejúčinnější formu. Sociální inženýrství se do popředí dostalo s kauzou Mitnicka, 384 který je mnohými považován za hackera, avšak sám se spíše považuje za sociotechnika. Mitnick ve svých knihách385 ukazuje, jak jednoduše lze získat informace, které jsou citlivé a představují bezpečnostní riziko pro jedince i organizace. V rámci slyšení před U.S. Senate Committee on

Governmental Affairs,386 kde Mitnick vypovídal, jak získával hesla a citlivé informace k počítačovým systémům firem, do kterých pronikl, mimo jiné Mitnick uvedl: „Představil jsem se jako někdo jiný a prostě jsem o ně požádal."

Pro sociální inženýrství je jedním z klíčových faktorů zisk co největšího množství informací o cíli útoku (ať již počítačovém systému, právnické či fyzické osobě). Mnohdy dochází k dlouhodobému působení na klíčovou osobu a budování „důvěry" mezi útočníkem a obětí před vlastním útokem, přičemž útočník typicky využívá lidské neopatrnosti, důvěřivosti, ochoty pomoci jiným, lenosti, slabosti, strachu (např. aby se osoba nedostala do problémů), neodpovědnosti, hlouposti aj. Výše uvedené lidské vlastnosti značně napomáhají útočníkovi realizovat jeho útok. Sami si položte otázku, jak moc si ověřujete protistranu například při telefonátu či komunikaci skrze ICT? Jak moc si prověřujete paměťová média (USB disky, paměťové karty aj.), které jste získali darem na prezentační akci?

Zejména v oblasti ICT je možné sledovat stále sofistikovanější a propracovanější útoky [např. kvalitně připravené podvodné e-maily, reálné instituce (použité jako domnělý odesílatel), přesměrování na podvodné stránky či instalace malware obsaženého v příloze dokumentu nebo na paměťovém médiu aj.387]. Sociální inženýrství bylo i jedním z nezbytných prostředků, bez nichž bychom nemohli provést například útoky popsané v kap. 3.4 Projekty testující zranitelnosti uživatelů sociálních sítí.

Útoky sociálního inženýrství jsou zpravidla vedeny třemi způsoby, přičemž tyto způsoby jsou navzájem kombinovány:

1) **Sběr volně** (veřejně) dostupných dat o cíli útoku
2) **Fyzický útok** (útočník se například vydává za pracovníka servisní agentury – např. servis tiskáren, pracovník údržby aj.), při kterém se útočník snaží získat co nejvíce informací „zevnitř" společnosti, případně citlivé informace o jednotlivých pracovnících (včetně např. prohledávání odpadků aj.)

3) Psychologický útok

Mezi nejčastější metody útoků sociálního inženýrství lze zařadit:
1) Podvodný e-mail či falešná webová stránka388
2) Telefonický hovor
3) Útok „tváří v tvář"
4) Prohledávání odpadků („Dumpster diving" a také „cezení dat")
5) Prohledávání webu, sociálních sítí aj. (jedná se o jednoduše dosažitelný otevřený zdroj dat pro útočníky sociálního inženýrství, který pomáhá zjistit, případně ověřit informace o potenciálním cíli). Veřejné informace dostupné online (např. životopisy, práce, teze, návrhy aj. uveřejněné na Internetu). Výroční zprávy a jiné veřejně dostupné informace o společnosti
6) Doručení reklamních či jiných materiálů na CD, DVD či jiném paměťovém nosiči
7) Ponechání paměťového média (USB aj.) v zájmové oblasti (např. firmě, u domu zaměstnance aj. toto médium pak typicky obsahuje malware) 389
8) Nabídka vyzkoušení služby online (např. nabídka cloudového úložiště, či některé zajímavé služby zdarma aj.)
9) Dodávka či nalezení zařízení (počítačového systému)
10) Falešný servisní technik
11) Jiné

Pokud jde o cíl útoků sociálního inženýrství v rámci organizace, pak se možnými cíli mohou stát například:

- řídící pozice,
- IT oddělení,
- pracovníci help desků,
- recepční (sekretariáty),
- bezpečnostní pracovníci,
- správa budov,
- úklid aj.

Sociotechnik je schopen díky svým schopnostem manipulovat s lidmi, nicméně prostá manipulace není v některých případech dostačující a je třeba propojit tyto informace s technickými znalostmi v oblasti ICT. Na závěr této kapitoly uvádím příklad, na němž Mitnick demonstruje právě propojení sociálních technik se znalostmi ICT.

Mladý hacker, kterému budu říkat Ivan Peters, si dal za cíl získat zdrojový kód nové hry. Bez potíží se dostal do firemní sítě WAN, protože jeho hackerský kolega se už dříve dokázal nabourat na jeden z jejich webových serverů. Po odhalení jisté slabiny v softwaru div že nespadl ze židle. Ukázalo se, že systém používal tzv. dual homing, což znamená, že měl odtud přístup i do vnitřní sítě. Avšak po připojení stál Ivan před podobným problémem, před jakým stojí turista v Louvre, který chce najít portrét Mony Lisy. Bez průvodce by se tam mohl motat celé týdny. Byla to globální korporace se stovkami kanceláří a tisíci serverů, která ve své síti nezveřejňovala indexy vývojářských systémů nebo jiné průvodcovské služby po svých datech. Místo toho, aby k nalezení serveru, na který se potřeboval dostat, použil technologické metody, využil metodu sociotechnickou. Uskutečnil několik telefonátů na základě postupů v této knize už popsaných. Nejprve zatelefonoval na technickou pomoc oddělení informatiky, představil se jako zaměstnanec firmy a řekl, že by rád probral jistý problém spojený s rozhraním produktu, na kterém pracovala jeho skupina. Požádal o telefonní číslo na šéfa projektů ve skupině programátorů, kteří se zabývali hrami. Potom zavolal na toto číslo a předstíral, že je pracovníkem oddělení Informatiky. „Ještě dnes večer," řekl, „budeme měnit router a chceme se ujistit, že lidé z vaší skupiny neztratí spojení se serverem. Který server používáte?" Síť byla neustále vylepšována a sdělení jména serveru nemůže ničemu vadit, že? Vždyť je přece chráněn heslem a samotná znalost jména nikomu nic nepřinese. A tak šéf projektů uvedl jméno serveru. Ani se nepokusil o zpětné zavolání a ověření této historky nebo alespoň o zapsání jména a telefonního čísla volajícího. Prostě sdělil jména serverů: ATM5 a ATM6.

Nyní se Ivan vrátil k technologickým metodám, aby získal autentikační informace. Ve většině případů je prvním krokem identifikace účtu se snadným heslem, které dovolí získat v systému první opěrný bod. Pokud se útočník pokouší za pomoci hackerských nástrojů vzdáleně identifikovat hesla, vyžaduje to být po dlouhé hodiny připojen k firemní síti. Objevuje se tu nebezpečí: čím déle bude připojen k síti, tím větší je riziko jeho odhalení a dopadení. Nejprve použil Ivan enumeraci, která umožňuje odhalit podrobnost o systému. Jako obvykle je možné vhodné nástroje nalézt na Internetu, (http://mtslenth.0catch.com). Ivan našel na webu několik volně dostupných hackerských nástrojů, které mu dovolily proces zautomatizovat a vyhnout se tak ruční práci, která by prodlužovala čas operace, a tím by zvětšovala i riziko dopadení. Věděl, že firma většinou používá servery na platformě Windows a stáhl si program NTBEnum - enumerační nástroj391 NetBIOS (basic input/output system). Zadal IP adresu serveru ATM5 a spustil program. Nástroj dokázal identifikovat několik existujících kont na serveru. Po identifikaci existujících kont stejný program umožnil spuštění slovníkového útoku. Slovníkový útok je dobře známý lidem zabývajícím se bezpečností počítačových systémů a samozřejmě i hackerům. Ostatní lidi fakt, že je něco takového vůbec možné, šokuje. Tento útok má za cíl zjištění hesel uživatelů pomocí obecně užívaných slov. Všichni jsme v některých věcech líní, ale nikdy mne nepřestane udivovat, že při výběru hesla má lidská kreativita a představivost prázdniny. Většina z nás chce mít heslo, které nás ochrání, ale zároveň je lehké si ho pamatovat. Obvykle to znamená použití nějakého nám blízkého slova. Mohou to být například naše iniciály, druhé jméno, přezdívka, jméno manžela, název oblíbené písničky, filmu či značky piva. Dále pak jméno ulice či města, kde bydlíme, značka auta, kterým jezdíme, oblíbené prázdninové místo nebo jméno potoka, kde nejlépe berou pstruzi. Vidíme to pravidlo? Většinou jsou to jména nebo výrazy, které lze najít ve slovníku. Slovníkový útok zkouší postupně výrazy ze slovníku jako heslo jednoho či více uživatelů. Ivan provedl slovníkový útok ve třech fázích. V první fázi seznam 800 nejčastěji používaných hesel. Seznam obsahuje taková jako secret, work nebo password (tedy tajné, práce, heslo). Kromě toho program tvořil permutace těchto výrazů s doplněnými číslicemi nebo s číslem aktuálního měsíce. Program zkoušel každé heslo na všech nalezených účtech v systému. Bez výsledku. Ve druhé fázi si otevřel stránku vyhledávače Google a zadal výraz „wordlists dictionaries“ a našel tisíce stran obsahující seznamy slov a anglické i jiné slovníky. Stáhl si celý elektronický anglický slovník. Doplnil ho o několik seznamů výrazů, které našel vyhledávač. Ivan si vybral adresu www.outpost9.com/files/Wordlists.html. Z této stránky se mu podařilo stáhnout (úplně zadarmo) sadu souborů obsahující příjmení, neobvyklá jména, jména a výrazy spojené s politikou, jména herců a slova a jména pocházející z Bible. Jiná stránka se seznamy výrazů je dostupná na univerzitě v Oxfordu na adrese ftp://ftp.ox.ac.uk/pub/wordlists. Na jiných adresách můžeme najít seznamy se jmény postav z animovaných filmů, citáty ze Shakespeara, z Odyssey, z Tolkiena i Hvězdných válek a také slova spojená s vědou, náboženstvím atd. (Jedna internetová firma prodává seznam obsahující 4,4 milionu slov a jmen za pouhých 20 dolarů.) Atakující program může být zkonfigurován i tak, aby tvořil na základě výrazů ze slovníku anagramy - to je další oblíbená metoda uživatelů, která má zvětšit jejich bezpečnost. Když si Ivan vybral seznam, který použije a spustil program, přepnul ho do automatického režimu a mohl

se tak věnovat něčemu jinému. Člověk by si myslel, že takový útok dá útočníkovi čas na delší šlofíček a dokonce, že až se vzbudí, bude pokrok nevelký. Ve skutečnosti může být - v závislosti na druhu napadeného systému, konfiguraci bezpečnostních systémů a rychlosti připojení - plná slovní zásoba z anglického slovníku otestována za 30 minut! Během útoku zapnul Ivan druhý počítač a rozběhl podobný útok na druhý server, který používala skupina programátorů, ATM6. O dvacet minut později se podařilo něco, co se většině lidí zdá nemožné: prolomit heslo a odhalit, že jeden z uživatelů si zvolil heslo „Frodo", jméno jednoho z hobitů, hrdiny Pána prstenů. S heslem v ruce se Ivan mohl připojit k serveru ATM6. Čekala tam na něho dobrá a špatná zpráva. Dobrá, že konto, na které se naboural, mělo administrátorská práva. A špatná, že tam nikde nemohl najít zdrojový kód hry. Zřejmě byl na druhém serveru, ATM5, který se slovníkovému útoku ubránil. Ivan však neházel flintu do žita - stále ještě měl v zásobě pár triků. V některých operačních systémech Windows a UNIX jsou zašifrovaná hesla přístupná každému, kdo má přístup na počítač, kde jsou umístěná. Důvodem je fakt, že zakódovaná hesla nelze dekódovat zpět a tedy není důvod je chránit. Tato teorie je mylná. Pomocí dalšího nástroje dostupného na síti, pwdump3, si stáhl zakódovaná hesla ze serveru ATM6. Typický soubor se zakódovanými hesly vypadá takto:

Administrator: 500:95E4321A38AD8D6AB75E0C8D76954A50:2E48927AQB04F3BFB341E266D6L
akasper:1110:5A8D7E9E3C3954F642C5C736306CBFEF:393CE7F90A8357F157873D72D
digger:1111:5D15COD58D0216C525AD3B83FA6627C7:17AD564144308B42B8403D01AE256555
ellgan:1112:2017DA45D8O1383EFF17365FAF1FFE89:07AEC950C22CBB9C2C734EB89j1
tafeeck:1115:9F5890B3FECCAB7EAAD3B435B51404EE:1F0115A728447212FC05E1D20820335
vkantar;1116:81A6A5D035596E7DAAD3B435B51404EE:B933D36DD12258946FCC7BD153F1CD6
vwallwick:1119:25904EC665BA30F44494F42E1054F192:15B2B7953FB632907455D2706A432 mmcdonald:
1121:A4AED098D29A3217AAD3B435B51404EE:40670F936B79C2ED522F5ECA939c
kworkman:1141:C5C598AF45768635AAD3B435B51404EE:DEC8E827A121273EF084CDBF5FD192

Když měl soubor u sebe na počítači, použil Ivan další nástroj, který prováděl tzv. útok hrubou silou. 392 Ten zkouší všechny kombinace alfanumerických a většiny speciálních znaků. Ivan použil nástroj L0phtcrack3 (čti loft-crack; je dostupný na adrese www.atstake.com; jiný zdroj vynikajících nástrojů na hádání hesel je www.elcomsoft.com). Správci používají L0phtcrack3 na vyhledávání „slabých“ hesel a hackeři na jejich proražení. L0phtcrack3 umožňuje zkoušet hesla s kombinacemi písmen, číslic a většiny symbolů včetně @#$%^&. Systematicky testuje všechny možné kombinace většiny znaků. (Pokud jsou však v hesle použity neviditelné znaky, L0phtcrack3 nebude schopný heslo odhalit.) Tento program pracuje s neuvěřitelnou rychlostí, která může na počítači s frekvencí procesoru 1 GHz dosáhnout hodnoty 2,8 milionu pokusu za sekundu. Dokonce i při této rychlosti může, pokud správce dobře zkonfiguroval systém Windows (tj. vypnul používání hašování LANMAN), prolomení hesla zabrat hodně času. Z tohoto důvodu si útočník často stahuje soubory s hesly na svůj počítač a spouští útok u sebe, aby neriskoval odhalení během dlouho udržovaného spojení. Ivan nemusel čekat dlouho. O několik hodin později našel program hesla všech členů skupiny programátorů. Byla to však hesla uživatelů na ATM6, kde nebyl zdrojový kód. Co teď? Stále nebyl schopen získat hesla umožňující přístup k serveru ATM5. Jako hacker si uvědomoval zlozvyky většiny uživatelů a došel k závěru, že si někdo z členů týmu mohl vybrat stejné heslo na obou serverech. A bylo to tak. Jeden z programátorů měl heslo gamers jak na ATM5, tak i na ATM6. Před Ivanem se otevřely dveře k hledání zdrojového kódu. Když ho našel a stáhl si celý strom, učinil ještě jednu pro hackera typickou věc. Změnil heslo na spícím kontě s administrátorskými právy, čistě pro případ, že by se sem chtěl později vrátit a stáhnout si novou verzi programu.

K redukci rizik sociálního inženýrství je nezbytné zvyšovat povědomí o možných hrozbách nejen v rámci organizace, ale v rámci celé společnosti. Jak jsem již uvedl dříve, sociální inženýrství pomáhá uskutečnit útok, přičemž je zcela na útočníkovi, aby určil, kdo bude jeho cílem. Pro útočníka je mnohem snazší zaměřit svůj útok na masy nezkušených a neznalých lidí, než na relativně dobře chráněnou společnost. V této souvislosti je vhodné připomenout dva výroky, které mohou komukoli pomoci v rámci obrany nejen před sociálním inženýrstvím:

„Důvěřuj, ale prověřuj.“ Ronald Regan a „Přežije jen paranoik.“ Andrew S. Growe