UNIVERZITA KARLOVA

Právnická fakulta

Jan Kopáč

Kriminologické aspekty kybernetické kriminality

Diplomová práce

Vedoucí diplomové práce: doc. JUDr. Bc. Tomáš Gřivna, Ph.D.

Katedra: Katedra trestního práva

Datum vypracování práce: 20. 10. 2020

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 186 813 znaků včetně mezer.

……

Jan Kopáč

V Praze dne 19. 10. 2020

Rád bych poděkoval vedoucímu své diplomové práce, panu doc. JUDr. Bc. Tomáši Gřivnovi, Ph.D. za pomoc a rady, které mi pomohly při psaní mé práce. Dále bych rád poděkoval všem, kteří mi byli oporou a měli se mnou trpělivost během studia, a to zejména rodičům.

Obsah

Úvod

Oblast informačních a komunikačních technologií je patrně jedním z nejrychleji se rozvíjejících sektorů vůbec. Pro dnešní mladistvé je znalost prostředí počítačů a mobilních zařízení něčím, co neodmyslitelně patří do jejich každodenního života. Naopak pro generaci našich prarodičů, jsou počítače často pekelným zařízením a doufají, že se s ním nebudou muset nikdy potýkat. Tyto dvě skupiny obyvatelstva dělí jen několik desítek let, přesto je jejich postoj k informačním a komunikačním technologiím diametrálně rozdílný.

Není tomu ani půl století kdy síť, která je pro dnešní společnost naprosto stěžejní a přímou součástí každodenního života, ještě neexistovala a kdy počítače byly synonymem místnosti plné obřích kovových zařízení, ke kterým měla přístup jen vybraná hrstka obyvatelstva. V dnešní době probíhá spíše diskuze na téma, zda je vhodné, aby dítě mělo již v pěti letech svůj vlastní telefon či tablet a zda se takovým způsobem zábavy nezanedbává výchova.

Vývoj v této oblasti se však nezpomaluje, spíše naopak. Nová technologie je každoročně na velkých veletrzích překonána technologií jinou, o něco propracovanější, dokonalejší a ve všech ohledech lepší. Rok starý mobilní telefon je již zařízením, na které výrobce téměř neposkytuje podporu, pár let stará televize již nemá kvalitní obraz a téměř nový počítač nesplňuje výkonnostní požadavky na nové hry.

S tímto prudkým vývojem v oblasti ICT souvisí propojení dnešní společnosti s technologiemi a s prostorem, ve kterém tyto technologie pracují. V dnešní době odejít do práce bez telefonu je skoro stejný problém, jako si zapomenout klíče. Když se v práci odstaví počítačová síť, tak mnohý zaměstnavatel automaticky reaguje zkrácením pracovní doby a odesláním zaměstnanců domů, neboť podnik není schopen dále fungovat.

Tento, už téměř dvě desítky let vzrůstající fenomén, se mlčky stal součástí našich životů. Přesto si mnoho uživatelů kyberprostoru neuvědomuje, že i ve virtuálním světě je nutno se chovat podobně jako v tom reálném. Je otázkou, kde by se lidé této obezřetnosti mohli naučit, když jejich rodiče mnohdy nemají s tímto prostředím mnoho zkušeností a ve školách i ve společnosti se o rizicích číhajících v kyberprostoru mluví jen zřídka.

Faktory způsobující, že se kyberprostor stává čím dál více atraktivnějším prostředím pro páchání trestné činnosti, tkví především v jeho oblíbenosti, závislosti společnosti na něm a také chování obětí, které vzhledem ke zprostředkovanému kontaktu se světem ztrácejí základní obezřetnost a stejně jako případný pachatel mají pocit anonymity.

Smyslem této práce je blíže popsat kriminologické aspekty, které se týkají kybernetické kriminality, ať už jde o pachatele, o specifické znaky této kriminality nebo o samotné formy

protiprávního jednání v kyberprostoru, přičemž zvláštní pozornost bude věnována zejména nezákonnému jednání v oblasti počítačových dat a systémů a formy a způsoby porušování autorských práv v kybeprostoru.

První část této práce tvoří vzhledem k tématu a jeho propojenosti s technickými znalostmi a s terminologií v prostředí informačních a komunikačních technologií vysvětlení několika pojmů a stručný přehled počátků a postupného vývoje v této oblasti.

Během psaní této práce bych se rád zaměřil na právní úpravu týkající se této problematiky a nakonec zhodnotil, zda je zákonodárcem zvolena správná a efektivní forma, jak takové trestné činnosti předcházet a jak jí především trestat.

Samostatnou část této práce budou tvořit znaky, které jsou pro kybernetickou kriminalitu příznačné a díky kterým je tato forma kriminality stále na vzestupu a zároveň čím dál nebezpečnější.

Důležitou a pravděpodobně nejobsáhlejší částí je přiblížení jednotlivých škodlivých jednání v prostředí kyberprostoru s uvedením vybraných případů a případnou odpovídající trestněprávní kvalifikací.

Jednu kapitolu bych také rád věnoval vybraným dílčím oblastem upraveným v zahraničí a případnému porovnání s právní úpravou v České republice.

Závěrečná část této práce bude věnována současné situaci z pohledu kybernetické kriminality a její očekávaný vývoj a také zhodnocení situace v rámci naší země.

1 Terminologie a vývoj

Pro lepší pochopení problematiky kybernetické kriminality je nutno zpočátku ujasnit, co taková kriminalita vlastně znamená a co obnáší. I přesto, že v dnešní době nejde o nikterak nový společenský fenomén, může mít většina laického obyvatelstva problém jednoznačně odlišit, zda se jedná o kybernetickou kriminalitu a co všechno obnáší, a jaké chování v prostředí internetu a počítače je legální a které už ne.

Dále v této kapitole popíšu samotný vynález počítače a co mu předcházelo, rozvoj internetu a jednotlivé termíny, se kterými se budeme v textu dále setkávat.

1.1 Historie a vznik počítače

Kvůli omezené kapacitě lidské paměti začala u člověka vznikat potřeba vymyslet pomůcky pro ukládání hodnot a případné operace s nimi. Ještě před potřebou operací stačilo člověku pouhé zobrazení hodnot a k tomu bral inspiraci ze svého okolí – především vlastní části těla (prsty na rukou a nohách) a přírodního materiálu, který mu nabízelo okolí jako například klacíky, kosti nebo malé oblázky (latinsky calculus), z čehož vychází později slovo kalkulátor. Později lidé začali hodnoty zaznamenávat pomocí zářezů do dřívek nebo děláním uzlů na provazech. Vyspělejšími a šířeji použitelnějšími nástroji byly abakus a později počítadlo. Abakus se hodil například na počítání ve větším rozsahu, při kterém se pracovalo s mezivýsledkem. Princip práce s abakusem spočíval v pokládání kamenů (později mincí) podle předem dohodnutého klíče na zem (tabuli atd.) na předem vytvořené linky.[1] Vznik abakusu se předpokládá zhruba před 5000 lety a samotný název vycházel ze slova prach („abaq“). Abakus byl nejspíše vynalezen v Babylonii (území dnešního Iráku) kolem 4. století před naším letopočtem. V Evropě se podobnému zařízení říkalo sčot nebo také západní abakus.[2] Na podobném principu jako abakus, ale o něco modernější, byly mincovní desky (počítací desky) na území dnešního Německa nazývané Rechenbank (počítací lavička) - z tohoto výrazu údajně vzniklo označení banka pro dnes nám známé finanční instituce.

Dalším významným milníkem byl vynález knihtisku, jenž umožnil lepší šíření učení počtářských škol – především z území Itálie. Z tohoto období také pochází nejstarší početnice

[1] NAUMANN, Friedrich. Dějiny informatiky: od abaku k internetu. Praha: Academia, 2009. Galileo. ISBN 978-80-200-1730-7. s. 40-46

2 A HISTORY OF THE COMPUTER: PREHISTORY. PBS.org [online]. [cit. 2020-06-30]. Dostupné z: https://www.pbs.org/nerds/timeline/pre.html

v němčině, tzv. Trenský algoritmus z roku 1475. Je v něm například popsán způsob počítání na linách, který vychází z počítání s abakem.[3]

V roce 1614 objevil skotský matematik John Napier převratnou matematickou metodu, která umožnovala násobit a dělit za pomoci sčítání a odčítání logaritmů. Na základě toho vznikly logaritmické tabulky, které následoval vznik logaritmického pravítka. Napier je známý také díky vynálezu početního přístroje zvaného „Napierovi kosti" a zpopularizoval používání desetinné tečky.[4] V roce 1623, krátce po vytvoření logaritmických tabulek, vynalezl německý konstruktér Wilhelm Schickard první mechanický kalkulátor. Kalkulátor, jehož byly vyrobeny celkem tři kusy, dokázal sčítat, odčítat, násobit i dělit s využitím šestipolohového sčítacího strojku a jeho vzájemné součinnosti s počítacími válečky.[5]

Dalším významným pokrokem, který již položil základy dnešního moderního počítače, byl vynález diferenčního stroje Charlese Babbage mezi lety 1820 až 1821. Jednalo se o obří, párou poháněný mechanický kalkulátor sloužící k výpočtu námořnických tabulek pro určení polohy z výšky hvězd nad obzorem. Tyto stále stejné početní operace si Babbage chtěl usnadnit mechanickým zařízením.[6] Následně se Babbage pokusil vytvořit dokonalejší verzi svého diferenciálního stroje – tzv. analytický stroj, ale bohužel zůstalo jen u návrhu. Důvodem, proč nezrealizoval svůj návrh, byla především nemožnost vytvořit dostatečně přesná ozubená kola do tohoto mechanismu. Pokud by se podařilo vynález dokončit, šlo by o vůbec první Turingovsky úplný[7] počítač.[8]

Novodobá historie počítačů, kdy už jde o přístroje fungující na podobných principech jako dnes, se dělí na jednotlivá období zvaná generace. Dosud známe o celkem 5 generací, které se odlišují součástkami, ze kterých je přístroj vyroben, množstvím operací, které je stroj schopen uskutečnit za sekundu, a také počtem skříní, které tvoří jeden počítač.

O první vývojové etapě se mluví jako o nulté generaci počítačů. Hybnou silou samotného vývoje byl zbrojní průmysl a potřeba stále modernější techniky pro případný válečný konflikt. Pro

---

[3] NAUMANN, Friedrich. Dějiny informatiky: od abaku k internetu. Praha: Academia, 2009. Galileo. ISBN 978-80-200-1730-7. s. 49-51

[4] Napier's Bones [online]. [cit. 2020-07-05]. Dostupné z: https://history-computer.com/CalculatingTools/NapiersBones.html

[5] Wilhelm Schickard [online]. [cit. 2020-07-06]. Dostupné z: https://history-computer.com/MechanicalCalculators/Pioneers/Schickard.html

[6] A HISTORY OF THE COMPUTER: PREHISTORY [online]. [cit. 2020-07-06]. Dostupné z: https://www.pbs.org/nerds/timeline/pre.html

[7] Turingovská úplnost značí schopnost emulovat jiné stroje bez nutnosti fyzické přestavby.

[8] Historie počítačů [online]. [cit. 2020-07-06]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=20692

nultou generaci je specifické, že jako hlavní součástka je používáno relé.[9] První takový stroj sestavil v roce 1938 německý inženýr Konrad Zuse. Tento počítač dostal označení Z1, ale pro svoji poruchovost nebyl v praxi příliš využitelný. Vylepšená verze Z2 už obsahovala 200 relé, ale paměť byla převzata ze Z1. Zuse se následně spojil s Helmutem Schreyrem a společně sestavili počítač Z3, který již tvořilo více než 2600 elektromagnetických relé. Na druhé straně oceánu byly nejvýznamnější projekty realizovány v letech 1939-1944 – konkrétně se jednalo o stroj Mark I, který měřil 15 metrů, a jeho vylepšená verze Mark II obsahující již 13 000 relé. Na našem území byl první reléový počítač označený zkratkou SAPO uveden do provozu až v roce 1957.

V poválečném období, přesněji mezi lety 1945 až 1950, vznikaly počítače první generace. Pro tyto počítače je charakteristické používání elektronek a omezování relé. Charakteristické pro tyto stroje byla velká spotřeba energie a velikost přes celé místnosti. Zástupcem této generace je elektronkový počítač ENIAC.

Stejně jako předchozí generace, i generace druhá je charakteristická použitím specifických součástek. Jde o tranzistory, které jsou již polovodičem a které dovolily zlepšit všechny významné parametry (velikost, spolehlivost, výpočetní rychlost a také energetickou náročnost). Druhá generace počítačů se uplatňovala mezi lety 1951 až 1964. Kladl se v ní důraz na snadnější obsluhu, díky čemuž vznikaly první operační systémy. Mezi hlavní zástupce druhé generace patří stroj s názvem UNIVAC, který byl prvním sériově vyráběným počítačem nabízeným ke komerčním účelům.[10]

Se třetí generací přišly významné změny hlavně co do rychlosti, menších rozměrů, mnohem vyššího výkonu a celkové dostupnosti. Tyto stroje už zvládly multitastking a obsahovaly integrované obvody.[11]

Čtvrtá generace se objevila kolem roku 1981 a trvá dodnes. Charakteristickým rysem pro tuto generaci jsou mikroprocesory a používání počítačů pro soukromé účely. V této době se vývojáři mnohem více soustřeďují na vznik softwaru a zdokonalování operačních systémů.

---

[9] Historie počítačů [online]. [cit. 2020-07-06]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=20692

[10] Dějiny počítačů [online]. [cit. 2020-07-09]. Dostupné z: https://cs.wikipedia.org/wiki/D%C4%9Bjiny_po%C4%8D%C3%ADta%C4%8D%C5%AF

[11] The Evolution of Computers [online]. [cit. 2020-07-09]. Dostupné z: https://www.nortonsecurityonline.com/security-center/evolution-of-computers.html

Někdy se také mluví o páté generaci. Tato skupina představuje spíše pohled do budoucna a zahrnuje umělou inteligenci a kvantové počítače. V roce 2019 byl jako první komerčně prodávaný počítač představen stroj s názvem IBM Q System One.[12]

1.2 Internet a jeho rozvoj

Počátky internetu souvisí s vynálezem počítače, ale také (a především) s všudypřítomným konfliktem dvou mocností během studené války. Obavy USA ze vzrůstajícího vědeckému pokroku v SSSR se stupňovaly po startu Sputniku I. Začaly se objevovat spekulace o útoku z vesmíru a zničení dálkových komunikačních zařízení. Reakcí ministerstva obrany USA bylo založení *Advanced Research Projects Agency* (ARPA), které byl až do založení NASA v roce 1958 svěřen dohled nad celým vesmírným programem a později se začala orientovat na spolupráci s univerzitami.[13]

Důležitou osobou v rámci agentury byl J. C. R. Licklider, který měl na starosti oddělení Command and Control. Jeho úkolem bylo vytvoření sítě k přenosu informací, která bude decentralizovaná, aby při případném útoku nebyla narušena její funkčnost.

V roce 1969 byla zprovozněna síť ARPANET, která spojovala čtyři univerzitní počítače v různých částech USA a pomocí které byla odeslána první zpráva.[14] Později došlo i k přenosu celé věty „Are you receiving this?“, která symbolizovala úspěch při vzniku decentralizované sítě.

V roce 1973 se k ARPANETu připojily i univerzity mimo území USA, konkrétně ve Velké Británii a v Norsku. ARPANET skončil v roce 1990. Byl postupně nahrazován INTERNETem, který funguje na podobném principu a předává si informace pomocí protokolu TCP/IP. Od roku 1990 se stal internet přístupný pro civilní a později dokonce komerční účely.[15] Jeho popularita se velice rychle rozšířila a v dnešní době je k němu připojeno už téměř 60 % světové populace. Například v roce 1997 měl internet necelých 70 milionů uživatelů a v dnešní době disponuje internetovým připojením téměř 5 miliard lidí.[16]

---

[12] Dějiny počítačů [online]. [cit. 2020-07-09]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=20692

[13] NAUMANN, Friedrich. Dějiny informatiky: od abaku k internetu. Praha: Academia, 2009. Galileo. ISBN 978-80-200-1730-7, s. 345

[14] Who Invented the Internet? [online]. [cit. 2020-07-12]. Dostupné z: https://www.history.com/news/who-invented-the-internet

[15] Internet [online]. [cit. 2020-07-12]. Dostupné z: https://wikisofia.cz/wiki/Internet

[16] Internet World Stats [online]. [cit. 2020-07-12]. Dostupné z: https://www.internetworldstats.com/stats.htm

Z hlediska samotného pojmu lze konstatovat, že internet je *složitý informační systém jednotlivých sítí, tedy prostředek, prostředí, medium, jehož prostřednictvím dokážou počítače na celém světě vzájemně komunikovat. Internet není právnickou osobou ani subjektem práv a povinností, jako celek nemá svého majitele, který by byl za něj odpovědný, ani centralizované řízení, pouze jednotlivé servery nebo části kabelových spojů jsou ve vlastnictví konkrétních fyzických nebo právnických osob, které však nelze vždy identifikovat a autentizovat. Objekty nacházející se v tomto prostředí mají nereálný charakter, čas na internetu je prakticky jednotný, principy teritoriality na něm ztrácejí téměř smysl, internet je totálně globální a nezná žádné hranice.*[17]

1.3 Kyberprostor a pojem kybernetické kriminality

Pojem kyberprostor poprvé použil ve své povídce „Burning Chrome“ spisovatel William Gibson. Ve své další knize „Neuromancer“ tento pojem popsal následovně: *„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 seřazená v mysli, shluky a souhvězdí dat. Jako světla města…“.* V tomto díle je kyberprostor přirovnáván k přímému spojení mozku člověka s počítačem[18]

Pojem se postupně ujal a začal se více používat. Jako první tento termín s počítačovými a telekomunikačními sítěmi použil americký básník John Perry Barlow, který je mimo jiné autorem Deklarace nezávislosti kyberprostoru, ve které se vyhrazuje proti jakékoliv nadvládě nad kyberprostorem a vymezuje ho jako globální společenský prostor, který je nezávislý na jakékoliv vnější vládě a nelze jej omezit hranicemi. Barlow definoval kyberprostor jako prostor médiové komunikace, který je bez stanovených hranic a tvoří ho v rámci něj samotného transakce, vztahy a myšlenky. Jedná se o svět elektronické komunikace, který se nám zprostředkuje skrze monitor připojený k počítači.[19] Barlow je také zakladatelem organizace Elektronic Frontier Foundation, jejíž aktivita směřuje především v obraně svobody projevu na internetu. K svobodě na internetu se v roce 2011 vyjádřil následovně: *„Svobodně poznávat je právo, které dosud ještě nikdy nebylo*

[17] VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3. s. 533

[18] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2. s. 17

[19] Kybeprostor [online]. [cit. 2020-07-18]. Dostupné z: https://wikisofia.cz/wiki/Kyberprostor

prosazováno, protože to prostě nebylo možné. Jenže díky internetu, pokud půjdeme správnou cestou a pokud budeme bdělí, bude moci každý na celém světě naplňovat svou zvědavost v určité oblasti do takové úrovně, která odpovídá veškerému vědění zbytku lidské populace… Každý může znát všechno, co chce. A to je obrovská změna v tom, co to znamená být člověkem. Nic takového se nikdy předtím nestalo. Bohužel je ale mnoho sil, které se snaží kvůli svým krátkozrakým zájmům tomuto vývoji bránit.“[20]

Na Barlowovo pojetí kyberprostoru navázal americký antropolog David Hakken, který kyberprostor popsal jako *„sociální arénu, do níž vstupují všichni sociální aktéři, kteří používají ke vzájemné sociální interakci pokročilé informační technologie.“* Dále vyjádřil myšlenku, že kyberprostor zasahuje do všech kulturních sfér a životních stylů, které jsou svázány právě prostřednictvím pokročilých informačních technologií.[21]

Určitou definici kyberprostoru přinesl také francouzsko-kanadský filozof Pierre Lévy. Podle něj se jedná o „*nové komunikační prostředí, které povstává z celosvětového propojení počítačů. Tento termín označuje nejen infrastrukturu digitální komunikace, ale zároveň nesmírný oceán informací, který v ní sídlí, stejně tak lidské bytosti, které se po něm plaví a zásobují jej.“*[22]

V dnešní době je termín kyberprostoru zakotven a definován zákonem. Jeho právní úprava se nachází v zákonu o kybernetické bezpečnosti, § 2, písm. a) a zní následovně: v tomto zákoně se rozumí: *kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.*[23] Na otázku, co se skrývá pod pojmem služba elektronických komunikací, nám zákonodárce tento pojem blíže definoval v zákoně o elektronických komunikacích, § 2, písm. n) jako: *službou elektronických komunikací služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize, s výjimkou služeb, které nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaným*

[20] BRDIČKA, Bořivoj. Barlowova Deklarace nezávislosti kyberprostoru [online]. [cit. 2020-07-18]. Dostupné z: https://spomocnik.rvp.cz/clanek/21714/BARLOWOVA-DEKLARACE-NEZAVISLOSTI-KYBERPROSTORU.html

[21] Kyberprostor [online]. [cit. 2020-07-18]. Dostupné z: https://cs.wikipedia.org/wiki/Kyberprostor

[22] Kyberprostor [online]. [cit. 2020-07-19]. Dostupné z: https://wikisofia.cz/wiki/Kyberprostor

[23] Zákon č. 181/2014 Sb.; Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů ve znění pozdějších předpisů

službami elektronických komunikací; nezahrnuje služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací.[24]

Na chápání kyberprostoru z hlediska samotné teorie existují různé definice. Například slovník univerzity z Cambridge obsahuje dvě definice, kde jedna mluví o kyberprostoru jako elektronickém systému, který dovoluje počítačovým uživatelům po celém světě komunikovat nebo zpřístupňovat informace pro jakýkoliv účel.[25] Již odbornější definici najdeme v učebnici kriminologie, kde je kyberprostor popsán jako virtuální prostor, zejména svět internetu, který zahrnuje i jiné sítě a mobilní technologie. Tento prostor se využívá především ke komunikaci, získávání informací, jako přístup k informačním systémům nejen veřejné správy, pro komerční účely, jako místo pro zábavu, ale jak je ve společnosti běžné, tak slouží také k páchání trestné činnosti.[26] Smejkal hovoří o kyberprostoru jako o něčem, co musíme spíše intuitivně nežli striktně chápat jako nehmotný svět informací, který existuje díky vzájemnému propojení systémů, jak komunikačních, tak i informačních. Takovéto propojení vzniká převážně prostřednictvím sítě Internet.[27] T. Gřivna popsal kybernetický prostor následovně „*Kybernetický prostor nemá hmotnou podstatu, je imaginární. Jeho vznik a další existence je však závislá na světě reálném. Vznik kyberprostoru byl esenciálně spjat s určitou úrovní technologické vyspělosti společnosti, s rozvojem informačních a telekomunikačních technologií. Připojením na komunikační a informační služby vytvářejí jednotlivý uživatelé určitý druh společného prostoru, který lze nazvat „kyberprostorem“.*[28] Definice kyberprostoru je obsažena také v komentáři k trestnímu zákoníku od Šámala, který jej popsal jako imaginární a metaforický prostor, který zahrnuje nejen internet, ale také veškeré světové sítě. Kyberprostor má podle něj reálnou, ale i fiktivní podobu a je to místo, kde jsou informace a probíhají zde emailové komunikace etc.[29]

Definice a ujasnění toho, co kyberprostor znamená a co vše zahrnuje, je důležité především k pochopení toho, co vše je vlastně kybernetická kriminalita a jaké jednání se za ní považuje.

---

[24] Zákon č. 127/2005 Sb.; Zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) ve znění pozdějších předpisů

[25] Volně přeloženo z [online]. [cit. 2020-07-20]. Dostupné z: https://dictionary.cambridge.org/dictionary/english/cyberspace

[26] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 338

[27] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a-nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 130

[28] GŘIVNA, Tomáš. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. Acta Universitatis Carolinae. Iuridica. 2008, 2008(4), 21-34. ISSN 0323-0619.

[29] ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5.

Samotná definice kybernetické kriminality vychází z její dřívější formy, z kriminality počítačové, která byla definována již v roce 1995 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:*

a) jako předmět trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité, nebo

b) jako nástroj trestné činnosti“[30]

K této definici je potřeba doplnit, že o počítačovou kriminalitu se nebude jednat v případech, kdy nebude počítač a jeho součást předmětem útoku kvůli svým specifickým vlastnostem. Například hození monitoru z okna a způsobení újmy na zdraví by se nepovažovalo za počítačovou kriminalitu.

Podle Jirovského můžeme kybernetickou kriminalitu označit také kybernalitou a rozumíme jí *takovou činnost, kterou je porušován zákon nebo je v rozporu s morálními pravidly společnosti.* Tato činnost je mířena přímo proti počítačům a jejich příslušenství nebo sítím, či v ní figuruje počítač pouze jako nástroj k páchání samotné trestné činnosti. Další možností je, že síť slouží jako prostředí pro páchání takové činnosti.[31] Smejkal vyčlenil kybernetickou kriminalitu na podobném principu jako je charakterizována kriminalita hospodářská, majetková, násilná atp. tak, že probíhá v určitém prostředí – v kyberprostoru. Dochází tedy k naplnění různých skutkových podstat napříč trestním zákoníkem.[32]

Teorie spojuje přechod z počítačové na kybernetickou kriminalitu zejména s připojením České republiky k internetu a tím také k většímu propojení každodenního života s prostředím informačních a komunikačních technologií.[33] Kybernetickou kriminalitu lze šířeji také chápat jako skupinu zaštiťující všechna protiprávní jednání podle trestního zákoníku, ve kterých se vyskytuje

[30] SMEJKAL, Vladimír, Tomáš SOKOL a Martin VLČEK. Počítačové právo. Praha: C.H. Beck, 1995. Právo a hospodářství (C.H. Beck). ISBN 80-7179-009-5. s. 100

[31] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2. s 19\

[32] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 23

[33] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 389

počítač či jeho části, jakékoliv jemu podobné zařízení sloužící ke zpracování dat nebo médium schopné uchovávat data samostatně nebo jako součást kyberprostoru.[34]

[34] VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3. s. 545

2 Právní úprava

Než začnu mluvit o konkrétní právní úpravě, je důležité si objasnit obecnou působnost práva v prostředí kyberprostoru. Již podle J. Barlowa a jeho Deklarace nezávislosti kyberprostoru z roku 1996 je kyberprostor místem, nad kterým nemá žádná země legislativní pravomoc a nelze se domáhat žádné právní regulace – jedná se o prostor suit generis. Dle Smejkala je kyberprostor místem, ve kterém neplatí žádné zákony a je třeba se řídit těmi, které jsou pro lidstvo obecně závazné.[35] Takovýto prostor je však z hlediska rozdílných právních norem a představ o podobě toho, co je legální a správné napříč internetem, těžké si představit.

Dle Koloucha je stěžejní si položit dvě otázky – zda na internetu platí právo a v případě kladné odpovědi, jaké právní normy se v rámci bez hraničního prostředí, jakým kyberprostor je, uplatní. Druhou otázkou je, jakým způsobem již zvolené právo aplikovat a případné sankce a opatření vymáhat.

Kolouch demonstroval problematiku vynutitelnosti práva na případu vraždy kvůli krádeži v počítačové hře.[36] V tomto případě se poškozený obrátil na policii kvůli krádeži virtuálního vlastnictví a byl odmítnut, že takovéto vlastnictví reálně neexistuje, a tudíž se na něj zákony nevztahují. Jelikož se svých virtuálních práv u policie nebyl schopen dovolat, tak vzal právo do vlastních rukou a virtuálního zloděje zabil.

Tento případ dokazuje, že s rostoucím prolínáním virtuálního života s reálným, kdy lidé již často více vnímají a více se ztotožňují s virtuálním životem, je bezpodmínečně nutné vyřešit právní odpovědnost za chování v prostředí kyberprostoru. Výstižnou ukázku možné budoucnosti prezentuje například film Ready Player One.[37]

Z hlediska působnosti práva na internetu je znám například případ LICRA vs. Yahoo!, ve kterém šlo od dostupnost internetové aukce s nacistickými předměty, jejichž prodej je ve Francii protiprávní. Francouzský soud v tomto případě rozhodl, že je společnost Yahoo! (která má fyzicky servery na území USA) schopna z velké části francouzským občanům zablokovat přístup na takové stránky, tudíž ať tak v určité lhůtě učiní. Proti tomuto rozhodnutí společnost Yahoo! nepodala odvolání, avšak předložila před soud v USA žádost o rozhodnutí, že rozsudek

[35] SMEJKAL, Vladimír. Internet a §§§. Praha: Grada, 2001. ISBN 80-247-0058-1. s. 32
[36] Chinese gamer sentenced to life [online]. [cit. 2020-08-17]. Dostupné z: http://news.bbc.co.uk/2/hi/technology/4072704.stm
[37] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf

francouzského soudu nemůže působit na americkou společnost. Soud v USA následně rozhodl o protiústavnosti výkonu francouzského práva v USA.[38]

2.1 Vnitrostátní úprava

Z hlediska aplikovatelnosti české právní úpravy na jednání v kyberprostoru lze diskutovat hned o několika zákonech, které byť dílčí část materie upravují. V popředí je především zákon č. 40/2009 Sb., trestní zákoník, a zákon č. 181/2014 Sb., o kybernetické bezpečnosti, kterým budu věnovat dál v textu vlastní část.

Dalšími zákony, dle kterých se může uživatel dovolávat svých práv v prostředí kyberprostoru, jsou zákon č. 251/2016 Sb., o některých přestupcích, ve kterém jsou v § 7 blíže specifikovány přestupky v oblasti občanského soužití, kterých se kdokoliv může v prostředí kyberprostoru dopustit. V oblasti autorských práv je dominantní postavení zákona č. 121/2000 Sb. Zákon o právu autorském, ve kterém je v § 40 zakotven způsob ochrany takto nabytých práv. Mezi další významné zákony, které tvoří legislativní rámec způsobu vystupování na internetu, patří například zákon č. 480/2004 Sb., o některých službách informační společnosti, zákon č. 127/2005 Sb., o elektronických komunikacích, a s příchodem GDPR pro širokou veřejnost již známější zákon č. 110/2019 Sb., o zpracování osobních údajů.

Při výčtu zákonů, které mohou upravovat počínání jedince v kyberprostoru, nelze opomenout na komplexní kodex soukromého práva, zákon č. 89/2012. Sb., Občanský zákoník, který má v sobě zakotvenou ochranu podoby a soukromí fyzické osoby. V § 84 tohoto zákona je uvedeno:

Zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.[39]

Tato ochrana se dále vztahuje také na soukromé písemnosti, které je možno považovat za osobní.

2.1.1 Trestní zákoník

Z hlediska trestního práva a zaměření této práce se jedná o nejvýznamnější zákon. Trestní zákoník je jediným právním dokumentem, ve kterém jsou obsaženy veškeré trestné činy, které český právní řád zná. Oproti starému trestnímu zákoníku, tedy zákonu č. 140/1961, zákon

[38] LICRA v. Yahoo! [online]. [cit. 2020-08-18]. Dostupné z: https://en.wikipedia.org/wiki/LICRA_v._Yahoo!
[39] Zákon č. 89/2012

č. 40/2009 lépe reflektuje závazky vyplývající pro Českou republiku z mezinárodních smluv. Z pohledu kybernetické kriminality trestní zákoník reaguje na ratifikaci Úmluvy o počítačové kriminalitě především prostřednictvím implementace zahrnuté do § 230 TZ.[40]

Typickými trestnými činy souvisejícími s kyberprostorem jsou trestné činy § 230 Neoprávněný přístup k počítačovému systému a nosiči informací, § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat a § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti. V rámci konzistence terminologie se používá pojem počítačový systém namísto informační systém, který je definován následovně: *„jakýkoli přístroj nebo skupina vzájemně propojených nebo přidružených přístrojů, z nichž jeden nebo více provádí na základě programu automatické zpracování počítačových údajů, jakož i počítačové údaje uložené, zpracované, opětovně vyhledané nebo přenesené tímto přístrojem či skupinou přístrojů za účelem jeho či jejich provozu, použití, ochrany a údržby.“*[41]

Dalším způsobem, jakým se rozmach kybernetické kriminality a tím pádem nový způsob páchání trestných činu projevil v trestním zákoníku, je přidání či rozšíření kvalifikovaných skutkových podstat u vybraných trestných činů. Tato skutková podstata zní následovně „*veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem*“ nebo jako v případě § 354 odst. (1) písm. c) *prostřednictvím prostředků elektronických komunikací.*

Posledním způsobem, jaký zákonodárce vybral pro vznik nové trestné činnosti, je ponechání stávajících skutkových podstat na nové trestné činy, jelikož způsob páchání ve virtuálním světě odpovídá skutkové podstatě v reálném světě, a tudíž není zapotřebí zvláštní skutková podstata. Takovýmto jednáním je klasicky podvod, který je upraven v § 209 TZ a odpovídá Phishingu, který je rozebrán v kapitole 5.1.4.

2.1.2 Zákon o kybernetické bezpečnosti

Prvním významným impulsem ke vzniku zákona o kybernetické bezpečnosti bylo založení věcného záměru usnesením vlády ze dne 30. 5. 2012. Zároveň byl ředitel Národní bezpečnosti pověřen vypracováním návrhu tohoto zákona.

---

[40] Důvodová zpráva PSN: příloha t0410a0.pdf [online]. [cit. 2020-08-18]. Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?O=5&CT=410&CT1=0#prilohy s. 265-266

[41] Vládní návrh zákona [online]. [cit. 2020-08-18]. Dostupné z: https://www.psp.cz/sqw/text/orig2.sqw?idd=133551 s. 45

Nutnost vzniku tohoto zákona souvisí s výrazným nárůstem používání informačních technologií a s tím související vzrůstající závislosti společnosti na jejich fungování vzhledem k propojení informačních technologií již už se základními potřebami. S takovouto závislostí se však na druhé straně pojí také možné riziko zneužívání takovýchto technologií a případné způsobení značných škod. V případě nejhoršího scénáře se prostřednictvím útoků na informační technologie může ohrozit až samotná existence státu.

Dalším důvodem pro vznik zákona byly mezinárodní závazky vůči státům patřícím do Severoatlantické aliance a Evropské unie, především kvůli specifickému znaku kybernetické kriminality a to, že tato kriminalita nezná hranic.[42] Přehlížet nelze ani fakt stále častějších útoků souvisejících s terorismem, a to včetně kyberterorismu.

Cílem, který si zákonodárce od tohoto zákona sliboval, bylo stanovení podmínek pro fungování a efektivní spolupráci mezi soukromým a veřejným sektorem za účelem řešení případných kybernetických bezpečnostních incidentů. K tomu přispívá zakotvení práv a povinností, které mají mít za cíl zvýšení bezpečnosti kyberprostoru. Primárním cílem této legislativní úpravy je ochránit alespoň nejdůležitější části infrastruktury, které jsou bezpodmínečně nutné pro fungování státu – zejména kritické informační a komunikační struktury, významné informační systémy etc.[43]

Během své existence prošel zákon několika úpravami. Nejvýznamnější byla novelizace v roce 2017, která dala základ pro vznik Národního úřadu pro kybernetickou a informační bezpečnost. Na základě činnosti a zkušenosti tohoto úřadu byla rozšířena působnost tohoto zákona nejen na správce důležitých systémů, ale také na provozovatele takových systémů.[44]

Předmět úpravy zákona o kybernetické bezpečnosti je upraven v § 1 odst. (1) následovně:

(1) Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.

Z komentáře k tomuto zákonu můžeme říct, že kybernetickou bezpečností *rozumíme souhrn prostředků směřujících k zajištění ochrany kybernetického prostoru. Tyto prostředky mohou být různého charakteru-právní, organizační, vzdělávací, technické apod. Pro účely zákona*

---

[42] MAISNER, Martin. Zákon o kybernetické bezpečnosti: komentář. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8. s. 1-2

[43] SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8. s. 75-76

[44] DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4. s. 58-59

o kybernetické bezpečnosti je však nutno termín „kybernetická bezpečnost“ chápat především ve smyslu právních prostředků zajišťujících ochranu kybernetického prostoru, které jsou obsaženy v tomto zákoně.[45]

2.2 Mezinárodní právní úprava

Již z textu výše jasně vyplývá, že vnitrostátní právní úprava je výrazně ovlivněna děním na mezinárodní úrovni. Důvodem je specifický charakter kybernetické kriminality a s tím související častý výskyt mezinárodního prvku v této trestné činnosti. Kvůli tomu je důležitá harmonizace na úrovni mezinárodních organizací a přistoupení k této harmonizaci co největším počtem (ideálně všech) států.

2.2.1 Úmluva o počítačové kriminalitě

Nejvýznamnějším dokumentem v oblasti mezinárodního kybernetického práva je již poměrně stará Úmluva o počítačové kriminalitě, která byla otevřena k podpisu v Budapešti dne 23. 11. 2001.[46]

Za zrodem Úmluvy stojí komise expertů složená ze zástupců z Rady Evropy, USA, Kanady, Japonska a dalších zemí světa, která byla složena na základě rozhodnutí Evropského výboru pro otázky kriminality. Cílem byla harmonizace právních řádů s větší závazností nežli pouhé doporučení. Harmonizace se měla týkat nejen trestního práva hmotného, ale také měla zahrnovat procesně právní úpravu a zakotvit pravidla pro mezinárodní spolupráci.

K platnosti této Úmluvy došlo splněním podmínky ratifikace alespoň pěti smluvními stranami, z nichž alespoň tři byly členy Rady Evropy, a to dne 1. 7. 2004.[47]

K dnešnímu dni k Úmluvě přistoupilo 68 států, z nich tři stále tuto Úmluvu neratifikovali. Česká republika podepsala Úmluvu dne 9. 2. 2005 a ratifikoval ji až 22. 8. 2013.[48]

Z hlediska struktury je Úmluva složena ze 48 článků a obsahuje preambuli a 4 kapitoly. V první kapitole jsou definovány pojmy, se kterými Úmluva pracuje. Druhá kapitola zahrnuje

---

[45] MAISNER, Martin. Zákon o kybernetické bezpečnosti: komentář. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8. s. 62

[46] Úmluva o počítačové kriminalitě - Convention on Cybercrime [online]. [cit. 2020-08-19]. Dostupné z: https://cs.qwe.wiki/wiki/Convention_on_Cybercrime

[47] GŘIVNA, Tomáš a Radim POLČÁK, ed. Kyberkriminalita a právo. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4. s. 103-104

[48] Chart of signatures and ratifications of Treaty 185 [online]. [cit. 2020-08-19]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=SnCoQlkS

požadovanou vnitrostátní úpravu jak hmotného, tak i procesního trestního práva. Ve třetí kapitole jsou upraveny závazky týkající se mezinárodní spolupráce. Poslední kapitola obsahuje závěrečná ustanovení.[49]

Dne 7. 11. 2002 byl přijat výborem ministrů Rady Evropy dodatkový protokol k Úmluvě o počítačové kriminalitě. V tomto dodatkovém protokolu je požadavek na smluvní strany, aby kriminalizovaly šíření rasistického a xenofobního materiálu za využití počítačových systémů. Dále jsou postihovány také hrozby a urážky takového druhu. Zvláštní úpravu má také popírání holocaustu a dalších uskutečněných genocid.

2.2.2 Právní předpisy EU

Evropská unie se snaží o harmonizace právních řádů v rámci unie v prostředí kyberprostoru především pomocí nařízení a směrnic. Jednou z takových snah o harmonizaci je například směrnice 2013/40/EU, o útocích na informační systémy, ve které je snaha o sjednocení minimálních pravidel pro posuzování trestného činu v této oblasti a co největší sblížení případných sankcí za takové provinění. Dále upravuje spolupráci mezi orgány členských států.

Nařízení č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, se v českém právním řádu se promítlo zejména v rámci zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

Dalším aktem v rámci Evropské unie bylo usnesení Evropského parlamentu č. 2017/2068(INI) o boji proti kybernetické kriminalitě ze dne 3. 10. 2017, ve kterém je rekapitulován současný stav kybernetické kriminality a doporučuje zvýšení opatření v oblasti prevence, odpovědnost poskytovatelů služeb, posílení spolupráce na úrovni policejní a justiční a prosazování práva v kyberprostoru.[50]

[49] GŘIVNA, Tomáš a Radim POLČÁK, ed. Kyberkriminalita a právo. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4. s. 105

[50] SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

3 Specifické znaky kybernetické kriminality

Kriminalita v oblasti kyberprostoru je atypická nejen z hlediska prostředí, ve kterém se uskutečňuje, ale existuje mnoho dalších důvodů pro její specifičnost oproti ostatním druhům kriminality. Jedná se o znaky, které jsou pro tento druh kriminality příznačné, a také díky nim zažívá posledních několik let kybernetické kriminalita takový rozmach.

3.1 Anonymita

Jedním z důvodů vysokého nárustu kriminality v prostředí kyberprostoru je bezesporu anonymita uživatele. Avšak tato anonymita je pouze zdánlivá, ale i tak přispívá k tomu, že si pachatel vážnost svého jednání neuvědomuje. To je způsobeno především odstupem od samotného trestného činu, způsobeném vzdáleností, kterou poskytuje kybernetický prostor. Díky těmto okolnostem pachatel často nabere potřebnou kuráž pro páchání trestné činnosti. Taková představa anonymity v kyberprostoru se podle Koloucha zdá být značně naivní.[51] Každý uživatel nacházející se v kyberprostoru po sobě zanechává stopu v podobě IP a MAC adresy náležící zařízení. Tato adresa je specifická pro každé jedno zařízení, avšak dá se pomocí softwaru měnit. V případě IP adresy existuje software, který dokáže tuto adresu vydávat za jinou. V případech, kdy se podaří unikátní adresu spojit s konkrétním zařízením, nastává problém v dokázání, že konkrétní jeden pachatel se dopustil protiprávního jednání.[52] Dalším z běžných způsobů, jak pachatelé předcházejí identifikaci, je využití veřejně přístupných zařízení, u nichž je velice obtížné dohledat konkrétního uživatele. Při prolamování pomyslné anonymity pachatele se často naráží také na problém, že se údaje o pohybu na síti uchovávají jen omezený čas a často se v tomto případě vyskytuje mezinárodní prvek (využití serverů v cizím státě), který celé dokazování komplikuje.

3.2 Latence

Kybernetická kriminalita má zdaleka nejvyšší latenci oproti všem ostatním druhům kriminality. Některé studie uvádějí latenci v rozmezí 90–95 %, která poskytuje případnému

[51] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 133

[52] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 390

pachateli poměrně bezpečné zázemí pro nelegální činnost.[53] Takto vysoká hodnota má hned několik příčin. Jako první je významné chování a znalost prostředí, ve kterém se oběť trestného činu pohybuje. Mnoho uživatelů často nemá povědomí o hrozbách, které se v kyberprostoru vyskytují a ani nejsou dostatečně chráněni před takovými útoky (například pomocí antivirového programu). Oběť tím značně usnadní pachateli páchání nelegální činnosti. Často ani nemá ponětí, že se stala cílem útoku v kyberprostoru nebo že je její zařízení využíváno k páchání další trestné činnosti.[54] Dalším důvodem neoznámení trestné činnosti ze strany poškozeného je neznalost právního řádu a tím pádem nevědomost nelegálnosti takového jednání či naopak vědomí vlastního nelegálního chování v kyberprostoru (typicky se jedná o vlastní nelegální softwarový obsah v počítači) nebo nesouhlas se společenskou škodlivostí v případě využívání produktu takové činnosti (typický příklad porušování autorských práv).[55]

Pro skupinu podnikajících subjektů je příznačné neoznámení, že se staly obětí kybernetického útoku. Důvodem je zejména možná medializace tohoto útoku a hrozba ztráty důvěry klientů (zejména u společnosti nakládající s prostředky a osobními údaji klientů), která by v konečném důsledku způsobila sekundární viktimizaci a následně mnohem větší ztráty nežli primární útok. Takovéto chování by mělo být již minulostí, a to vzhledem k ohlašovací povinnosti uložené dle zákona o kybernetické bezpečnosti vybraným subjektům (tzv. povinným subjektům).[56] Oproti tomu jsou někdy údaje týkající se četnosti útoku a hrozeb na internetu zveličovány, aby motivovaly potencionální oběti k nákupu ochranného softwaru.[57]

V poslední řadě je důvodem vysoké latence kybernetické kriminality neschopnost zákonodárce včas a efektivně reagovat na rychlost vývoje v prostředí informačních a komunikačních technologií a přizpůsobení legislativy rychlosti pokroku.[58]

---

[53] DIANIŠKA, Gustáv. Kriminológia. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2009. Právnické učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 978-80-7380-198-4. s.220

[54] Například k těžbě bitcoinů viz: https://www.e15.cz/kryptomeny/ceske-pocitace-zaplavil-program-ktery-tezi-kryptomeny-bez-vedomi-uzivatelu-1341752

[55] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 391

[56] Hlášení bezpečnostních incidentů [online]. [cit. 2020-07-27]. Dostupné z: https://www.pravniprostor.cz/clanky/pravo-it/hlaseni-bezpecnostnich-incidentu-co-stanovuje-zakon-o-kyberneticke-bezpecnosti-a-co-gdpr

[57] ZAVRŠNIK, Aleš. Kyberkriminalita. Přeložil David BLAŽEK. Praha: Wolters Kluwer, 2017. Právní monografie. ISBN 978-80-7552-758-5. s. 48

[58] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 392

3.3 Dostupnost a globálnost

V případě dostupnosti lze hovořit o finanční náročnosti na pořízení potřebné techniky a jejím rozšířenosti po celém světě. Z hlediska rozšířenosti je směrodatná především statistika aktivních uživatelů internetu. Ze statistiky vyplývá, že k dnešnímu dni je téměř 60 % (4,57 mld.) obyvatelstva planety aktivní na internetu.[59] Ve srovnání s tím například střelných zbraní v rukou civilistů je 850 milionů, z toho necelých 400 milionů v USA.[60] Dalším aspektem, který ukazuje dostupnost kybernetické kriminality je, že kyberprostor pro svojí vlastní existenci nepotřebuje žádné aktivní či pasivní konání jednotlivce nebo nějaké skupiny – existuje již nezávisle a je přístupný, kdykoliv si člověk zamane.

Rozmachu kybernetické kriminality také napomáhají nízké náklady na pořízení vybavení potřebného k páchání nelegálních aktivit v prostředí kyberprostoru. Na začátku samotného technologického boomu bylo vlastnictví stolního počítače doménou vyšší třídy, hlavně pro vyvolené byly později i telefony. V dnešní době má telefon s přístupem na internet a všemi možnými vymoženostmi už téměř každé dítě ve školním věku. Dle statistik už v roce 2016 používalo internet 76,5 % obyvatel České republiky starších 16 let – v tomto případě za posledních 10 let došlo k nárůstu o 10 %. Dospělých uživatelů, kteří mají internet přístupný přímo z mobilu, bylo dle statistik 41 %.[61]

Velkým lákadlem je také možnost získání velkého majetkového prospěchu při vynaložení poměrně malých vstupních nákladů. Často má každý občan ve svém vlastnictví již potřebné vybavení, aby mohl začít v prostředí kyberprostoru škodit, a často nejsou potřeba ani znalosti v oblasti IT za pomocí využití softwaru určeného k páchání trestné činnosti – tzv. exploit.[62]

Globálnost se v mnoha bodech prolíná s dostupností. V dnešní době již není pochyb o tom, že internet je přístupný téměř po celém světě a umožnuje páchat trestnou činnost nehledě na vzdálenost. Taková rozšířenost může z hlediska hmotného práva působit potíže. Velice často se při páchání kybernetické kriminality vyskytuje mezinárodní prvek, avšak zákonodárce (v případě zahraničních prvků by se dalo spíše mluvit o společenství na úrovni například OSN) prozatím

---

[59] Global digital population as of July 2020 [online]. [cit. 2020-07-28]. Dostupné z: https://www.statista.com/statistics/617136/digital-population-worldwide/

[60] Gun ownership [online]. [cit. 2020-07-28]. Dostupné z: https://en.wikipedia.org/wiki/Gun_ownership

[61] Český statistický úřad [online]. [cit. 2020-07-28]. Dostupné z: https://www.czso.cz/csu/czso/internet-v-mobilu-ma-41-dospelych-cechu

[62] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 391

dostatečně na takové případy nereaguje. Může se dokonce stát, že jednání, které je v jednom státě povoleno, je ve druhém zakázáno. A jaký právní řád se pro posuzovaný případ použije, když kyberprostor nemá hranice a klasické zásady pro určování místní příslušnosti se na kybernetickou kriminalitu dají jen složitě aplikovat? K takovému případu došlo v roce 2001, kdy ruský občan vynalezl software, který byl podle ruského práva naprosto legální, ale při prezentaci v USA byl zatčen a souzen.[63]

V neposlední řadě je potřeba zmínit, že dnešní svět je z velké části na kyberprostoru závislý, a to nahrává jeho další globalizaci napříč celým světem. Jen málokdo si v dnešní době dokáže představit svět bez internetu. Kyberprostor je všudypřítomný, i běžné činnosti každého občana zahrnují práci s ním – například komunikace s úřady, bankou (podle statistik využívá internet ke správě vlastních financí již 5,5 milionů obyvatel České republiky)[64], komunikace s rodinou a v neposlední řadě i zábava.

3.4 Společenské rozdíly a absence nadnárodní ochrany

Specifickým znakem kybernetické kriminality je jeho rozšířenost po celém světě. I když mají lidé po celém světě přístup na stejný internet, tak nedisponují stejnou technologickou vyspělostí nebo stejnou kupní silou. To dle Dianiška způsobuje vysokou kriminalitu v oblasti autorských práv především k softwaru v oblastech východní Evropy.[65]

Častou motivací pro páchání trestné činnosti bývají finance, tudíž pro občany méně vyspělých států s nízkou životní úrovní může být kyberprostor zajímavým místem pro vysoký zisk.

Internet má specifické postavení zejména z hlediska postihnutelnosti vlastníka. Jsou zde pouze jednotliví poskytovatelé připojení, ale internet sám o sobě není vlastněn konkrétní osobou a díky své necentralizovanosti neexistuje dostatečně efektivní strážce chování na internetu. V určitém směru je řešením snaha OSN nastavit určitá pravidla a vydávat studie kybernetické kriminality, navíc je vytvořen Úřad OSN pro drogy a kriminalitu[66], který se zabývá i kyberprostorem, ale stále se nedá mluvit o efektivním strážci, který by popíral Barlowovu představu nezávislého internetu.

---

[63] United States v. Elcom Ltd. [online]. [cit. 2020-07-28]. Dostupné z: https://en.wikipedia.org/wiki/United_States_v._Elcom_Ltd.

[64] Český statistický úřad [online]. [cit. 2020-07-28]. Dostupné z: https://www.czso.cz/csu/czso/internetove-bankovnictvi-vyuziva-55-milionu-cechu

[65] DIANIŠKA, Gustáv. Kriminológia. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2009. Právnické učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 978-80-7380-198-4. s. 220

[66] Více viz https://www.unodc.org/

4 Pachatel kybernetické kriminality a jeho oběť

4.1 Pachatel

Obecně se pachatelem trestného činu rozumí ten, *kdo svým jednáním naplnil znaky skutkové podstaty trestného činu nebo jeho pokusu či přípravy, je-li trestná*[67]. Pachatelem může být rovněž právnická osoba, která je odpovědná podle zákona o trestní odpovědnosti právnických osob a řízení proti nim za všechny trestné činy vyjma těch, které jsou uvedeny v § 7 tohoto zákona.

Kybernetická kriminalita zahrnuje mnoho druhů trestné činnosti – od dětské pornografie přes bankovní krádeže až po organizovaný kyberterorismus směřující proti státům samotným. Tudíž se nedá hovořit o tom, že by existoval určitý profil, jaké vlastnosti, vzdělání a případně rodinné poměry jsou pro pachatele typické. Přesto je jedna schopnost, která je k páchání kybernetické kriminality nezbytná. Je to alespoň základní schopnost práce s počítačem. Zároveň je mylná představa, že pachateli jsou převážně odborníci. V dnešní době mohou pachatelé pocházet z různých vrstev, přičemž jejich schopnosti potřebné k páchání kriminality mohou být pouze dovednost vyhledání škodlivého softwaru na internetu a jeho následná instalace. Takový pachatel je v komunitě nazýván „script kiddie“, jelikož jeho schopnost spočívá pouze ve spuštění konkrétního programu bez jakékoliv schopnosti nebo hlubší znalosti.[68] To, že pachatel nemusí být nositelem zvláštních schopností nebo technik, dokládá také studie o kyberzločinu vypracovaná úřadem OSN pro drogy a kriminalitu.[69]

Pachatelé se často rekrutují v raném věku, takže není výjimkou, že jde o osobu z hlediska dikce zákona trestně neodpovědnou.[70] Nejčastějšími pachateli trestné činnosti v kyberprostoru jsou lidé ve věku 18-30 let.[71] Bohužel tato statistika není úplně vypovídající, protože v ní není zahrnuta kriminalita trestně neodpovědných osob, zejména dětí a mladistvých. Zároveň se spodní věková hranice stále posouvá níže z důvodu seznámení se s technikou a jejím používáním již v brzkém věku.[72]

---

[67] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

[68] VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3.

[69] Cybercrime study [online]. [cit. 2019-10-24]. Dostupné z: https://www.unodc.org, s. 39

[70] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7.

[71] Cybercrime study [online]. [cit. 2019-10-24]. Dostupné z: https://www.unodc.org, s. 41

[72] VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3.

Zajímavá je četnost trestných činů dle pohlaví. Jednotlivé studie se liší, ale 85–90 % trestných činů je spácháno muži.[73] Z hlediska recidivy vychází, že většina pachatelů působících v kyberprostoru nemá záznam v rejstříku trestů.[74] Předpokládám, že to může být způsobeno především vysokou latencí, která je typická pro kybernetickou kriminalitu, takže ve skutečnosti je oznámen jen zlomek trestných činů

Dříve bylo pro kybernetickou kriminalitu typické, že se zde téměř nevyskytovaly trestné činy proti životu a zdraví.[75] To způsobilo, že typické pro pachatele této trestné činnosti bylo, že nebyl násilník, ale spíše mu šlo o získání majetkového prospěchu, přístupu k utajeným informacím nebo získání prestiže v internetové komunitě. Dalšími typickými vlastnostmi pachatele bylo vzdělání zejména v technických oborech, vyšší inteligence, zneužívání svého výsadního postavení v zaměstnání, nespokojenost se svým pracovním zařazením a to, že jednají v zásadě individuálně.[76] Avšak v současnosti je mnoho systémů, například zdravotnických, dopravních či dokonce státních, přímo spojeno s kyberprostorem, což vytváří poměrně zajímavý prostor pro kyberterorismus a tím pádem i příliv případných násilných trestných činů.

Na rozlišování jednotlivých pachatelů existuje více kritérií. Pachatele internetové kriminality můžeme nejjednodušším možným způsobem dělit na amatéry a profesionály.[77] O něco málo rozmanitější dělení je na základě profesionality, motivací, schopností a znalostí na novice, kybernetické chuligány, vnitřní nepřítele, malé zlodějíčky, starou gardu, autory škodlivých kódů, profesionální kriminálníky a informační bojovníky.[78] Oproti tomu Smejkal dělí pachatele do 6 hlavních skupin, především podle motivace a způsobu útoku na: 1) pachatele rekrutované z řad zaměstnanců poškozené organizace, 2) průnikáře, kteří mají spíše anarchistické rysy a útočí především pomocí DoS/DDoS útoků, prolamováním a pronikáním do počítačových sítí a zavirováním počítačů, 3) pachatele organizovaného zločinu, zejména praní špinavých peněz, výroba a distribuce pornografie a výroba padělků, 4) profesionály, kteří slouží jako tzv. žoldáci v rámci ozbrojených sil nebo ve výzvědných službách, 5) kyberteroristy a 6) pachatelé většinou

[73] Cybercrime study [online]. [cit. 2019-10-24]. Dostupné z: https://www.unodc.org, s. 42
[74] VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3.
[75] POŽÁR, Josef. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8. s.129
[76] LÁTAL, Ivo, Počítačová (informační) kriminalita a úloha policisty při jejím řešení. Policista, 1998, č.3, příloha s. VIII
[77] LÁTAL, Ivo, Počítačová (informační) kriminalita a úloha policisty při jejím řešení. Policista, 1998, č.3, příloha s. IX
[78] HOLCR, Květoň a Jaroslav FENYK. Kriminológia. Bratislava: Iura Edition, 2008. ISBN 978-80-8078-206-1. s. 362

ve věku blízkém věku dětí nebo mladistvých, kteří často ani netuší, že páchají trestnou činnost anebo nepočítají s trestností daného jednání.[79] Následující kapitoly jsou detailněji zaměřeny na tři skupiny pachatelů kybernetické kriminality.

4.1.1 Hacker

Pro mnohé pojem hacker ztělesňuje obecně pachatele kriminality v prostředí počítačů či na internetu. Běžně se tedy v médiích a celkově ve společnosti setkáváme, že jakýkoliv trestný čin spáchaný prostřednictvím počítače spáchal hacker. Avšak tento pojem byl vymyšlen studenty *slavného Massachussetského technologického institutu, kde byl postaven první moderní počítačový systém.*[80] V Massachussetském technologickém institutu (MIT) byla Richardem Stallmanem založena nadace Free Software Foundation, ze které vyšel podnět, aby autorské právo označované anglicky jako copyright bylo nahrazeno termínem copyleft. Toto právo bylo podle nadace odvozeno od základních lidských práv a v nich zahrnutého práva na svobodu projevu, jehož součástí je i volné používání softwaru a svobodná komunikace na internetu[81]. Pojem hacker v té době ještě nebyl výraz pro někoho, kdo páchá kriminalitu, ale jednalo se spíše o osobu s určitou schopností počítačového programování. Samotný hacking v té době nebyl chápán jako činnost, která by byla ve společnosti nežádoucí. Po jisté době se poměrně stejnorodá skupina hackerů začala štěpit na dvě odvětví – na počítačové programátory a na opravdové hackery, kteří jsou dnes vnímáni negativně jako pachatelé nelegální činnosti v kyberprostoru. Rozdíl mezi hackery a programátory je v tom, že hackeři jsou považováni za manipulátory v celém technickém systému a působí v něm nikoliv za účelem jeho zlepšení, ale spíše ho nekonvenčním způsobem zneužívají.[82]

Studenti na MIT[83] postupně začali zkoumat počítačový software, který měli k dispozici. Zjištěné limity daného systému se postupem času snažili různým způsobem obejít a příslušný software rozšířit o další funkce. V té době termín hacker označoval experty v oboru a spíše

---

[79] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7. s. 689 - 690

[80] GŘIVNA, Tomáš a Radim POLČÁK. Kyberkriminalita a právo. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4. s. 38

[81] ZAVRŠNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017. Právní monografie. ISBN 978-80-7552-758-5. s. 12

[82] GŘIVNA, Tomáš a Radim POLČÁK. Kyberkriminalita a právo. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4. s. 39

[83] Massachusetts Institute of Technology (MIT)

progresivní programátory. Dále označoval osobu, která používala netradiční způsoby v oblasti práce s programy, která v případě potřeby neváhala porušit pravidla a program si upravit.[84]

V 70. letech 20. století se rozšířila metoda tzv. „phone phreakingu“ což znamenalo, prolomování a upravování telefonních systému takovým způsobem, aby byl uživatel schopen volat bez nutnosti za hovor platit.[85] Na základě tohoto objevu vyrobili dva členové Homebrew Computer Club of California tzv. modrou skřínku, která vydávala různé zvukové frekvence a díky tomu umožnila volání zdarma. Těmito členy klubu byli Steve Jobs a Steve Wozniak, kteří v roce 1977 založili společnost Apple Computers.[86] Jeden z prvních případů, kdy FBI oficiálně vyšetřovala a následně zatkla pachatele hackerství, se stal v roce 1983. Skupina mladistvých hackerů ze státu Milwaukee, která se přezdívala „414 s“, byla usvědčena z proniknutí do více než 60 počítačových sítí a následně za tyto činy odsouzena k podmíněnému trestu odnětí svobody.[87]

Podle rozdílných motivací, různých způsobů provedení a odlišné oblasti zájmu v rámci počítačové sítě se mezi hackery etablovaly tři základní skupiny – White Hats, Black Hats a Grey Hats.[88]

White Hats se snaží o pronikání do systému za účelem odhalení jeho slabin a následné opravy chyby a zamezení obdobnému průniku. Často se jedná přímo o zaměstnance dané společnosti nebo smluvně najaté externí zaměstnance, kteří „hackují“ daný systém jako prevenci před případným útokem třetích stran.[89] Takové jednání nezpůsobuje jednotlivci ani společnosti žádnou škodu, naopak upozorňuje na případné nedostatky v zabezpečení.[90]

Black Hats jsou přesným opakem White Hats. Dá se říci, že stojí na opačné straně barikády a jsou těmi, před kterými se White Hats snaží daný systém zabezpečit a komu chtějí zamezit v pronikání do systému a následnému cílenému páchání škody nebo snahy získat pro sebe či jiného

---

[84] CHATFIELD, Tom. Digitální svět: 50 myšlenek, které musíte znát. Vyd. 1. [Praha]: Slovart, 2013. 208 s. ISBN 978-80-7391-720-3 s. 96

[85] CHATFIELD, Tom. Digitální svět: 50 myšlenek, které musíte znát. Vyd. 1. [Praha]: Slovart, 2013. 208 s. ISBN 978-80-7391-720-3 s. 97

[86] ČERVENÝ, Ladislav. Historie hackerství [online]. 2003 [cit. 2019-11-11]. Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/2003/xcerveny.htm

[87] ČERVENÝ, Ladislav. Historie hackerství [online]. 2003 [cit. 2019-11-11]. Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/2003/xcerveny.htm

[88] KOLO UCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf, s. 273

[89] POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice. s. 231

[90] MATĚJKA, Michal. Počítačová kriminalita. Praha: Computer Press, 2002. ISBN 80-7226-419-2. s. 54

majetkový prospěch.[91] Mezi Black Hats patří široká škála pachatelů – od amatérů, kteří začínají s rozšiřováním různých typů malwaru až po zkušené hackery, kteří se zaměřují především na krádeže finančních dat, osobních dat a přístupových informací k bankovním účtům.[92]

Poslední ze tří základních skupin hackerů jsou Grey Hats. Už podle názvu je patrné, že stojí někde mezi předešlými dvěma skupinami. Jejich činnost není primárně nelegální a nesnaží se nikomu primárně způsobit újmu, avšak taková činnost jim není přímo zapovězena.[93] Často se snaží o nabourání systémů různých společností, ale oproti White Hats nemají k danému nabourání povolení od poškozeného. Následné odhalení nedostatku v zabezpečení daného systému často ohlásí majiteli a občas požadují malou odměnu za případné opravení daného problému. Pokud jim odměna není poskytnuta, tak často přejdou ke zveřejnění dané chyby na internetu, aby se o ní všichni dozvěděli.[94]

Další skupinou hackerů, která úplně nezapadá do uvedených základních skupin, jsou tzv. rodents, kteří hacking vnímají spíše jako určitou formu hry, resp. je pro ně hacknutí daného systému výzvou, kterou musí pokořit (známou výzvou mezi profesionálními hackery je např. hacknutí Pentagonu). Tzv. swappers se zaměřují na napíchnutí serveru a jeho následné využití k provozování her či výměně informací. Jedněmi z nejnebezpečnějších skupin jsou tzv. carders a trashers, u kterých je hlavním impulzem zištnost. Dalšími motivy jsou často jen snaha dokázát svou intelektuální nadřazenost, touha po adrenalinu, zvědavost či hra.[95]

4.1.2 Cracker

Skupina crackerů by se dala systematicky zařadit k hackerům, ale protože jejich činnost je velmi rozšířená a jistě se s ní téměř každý setkal, je jim zde věnována samostatná kapitola. Pojmy cracking a hacking jsou ve společnosti i ve sdělovacích prostředcích často zaměňovány nebo používány jako synonyma. Z kriminologického hlediska jsou crackeři koexistující subkulturou

---

[91] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 273

[92] What is the Difference Between Black, White and Grey Hat Hackers [online]. [cit. 2019-11-11]. Dostupné z: https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html

[93] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 273

[94] What is the Difference Between Black, White and Grey Hat Hackers [online]. [cit. 2019-11-11]. Dostupné z: https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html

[95] VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3. s.529

hackerů. Často využívají svých schopností a technické vybavenosti k páchání nelegálních skutků a vandalismu, který postrádá smysl.[96]. *Obsahově pojem cracking znamená prolamování nebo obcházení ochranných prvků počítačového systému, programů nebo aplikací, s cílem jejich následného neoprávněného užití.*[97] *Hackeři ze staré školy se zlostí vyvracejí svůj vlastní popis jako, že páchají násilí, sabotáže a že jsou zloději a pro takové z nich používají termín cracker k odlišení škodlivého druhu počítačového nadšence od hackerů samotných.*[98]

Nejčastěji bývají za crackery označováni členové jedné ze tří základních skupin hackerů, a to Black Hats. Je tomu tak především kvůli jejich činnosti spočívající v prolamování systémů za účelem způsobení škody nebo jiné újmy, získání informací nebo v poslední řadě obohacení sebe nebo jiného, což bývá také nejčastějším důvodem. Cracking je ve velké míře i v souvislosti s obohacením sebe či jiného spojen s porušováním autorských práv a s právy souvisejícími. V tomto ohledu ze strany crackerů nejčastěji dochází k obcházení ochranných prvků, které slouží k zabránění vytváření kopií a tím pádem i dalšího nelegálního šíření díla chráněného autorským zákonem.[99] Konkrétně takové jednání nejvíce postihuje herní průmysl, hudební a filmovou produkci a také kompletní softwarové vybavení počítače.[100]

Zajímavý je také pohled, jak crackery a jejich motivace vnímají jednotliví autoři. Například podle Válkové/Kuchty se crackeři specializují především na krádeže, tvoření nelegálních kopií a změny a úpravy programového vybavení.[101] Dle Gřivny/Scheinosta/Zoubkové je primární motivací crackerů dosažení neoprávněného prospěchu, zejména tedy získání dat, informací a přístupu pro vlastní potřebu nebo pro další obchodování.[102]

Činnost crackerů je poměrně široká a více se jí budu věnovat v následující kapitole, která bude zaměřena na jednotlivé projevy kybernetické kriminality.

---

[96] GŘIVNA, Tomáš a Radim POLČÁK. Kyberkriminalita a právo. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4. s. 39

[97] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 276

[98] YAR, Majid. Cybercrime and society. London: SAGE, 2006. ISBN 1-4129-0753-5. Dostupné také z: http://www.loc.gov/catdir/enhancements/fy0659/2005934725-d.html s. 23

[99] Zákon č. 121/2000 Sb. Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)

[100] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 276

[101] VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3. s.529

[102] GŘIVNA, Tomáš, Miroslav SCHEINOST, Ivana ZOUBKOVÁ, et al. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 394

4.1.3 Organizovaná zločinecká skupina

V celosvětovém měřítku není organizovaná kriminalita žádnou novinkou, avšak je nutné zmínit, že se jedná o jeden z nejzávažnějších druhů trestných činů přinášejících obrovské riziko pro stabilitu, bezpečnost a vývoj společnosti.[103] S kybernetickou kriminalitou se často pojí vidina velkého ekonomického prospěchu a je proto logické, že pozornost organizovaných zločineckých skupin se nutně musela zaměřit i na toto relativně nové místo páchání nezákonné činnosti.

Nejprve je potřeba definovat termín organizované kriminality. *Organizovaná kriminalita je soustavná a plánovitá trestná činnost páchaná hierarchicky strukturovanou skupinou osob, mezi nimiž existuje dělba činnosti. Jejím primárním cílem je dosažení vysokého zisku.*[104] Charakteristickými pojmovými znaky určujícími, zda se skutečně jedná o organizovanou kriminalitu a ne pouze o spolčení či srocení, jsou skupinovost, soustavnost, plánovitost, dělba činnosti, hierarchická struktura skupiny a úsilí o maximální zisk. Mezi další znaky, které již nejsou obligatorní, ale spíše fakultativní, patří používání násilí, přijímání ochranných opatření proti odhalení, internacionalizace, moderní infrastruktura a korupce státních orgánů.[105]

Největší nebezpečí organizované kriminality spočívá zejména v její kvalitativní odlišnosti od kriminality běžné. Rozdíl je především v tom, že zatímco u běžné kriminality je hlavním bodem zájmu pachatel a jeho trestný čin, u organizované kriminality jde až o druhotné ukazatele. Organizovanému zločinu je bližší model tzv „průmyslu zločinu“, který se spíše podobá podnikání podle modelu prosperujících podniků, avšak poskytujícímu nezákonné služby a zboží bez respektování společenských norem.[106] Členové organizované zločinecké skupiny využívají počítačů především ke skryté vzájemné komunikaci, k praní nelegálně získaných peněz a výrobě padělků, ať už se jedná o software nebo dokonce o falešné platební karty. Další rozsáhlou činností organizovaných skupin je dětská pornografie.[107] U ní dokonce existuje podezření, že organizované

[103] VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3. s. 479

[104] GŘIVNA, Tomáš, Miroslav SCHEINOST, Ivana ZOUBKOVÁ, et al. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 448

[105] GŘIVNA, Tomáš, Miroslav SCHEINOST, Ivana ZOUBKOVÁ, et al. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 448 a násl.

[106] VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3. s 480

[107] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7. s. 689

skupiny fungující na nadnárodní bázi mohou pomocí kompromitujícího materiálu vydírat vysoce postavené politiky i představitele obchodních společností a tím dosahovat svých cílů.[108]

Na větší míru trestné činnosti v prostředí internetu a činnost páchanou prostřednictvím počítačů organizovanými zločineckými skupinami reagoval Institut pro kriminologii a sociální prevenci ve svém šetření z roku 2017, kde byly podrobněji charakterizovány činnosti, které jsou uváděny pod obecnějším názvem počítačové kriminality. Jednalo se například o skimming a kriminalitu páchanou pomocí malware, ransomware a cryptolockeru. Nebezpečnost organizované kybernetické kriminality podle expertizy z roku 2016, kde byli dotazování příslušníci speciálních útvarů Policie České republiky, je vnímána zejména v legálnosti anonymizačních nástrojů pro internetová připojení a celková anonymita internetového prostředí, závislosti na počítačových systémech (například nedávný útok na nemocnici v Benešově[109]) a celková neregulovatelnost počítačového prostředí. Jako významné doporučení by bylo podle expertizy dobré zlepšit vybavenost IT a navázat kvalitnější spolupráci s IT experty.[110]

Celkové působení organizovaných zločineckých skupin v prostředí internetu je velice nebezpečné a obtížně kontrolovatelné především kvůli rychlosti komunikace, celkové anonymitě a případným následkům jednotlivých útoků. Takovéto skupiny mohou využívat specifická místa na internetu, například „dark web“, na němž je nelegální činnost na denním pořádku. Dochází zde zejména k prodeji drog, zbraní a lze zde získat nelegální pornografii. Velkým nebezpečím v rámci organizovaného zločinu jsou teroristické organizace, jejichž buňky využívají prostředí internetu ke zdánlivě anonymní komunikaci, která je navíc velice rychlá a těžko vystopovatelná. Neméně nebezpečnými jsou jednotlivé útoky prováděné organizovanými zločineckými skupinami – zde jim opět internet samotný nabízí velký prostor k páchání trestné činnosti s mnohem větším dosahem, než by byli schopni dosáhnout jinými prostředky. Velkým nebezpečím dnešní doby jsou teroristické útoky na jednotlivé klíčové instituce jako jsou například nemocnice, dopravní infrastrukturu, vládní instituce a případně obranné systémy.

---

[108] https://video.aktualne.cz/dvtv/matka-ji-prodala-pedofilum-znasilnily-me-stovky-muzu-hlavou/r~70ac19fef90e11e982ef0cc47ab5f122

[109] https://www.idnes.cz/praha/zpravy/kryptovirus-nemocnice-benesov.A191211_073802_praha-zpravy_alh?

[110] SCHEINOST, Miroslav, Martin CEJP, Petr POJMAN a Tomáš DIVIÁK. Trendy vývoje organizovaného zločinu a jeho vybraných forem. Praha: IKSP, 2018. ISBN 978-80-7338-171-4. s. 28 a s. 43

4.2 Oběť a její viktimizace

4.2.1 Oběť v obecné rovině

Z hlediska trestního práva je důležité zkoumat nejen pachatele trestné činností, ale také jejich oběti, tj. osoby, kterých se trestná činnost bezprostředně dotýká, poškozuje je nebo je ohrožuje na životě, zdraví, majetku, cti, svobodě nebo jiných podstatných právech. Samostatný vědecký podobor kriminologie, který se oběťmi přímo zabývá, se nazývá viktimologie. Pojem oběť je přímo upraven v zákoně o obětech trestných činů[111], a to následovně:

(2) Obětí se rozumí fyzická osoba, které bylo nebo mělo být trestným činem ublíženo na zdraví, způsobena majetková nebo nemajetková újma nebo na jejíž úkor se pachatel trestným činem obohatil.

(3) Byla-li trestným činem způsobena smrt oběti, považují se, utrpěli-li v důsledku smrti oběti újmu, za oběť též její příbuzný v pokolení přímém, sourozenec, osvojenec, osvojitel, manžel nebo registrovaný partner, druh nebo osoba, které oběť ke dni své smrti poskytovala nebo byla povinna poskytovat výživu. Je-li těchto osob více, považuje se za oběť každá z nich.[112]

Z tohoto zákonného ustanovení můžeme dojít k závěru, že obětí trestného činu nemůže být kolektivní subjekt, například právnická osoba. Pro účely zkoumání viktimizace z hlediska kybernetické kriminality budu však počítat i s kriminalitou spáchanou proti právnickým osobám. V tomto případě by se o právnické osobě dalo mluvit spíše nežli jako o oběti jako o poškozeném, což je trestně procesní institut zakotven v zákoně č. 141/1961, trestní řád, a dále upraven následovně:

(1) Ten, komu bylo trestným činem ublíženo na zdraví, způsobena majetková škoda nebo nemajetková újma, nebo ten, na jehož úkor se pachatel trestným činem obohatil (poškozený), má právo činit návrh na doplnění dokazování, nahlížet do spisů (§ 65), zúčastnit se sjednávání dohody o vině a trestu, zúčastnit se hlavního líčení a veřejného zasedání konaného o odvolání nebo o schválení dohody o vině a trestu a před skončením řízení se k věci vyjádřit. Jde-li o trestný čin zanedbání povinné výživy (§ 196 trestního zákoníku), rozumí se pro účely tohoto zákona majetkovou škodou, jež byla poškozenému způsobena trestným činem, i dlužné výživné.

[111] Zákon č. 45/2013 Sb.
[112] §2 zákona č. 45/2013 Sb., Zákon o obětech trestných činů a o změně některých zákonů

(2) Za poškozeného se nepovažuje ten, kdo se sice cítí být trestným činem morálně nebo jinak poškozen, avšak vzniklá újma není způsobena zaviněním pachatele nebo její vznik není v příčinné souvislosti s trestným činem.[113]

Zákon o obětech trestných činů pracuje ještě s pojmem zvlášť zranitelná oběť, která je blíže specifikována taxativním výčtem uvedeným v § 2 odst. 4 tohoto zákona. Jedná se například o dítě, osobu vysokého věku, hendikepovanou osobu, oběť trestného činu obchodování s lidmi, oběť teroristického útoku nebo oběti trestných činů proti lidské důstojnosti či jiným způsobem zvlášť zranitelné oběti.

Viktimologie je pokládána za součást kriminologie. Její počátky se dají datovat do poloviny 20. století. K jejímu vzniku nejvíce přispěl konec 2. světové války a s tím spojená péče a pomoc jejím obětem, zejména obětem holocaustu a jiných zločinů za války spáchaných. Dalším důvodem věnování pozornosti obětem trestných činů byla snaha o lepší pochopení samotného trestného činu a případné přispění k prevenci kriminality. Díky znalosti oběti a vztahu k pachateli trestnému činu kriminologická teorie lépe poznala skutkové okolnosti a motivy pro páchání trestné činnosti. Viktimologie od počátku usiluje o zlepšení pozice oběti trestného činu, které do té doby orgány činné v trestním řízení spíše přehlížely a nebyla jim státem a ani společností věnována dostatečná péče. Především díky tomu je na oběti v dnešní době brán větší zřetel a je jim poskytována ochrana, šetří se jejich práva, aby nedošlo k sekundární viktimizaci (například ze strany vyšetřujícího orgánu) a je jim poskytována případná pomoc.

Viktimologie zkoumá šest jevů, jimiž jsou:

- osoba oběti a její vlastnosti,
- vztah mezi subjektem trestného činu a obětí,
- role oběti v procesu viktimizace,
- zjišťování trestného činu a jeho dokazování před soudem a role oběti v tomto procesu,
- poskytování pomoci oběti a její následné nároky na odškodnění nebo případné náhrady škody,
- obecná ochrana obyvatelstva před viktimizací.

V posledních letech vykrystalizoval relativně samostatný obor, který se zajímá o oběť jako o zdroj informací o spáchaném trestném činu a objasnění okolností a následnému odhalení pachatele. Tento obor se nazývá kriminalistická viktimologie a zabývá se podrobněji například

[113] §43 zákona č. 141/1961 Sb., Zákon o trestním řízení soudním

výslechem svědků či rolí oběti při samotném oznámení trestného činu.[114] V první polovině 20. století se naprostá většina kriminologických teorií zabývala výhradně osobou pachatele a na oběť pohlížela pouze okrajově. Oběť byla v těchto případech považována za pasivního účastníka zločinu, který byl přinucen nést následky kriminálního chování. Kriminologie se zaměřovala na pachatele a různé vlivy, které jej vedly k páchání kriminality. Velkou změnu v tomto pojetí odstartovala práce Hanse von Hentiga publikovaná v roce 1948 pod názvem „Zločinec a jeho oběť"[115]. Podle této práce je o spáchaném zločinu nutno uvažovat jako o *vzájemné a dynamické interakci mezi pachatelem a obětí.* Přičemž na celý trestný čin je třeba nahlížet empirickým pohledem, tudíž vnímat skutečnost, že mnohé obětí mají svým přičiněním podíl na tom, že si pachatel vybrat zrovna je. Ať už tím, že pachatele k samotné trestné činnosti vyprovokovali či mu ji umožnili svým lehkomyslným či neopatrným počínáním. Autor je dokonce přesvědčen, že některá část obyvatelstva má větší dispozice stát se obětí trestného činu než zbytek populace.[116] Teorie pro tuto náchylnost stát se obětí trestného činu používá pojem viktimnost, která značí disponovanost stát se obětí trestného činu, ať už jde o jedince či o celou skupinu osob.

Nejvýznamnějšími vlastnostmi společnými pro větší skupinu osob z hlediska jejich viktimnosti jsou:

- zaměstnání/profese oběti – nejohroženější skupinou jsou ozbrojené složky, ale také lidé pracující na místech, která jsou náchylná pro majetkovou trestnou činnost – například banky, obchody nebo benzínové pumpy,
- věk oběti - mladší lidí jsou zpravidla více aktivní a tím se častěji ocitnou v nebezpečné situaci,
- psychické vlastnosti - agresivní člověk se snáze dostane do konfliktu a následně se i svým přičiněním stane obětí násilné trestné činnosti,
- příslušnost minoritě – národnostní, etnické, rasové, náboženské, s odlišnou sexuální orientací.

Významným pojmy pro teorii je také viktimizace, která označuje proces, během kterého se z potenciální oběti stává oběť faktická. Pro tento proces je stěžejní počínání pachatele. Neméně

---

[114] GŘIVNA, Tomáš, Miroslav SCHEINOST, Ivana ZOUBKOVÁ, et al. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 120 a násl.

[115] von HENTIG, Hans. The Criminal and His Victim. Studies in the Sociobiology of Crime: Yale University Press, New Haven 1948.

[116] TOMÁŠEK, Jan. Úvod do kriminologie. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-746-7. s. 146

důležitým pojmem je index viktimizace, který se zaměřuje na kvantitativní ukazatele počtu obětí a nabízí statistiky na národní i mezinárodní úrovni a jejich postupný vývoj v čase.[117]

4.2.2 Oběť kybernetické kriminality

Rozmach v oblasti informačních technologií vedl k rozsáhlé viktimizaci. Uživateli prostředí IT jsou především jednotlivci a společnosti. Společnosti jsou na rozdíl od jednotlivců běžně vybaveny aparátem (síťoví administrátoři atp.), který se stará o údržbu a ochranu počítačových a síťových systémů. Nejčastějšími oběťmi v kyberprostoru jsou podle dat zveřejněných Europolem obchodní společnosti následované státem a jeho organizační strukturou. Až jako třetí v pořadí je jednotlivec jako soukromá osoba. Z uveřejněných dat vyplývá, že pro trestnou činnost nejnáchylnější je hospodářský sektor. Důvod, proč tomu tak je, však není jen čistě ekonomický, ale je též důsledkem střetu dvou rozdílných kultur, kde na jedné straně stojí hackeři, kteří jsou v epicentru rozmachu internetu, a na straně druhé oběti, které se snaží maximalizovat vlastní zisk využíváním kyberprostoru.

Významným znakem trestné činnosti v oblasti kyberprostoru je, že jen malé množství útoků bývá skutečně odhaleno. Je to způsobeno především tím, že oběť vůbec nemusí zjistit, že se stala cílem útočníka. Často bývá využito jen zařízení oběti bez jejího vědomí. Není výjimkou, že k samotnému útoku dojde až s časovým odstupem od instalace škodlivého software do zařízení postiženého a útok probíhá z jiného místa. Odhalit takový útok bývá pro běžného uživatele počítačového zařízení velice obtížné a je požadována technická znalost informačních technologií.[118]

Dalším důvodem, kvůli kterému je obtížné mít přesná data a představu o počtu a závažnosti trestných činů je, že ne všechna trestná činnost je oznámena orgánům činným v trestním řízení. Například podle výzkumu z roku 2016 provedeného společností Barcleys a společností IoD bylo jen 28 % útoků v kyberprostoru uskutečněných proti společnostem oznámeno příslušným orgánům. Ještě tristnější statistiku zveřejnila v roce 2018 FBI. Podle ní pouze 15 % obětí oznámí policii, že se stali obětí kybernetického útoku. Zarážející je, že pokud jde o fyzické útoky, tak

[117] GŘIVNA, Tomáš, Miroslav SCHEINOST, Ivana ZOUBKOVÁ, et al. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 123 a násl.
[118] GŘIVNA, Tomáš a Radim POLČÁK. Kyberkriminalita a právo. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4. s. 35

první, co oběť udělá, je, že incident nahlásí policii, avšak v případě kybernetického útoku bývá policie často jako poslední instance, na kterou se oběť obrátí.[119]

Výše v textu bylo již zmíněno, že nejčastějšími cíli pro kybernetický útok bývají státní instituce nebo obchodní společnosti, a to především v oblasti bankovnictví a pojišťovnictví. Podle výzkumu z roku 2005, který provedla společnost Delloite, až 35 % útoků bývá provedeno zaměstnanci napadené společnosti. Výzkum dále ukázal, že až 98 % společností používá antivirový program a více než tři čtvrtiny společností používají privátní sítě, do kterých je přístup zvenčí velice obtížný.[120] Takovéto statistiky týkající se počtu útoků na obchodní společnosti bývají často zabarvené faktem, že často nemají zájem oznámit, že se staly obětí kybernetického útoku, aby veřejnosti neukázaly svoji zranitelnost a vlastní pochybení. Takovéto pochybení by mohlo mít za následek nedůvěru ze strany klientů a jejich následnou ztrátu pro společnost. Sekundární viktimizace způsobená oznámením trestného činu by pak mohla být mnohem horší než viktimizace primární.

Z hlediska sociálního pozitivismu je pachatel do jisté míry obětí prostředí, ve kterém se pohybuje. Tomu nasvědčuje také fakt, že útoky v kyberprostoru jsou ve dvou ze tří případů páchány převážně ze zvědavosti. Další důvody jsou spatřovány v tom, že kyberprostor je považován za příznivé prostředí pro páchání trestné činnosti. Tomu velice nahrává, že v kyberprostoru často bývá tenká hranice mezi legálním a nelegálním počínáním. Často se také stává, že z oběti se následně stane pachatel – typicky se to stává při tzv. spammingu, kdy prvotně infikované zařízení dále funguje jako odesílatel dalšího spamu.

Významným důvodem pro vysokou viktimizaci v prostředí kyberprostoru je také samotná povaha prostředí, ve kterém se pachatel i oběť pohybují. Anonymita a určitá nereálnost prostředí, ve kterém se oba subjekty pohybují, může pokřivit uvažování obou subjektů a vést k chování odlišnému, než je běžné ve vnějším světě.[121]

---

[119] [online]. [cit. 2020-04-28]. Dostupné z: https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html

[120] [online]. [cit. 2020-04-28]. Dostupné z: https://www.finextra.com/newsarticle/13864/banks-told-to-beware-enemy-within

[121] GŘIVNA, Tomáš a Radim POLČÁK. Kyberkriminalita a právo. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4. s. 37

5 Jednotlivé útoky v kyberprostoru

Cílem kapitoly je poskytnout ucelený pohled na kybernetickou kriminalitu. Pokusím se popsat veškeré možné protiprávní jednání v oblasti kyberprostoru a blíže popsat a pojmenovat, v čem takové jednání spočívá a případně o jakou trestně právní kvalifikaci se jedná z pohledu trestního práva hmotného. Mnoho pojmů popisujících jednotlivé praktiky kybernetické kriminality pochází z anglického jazyka, tudíž pro běžného uživatele může být většina aktivit abstraktních.

Pro přehlednost lze protiprávní jednání řadit do několika skupin vykazujících společné rysy, ať už jde o předmět útoku nebo o způsob jednání. Jedna taková taxonomie byla vytvořena Centrem excelence pro kyberkriminalitu (C4e) pod vedením agentury ENISA[122] a EC3[123]. V rámci tohoto dělení je definováno osm skupin, pod které jsou následně přiřazeny jednotlivé skutkové podstaty. Těmito skupinami jsou: sběr informací, škodlivý kód, dostupnost, pokus o průnik, průnik, informační bezpečnost, podvod a škodlivý obsah.[124]

Další možnou klasifikaci trestných činů souvisejících s počítači přinesla na mezinárodní úrovni OSN, resp. Úřad pro drogy a kriminalitu. Ten klasifikuje počítačovou trestnou činnost následovně:

1. *Činy proti počítačovým systémům*
    a. *Protiprávní přístup k počítačovému systému*
    b. *Protiprávní zasahování do počítačového systému nebo počítačových dat*
        i. *Protiprávní zasahování do počítačového systému*
        ii. *Protiprávní zasahování do počítačových dat*
    c. *Protiprávní zachycování počítačových dat nebo nezákonný přístup k těmto datům*
    d. *Jiné činy proti počítačovým systémům*[125]

Završnik pro účely své monografie použil dělení vycházející z Budapešťské úmluvy o počítačové kriminalitě z roku 2001 a trochu šířeji stanovil tři skupiny následovně:

[122] Evropská agentura pro bezpečnost sítí a informací. Viz www.enisa.europa.eu
[123] Evropské centrum pro kyberkriminalitu – spadající pod Europol
[124] POLČÁK, Radim. Právo informačních technologií. Praha: Wolters Kluwer, 2018. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-045-8. s. 558 - 566
[125] Mezinárodní klasifikace trestných činů pro statistické účely [online]. [cit. 2020-07-30]. Dostupné z: http://www.ok.cz/iksp/docs/442.pdf

a) *kriminalita spojená s integritou informačního systému a dat, respektive kyberkriminalita v užším slova smyslu: IKT*[126] *jsou terčem útoku v podobě ohrožení důvěrnosti počítačových dat nebo informačního systému či jejich integrity nebo přístupnosti;*

b) *kriminalita spojená s obsahem: (a) sexuální obsah (dětská a „extrémní" pornografie), (b) násilný obsah (kybernetické obtěžování a nenávistný projev) a (c) porušení práv duševního vlastnictví;*

c) *kriminalita spojená s počítači: IKT je nástrojem pro páchání tradiční (zpravidla majetkové) kriminality*.[127]

Na úrovni Rady Evropy byla Komisí expertů pro zločin v kyberprostoru v roce 2000 vytvořena poměrně jednoduchá klasifikace této trestné činnosti. Toto dělení se nesnaží o zahrnutí veškeré trestné činnosti v kyberprostoru konkrétně, ale spíše se zabývá obecným popisem, jak k trestné činnosti může docházet a zda se jedná o již známé kriminální chování či o jednání dosud neznámé. Konkrétně se dělí kyberzločin do dvou skupin:

1. *Dle pozice počítače při páchání trestné činnosti:*
   - *cíl (terč) útoku;*
   - *prostředek (nástroj) útoku.*
2. *Podle typy činu:*
   - *protiprávní jednání tradiční (např. padělání bankovek aj.)*
   - *protiprávní jednání nová (např. phishing, DDoS aj.)*[128]

Smejkal ve své nejnovější publikaci rozlišuje s ohledem na zvláštní část trestního práva hmotného 6 skupin trestné činnosti:

1. Sabotáže a útoky na zařízení ICT
2. ICT zařízení jako nástroje pro páchání trestné činnosti
3. Trestná činnost spojená se získáváním a šířením informací
4. Ochrana duševního vlastnictví v prostředí ICT
5. Ryze počítačové trestné činy
6. Ostatní trestné činy související s počítači

---

[126] Informační a komunikační technologie

[127] ZAVRŠNIK, Aleš. Kyberkriminalita. Přeložil David BLAŽEK. Praha: Wolters Kluwer, 2017. Právní monografie. ISBN 978-80-7552-758-5. s. 16

[128] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 38

Nejčastěji používaná je klasifikace podle Budapešťské úmluvy o kybernetické kriminalitě. Přejímají ji současné učebnice[129] a v lehce upravené podobě je použita i v této práci.

5.1 Útoky proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů

Pro tuto skupinu protiprávního jednání je příznačné páchání trestné činnosti pomocí škodlivého softwaru nebo manipulace uživatelem s cílem získat informace či provést určitou aktivitu.

Určující pro tuto skupinu je způsob nakládání s daty. Data lze odcizit, což způsobí narušení důvěrnosti, pozměnit, což naruší princip celistvosti (integrity) nebo zablokovat, což znemožní uživateli data používat.[130]

5.1.1 Sociální inženýrství

Ve své podstatě využívání sociálního inženýrství není přímo kybernetický útok, avšak je nutným prostředkem k jeho následnému provedení.

Hlavní motivací útočníka pro využití technik sociálního inženýrství k dosažení svého cíle je obecně známá poučka, že při prolamování jakéhokoliv zabezpečení je nejlepší útočit na jeho nejslabší článek. V případě technologií tím nejslabším článkem byl a vždy bude člověk, jehož činnost je vždy nutná pro fungování počítačového systému.

Sociální inženýrství by se dalo definovat jako snaha o ovlivňování, přesvědčování či manipulaci s obětí se záměrem získat určité informace nebo donutit ji k určité akci. Informace samotné jsou klíčovým elementem této techniky, kdy je potřeba o předmětu útoku získat co největší množství údajů. Často jde o dlouhodobou činnost, při které je nejdříve potřeba vybudovat důvěru mezi útočníkem a obětí. Takovéto praktiky mohou být efektivní především díky lidské neopatrnosti, snaze důvěřovat ostatním, hlouposti, snaze pomáhat, strachu a slabosti, které vytvářejí skvělé podmínky pro realizaci sociálního inženýrství.

Zpravidla se v rámci sociálního inženýrství používají tři způsoby útoku, příp. jejich kombinace:

1) sběr veřejně dostupných dat o předmětu útoku,

---

[129] Například učebnice kriminologie (*Kriminologie. 5., aktualizované vydání*)

[130] SCHNEIER, Bruce. The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters [online]. [cit. 2020-08-02]. Dostupné z: https://www.vice.com/en_us/article/qkjzwp/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster

2) tzv. fyzický útok spočívající v osobním kontaktu, např. při servisu atp.,
3) psychologický útok.

Mezi nejběžněji používané metody útoků pomocí sociálního inženýrství patří podvodné emaily, falešné webové stránky, útoky pomocí telefonních hovorů, sbírání informací z odpadků, vyzkoušení služby zdarma, nabídka paměťového nosiče zdarma, sběr veřejně dostupných informací ze sociálních sítí, reklamní materiály na CD, DVD a jiné.[131]

Známým případem využití technik sociálního inženýrství je kauza týkající se Američana Kevina Mitnicka, v dnešní době již autora a bezpečnostního konzultanta. Mitnick sám sebe považuje spíše za socio-technika, i když širokou veřejností byl dlouho považován za hackera. Za svoje činy byl odsouzen a strávil 5 let ve vězení. Následně mu bylo soudním opatřením zakázáno používat jakékoliv komunikační technologie. Po propuštění napsal několik knih, v nichž popsal své techniky vlamování do informačních systémů a stal se počítačovým konzultantem.[132]

5.1.2 Botnet

Botnetem se dá označit síť zneužívaných zařízení (v dnešní době se již nejedná jen o počítače, ale také například mobilní telefony, SMART televize aj.), která provádějí určitou akci podmíněnou příkazem správce této sítě. Botnet funguje na základě svého cíleného rozšíření po co největším množství zařízení například prostřednictvím nevyžádané pošty.[133] Při úspěšném zasažení zařízení se toto zařízení připojí do sítě jako tzv. bot, kterou řídí útočník pomocí C&C[134] serveru. Bot je ve své podstatě software, který se na infikované zařízení sám nainstaluje a často skrytě očím vlastníka tohoto zařízení v pozadí pracuje.[135]

Botnety nejsou využívány pouze pro účely nelegální. Původní myšlenka byla využít botnety ke složitým výpočtům, na které často nestačí ani superpočítače. Využití tisíců počítačů po celém světě je značně efektivnější a výsledky těchto výpočtů často umožňují vědecký pokrok. Princip je ten, že většina počítačů nevyužívá zcela svůj potenciál a často například při sledování filmu či psaní v textovém editoru funguje výpočetní potenciál na jednotky maximálně desítky procent

[131] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 186-188
[132] Kevin Mitnick [online]. [cit. 2020-08-03]. Dostupné z: https://en.wikipedia.org/wiki/Kevin_Mitnick
[133] BOTNET [online]. [cit. 2020-08-03]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/botnet/
[134] Command and control infrastructure – celek skládající se řídícího prvků a všech botů
[135] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 193-194

skutečného výkonu. Při efektivním využití tohoto potenciálu může být v kratším čase dokončeno mnoho, i pro nejmodernější superpočítače složitých, výpočetních operací.[136]

Podle struktury můžeme rozlišit dva typy botnetu:

1) s centralizovanou architekturou, ve které bot komunikuje přímo s C&C serverem,
2) s decentralizovanou architekturou, která funguje na principu P2P[137] a příkazy jsou mezi jednotlivými klienty sdíleny.

Botnety jsou často využívány jako prostředek k páchání další trestné činnosti. Dají se zařadit do kategorie crime-as-a-service, kde síť botnetů slouží k rozesílání spamu, phishingu, DDoS útokům etc. V roce 2014 se dokonce podařilo zaznamenat případ, že součástí takové sítě byla lednice, která odeslala více než 750 000 emailů.

Z hlediska klasifikace podle trestního práva hmotného se vlastník takové sítě botnetu dopouští trestného činu „neoprávněný přístup k počítačovému systému a nosiči informací“ podle § 230 TZ, kdy pachateli při splnění základní skutkové podstaty hrozí až dva roky odnětí svobody a případnému propadnutí věci.[138]

5.1.3 Malware

Výraz malware vznikl spojením anglických slov „malicious software“, které v překladu znamenají škodlivý software. Tento pojem označuje jakýkoliv škodlivý program nebo kód, který může systému způsobit škody. Takovýto nepřátelský software se snaží napadnout, poškodit nebo vyřadit z provozu počítače a počítačové systémy zejména tím, že nad nimi převezme kontrolu. Škodlivý software se může dál sám od sebe šířit, ale zároveň může také získávat další data z infikovaných sítí.[139] Určitou definici malwaru vytvořil Smejkal ve své publikaci, kdy malwarem označil programy, jejichž cílem je někomu nějak škodit. Jako malware lze označit téměř každý program, který umožní neoprávněný přístup k systému či jehož cílem je způsobení škody. Nepatří sem programy, které způsobí případnou škodu kvůli chybě, ale jejich účel je legální a s legitimními cíli.[140]

---

[136] Distribuované výpočty [online]. [cit. 2020-08-03]. Dostupné z: https://dc.czechnationalteam.cz/index.html

[137] Peer-to-peer – označení pro komunikaci přímo dvou klientů v rámci počítačové sítě. Jedná se o opak komunikace klienta přímo se serverem.

[138] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 194-196

[139] Malware [online]. [cit. 2020-08-05]. Dostupné z: https://www.malwarebytes.com/malware/

[140] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 191

Nejčastější způsob, jakým se dostane malware do počítače, bývá samotná instalace uživatelem prostřednictvím kliknutí na odkaz například v emailu nebo na internetové stránce. Dále bývá nechtěný software součástí klasického instalačního programu neškodlivého software a běžný uživatel si ani není schopen všimnout, že vedle požadovaného programu nainstaloval do počítače i malware. Mezi nejznámější typy malware patří:

1) adware
2) spyware
3) viry
4) červi
5) trojský kůň
6) backdoor
7) rootkity
8) keylogger
9) ransomware aj.[141]

5.1.3.1 **Adware**

Jako mnoho pojmů kybernetické kriminality i adware má svůj prapůvod v anglickém jazyce, a to konkrétně ze slovního spojení „advertising supported software“, což by se dalo volně přeložit jako software podporující reklamu. Tvůrci takového malware do něj zakomponují reklamu, anebo pomáhají s distribucí softwaru za účelem výdělku. Většina adwaru je bezpečná, ale jsou i případy, kde je adware spojen se spyware. Od třetích stran dostávají tvůrci adwaru odměnu podle třech různých klíčů – za otevření reklamy na cílový produkt, za zobrazení reklamy nebo za každou instalaci předmětného software do zařízení. Většina lidí bude znát adware jako nekonečně vyskakující reklamy na internetu, které se velice často vážou na stránky porušující právo duševního vlastnictví, například nelegální distribucí filmových kopií.[142]

[141] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 205

[142] What is Adware: What You Should Know and How to Protect Yourself [online]. [cit. 2020-08-05]. Dostupné z: https://www.kaspersky.com/resource-center/threats/adware

5.1.3.2 **Spyware**

Název je odvozen ze spojení anglického „spy“ (špion) a „ware“ (ze slova software). Cílem tohoto škodlivého programu je být co nejdéle utajen před uživatelem a získat co nejpřívětivější prostředí pro účel svojí existence, čímž je sledování činnosti uživatele a zaznamenávání a následné odesílání uložených souborů. Útočníkovi odesílanými údaji mohou být například osobní data, hesla a přístupy do internetového bankovnictví, informace o navštívených webových stránkách či veškeré činnosti na napadeném zařízení.[143]

Mezi velice časté způsoby, jak se cílové zařízení infikuje, je instalace společně s jiným software, jehož fungovaní se spyware vůbec nesouvisí (například počítačové hry, aplikace). Spyware stále zůstává nainstalován i při odinstalování původního chtěného programu.[144]

5.1.3.3 **Viry**

V minulém století se jednalo o dominantní formu malwaru. Virus je program, který se množí ve chvíli spuštění určeného software nebo jinak infikovaného souboru. Po aktivaci se může vázat také na běh času a šířit se prostřednictvím sítě nebo na jednotlivých paměťových mediích. Záměr je široký, od získávání dat ze systému přes využití několika zařízení pro cílený útok až k samotnému zničení infikovaného zařízení. Typické pro viry je jejich schopnost se dále šířit bez přičinění uživatele (velice podobně jako viry v lidském těle). Podle cíle útoku se rozlišují viry systémové (tzv. boot viry), souborové, multiparitní (napadají obě předešlé skupiny bez rozdílu) a makro viry (jejíž cílem jsou aplikace).

5.1.3.4 **Červi**

Hlavním rozdílem mezi viry a červy je jejich spojitost s dalším software. Červi na rozdíl od virů nepotřebují pro svou počáteční aktivaci další software, ke kterému by byly připojeny, a většinou se šíří samostatně. Následně se dokážou samy dále šířit rozesíláním své kopie po počítačové síti.[145] Původní myšlenka pro vytvoření červa byla prospěšná. Červ byl vytvořen, aby

---

[143] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 395

[144] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník Kybernetické bezpečnosti [online]. [cit. 2020-08-05]. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf s. 97

[145] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 208

sledoval vytíženost procesorů, které byly připojeny k síti a v případě, že nebyl jejich potenciál dostatečně využit, tak měl za úkol přidělit jim další práci. Později byli dokonce červi využiti pro odstraňování malware z infikovaných počítačů. Historicky „nejúspěšnějším“ červem byl v roce 2000 červ zvaný I LOVE YOU, který měnil systémové soubory a upravoval registry. Podle odhadů způsobil po celém světě škody větší než 5 mld USD.[146]

5.1.3.5 **Trojský kůň a backdoors**

Trojský kůň je výraz převzatý z řecké mytologie především díky způsobu, jakým funguje ve světě ICT. Často se tento škodlivý software prezentuje jako určitý program (často dokonce jako antivirový program), ale skutečným účelem tohoto programu je cílové zařízení infikovat a vytvořit přístup pro útočníka. Na rozdíl od virů se sám od sebe dál nešíří a zůstává pouze na infikovaném zařízení. Pomocí trojského koně dokáže útočník přes vzdálený přístup vykonávat mnoho činností, například volně nakládat se soubory, sledovat stisknuté klávesy, instalovat další programy, využívat výkon daného zařízení nebo dokonce libovolně zapínat webovou kameru.[147]

Existují i trojští koně, kteří jsou schopni bez jakékoliv iniciativy uživatele otevřít komunikační porty počítače. Takovéto porty následně slouží pro další napadení počítače dalším škodlivým software či pro vzdálený přístup. Takový trojský kůň se s ohledem na svojí funkci nazývá „backdoor“ z anglického slova „zadní vrata“.[148]

5.1.3.6 **Rootkity**

Podle definice je rootkit soubor několika aktivit, které slouží pro zahalení činností prováděných na operačním systému. Výraz „rootkit“ pochází z označení administrátora v operačním systému UNIX[149] a jeho funkce je dost podobná variantě trojského koně backdoor s tím rozdílem, že i po konfrontaci napadeného účtu by měl zůstat neodhalen. První rootkity byly vytvořeny k vymazání podezřelých aktivit, tzv. logů. Mezi nechvalně známé případy patří pokus společnosti SONY o zastavení pořizování nelegálních kopií obsahů jejich paměťových medií.

---

[146] Počítačový červ [online]. [cit. 2020-08-05]. Dostupné z: https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_%C4%8Derv

[147] KLIMEK, Libor, Jozef ZÁHORA a Květoň HOLCR. Počítačová kriminalita: v európskych súvislostiach. Bratislava: Wolters Kluwer, 2016. ISBN 978-80-8168-538-5. s. 44

[148] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 209

[149] Operační systém, který vznikl v roce 1969.

Společnost k tomu použila program zvaný XCP, který se po vložení do cílového zařízení sám bez vědomí uživatele nainstaloval. XCP následně znemožnil přístup jakýmkoliv jiným programům k disku a tím znemožnil případné porušování autorských práv. Na tento rootkit na mediích od společnosti SONY upozornil hacker Mark Russinovich a SONY musela po stížnostech a nelibosti veřejnosti všechna média obsahující rootkit stáhnout a vyměnit za média bez tohoto programu.[150]

Podle cíle útoku se rozličšují dva typy rootkitů, systémové a aplikační. Mezi jejich oblíbené cíle patří antivirové programy, které následně nejsou schopny tento škodlivý software odstranit.[151]

5.1.3.7 **Keylogger**

Keyloggery mohou být softwarové nebo hardwarové. Pomocí těchto nástrojů je útočník schopen zaznamenat úhozy uživatele na klávesnici a díky tomu následně získat přístup k různým účtům – ať už se jedná o sociální sítě nebo internetové bankovnictví.

V případě hardwarového keyloggeru je nutný fyzický přístup k napadenému počítači. Jedná se o zařízení, které je vloženo mezi klávesnici a počítač. V případě používání bezdrátové klávesnice existují tzv. sniffety, které jsou schopny zachytit data, která proudí mezí klávesnicí a přijímačem, který je v počítači a tato data odesílat útočníkovi. V tomto případě není nutný až tak blízky fyzický kontakt s napadeným PC.

Softwarový keylogger může mít uživatel v počítači dobrovolně (například sledovaní potomků na internetu) nebo, jak je tomu většinou, je naistalován bez vědomí uživatele, a pak je velice těžko odhalitelný. Běžný uživatel se může bránit pouze vhodným antivirovým programem a sledováním změn v rychlosti počítače.[152]

5.1.3.8 **Ransomware**

Jedná se o speciální druh malware, jehož cílem je zašifrování souborů a následné vydírání vlastníka těchto souborů. Ransomware se šíří především za pomocí červů či trojského koně, které po infikaci zařízení stáhnou tento škodlivý software.

---

[150] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2. s. 65

[151] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 209

[152] Keylogger (Keystroke logger) [online]. [cit. 2020-08-06]. Dostupné z: https://www.digitalnipevnost.cz/viki/keylogger-keystroke-logger

Obecně jsou známy dva typy ransomware, které odlišujeme podle rozsahu útoku. První typ útočí spíše na počítačový systém jako celek a znemožní jeho další použití například zabráněním načtení operačního systému nebo zamčením systémové obrazovky. Tento druh útoku nejspíš v nedávné době postihl nemocnici v Benešově.[153] Ve druhém případě jsou cílem útoku jen určitá data uživatele, která zůstanou uzamčena. Tento typ útoku je v dnešní době oblíbenější, a je to pouze několik dní, kdy americká společnost Garmin nejspíš zaplatila po takovém útoku na své servery výkupné.[154] Přesněji se tento malware nazývá crypto-ransomware a většinou cílí na textové dokumenty, obrázky, videa atd., která zašifruje a uživateli se zobrazí pouze okno s číslem účtu a částkou nutnou k zaplacení, aby byla data znovu přístupná. Často je k odeslání peněz také stanoven časový limit.

Mezi známé případy i v naší zemi se řadí tzv. policejní ransomware, který požadoval zaplacení částky za porušování autorských či jiných práv a následně by byla věc vyřešena bez dalších postihů. Tento ransomware fungoval jako vyskakující okno, které se na displeji zobrazovalo vždy navrchu a nešlo zavřít. Zajímavým zjištěním bylo, že dost lidí tomuto malware uvěřilo a požadovanou částku za zpřístupnění zaplatilo, čemuž nejspíš přispěla obava z autority policejního orgánu a dalších případných postihů při nezaplacení, kterou útočníci použili záměrně jako techniku sociálního inženýrství.

Z hlediska trestní odpovědnosti za takové jednání dle hmotné trestní právní úpravy v České republice na takové případy dopadá primárně § 230 TZ a při pouhém uchování škodlivého software může takovému jednání odpovídat § 231 TZ.[155]

5.1.4 Phishing a pharming

Jedná se o kombinaci klasického podvodného jednání známého z reálného světa s výhodami specifického prostředí kyberprostoru. Někdy se můžeme setkat s českým označením rhybaření. Podstata phishingu spočívá v podvodném jednání, které směřuje k získání citlivých informací

[153] Více viz: https://www.irozhlas.cz/zpravy-domov/nemocnice-benesov-kyberneticky-utok-ransomware-vykupne-ochrana-osobnich-udaju_2001140615_cha

[154] Více viz: https://www.msn.com/cs-cz/zpravy/v%C4%9Bda-a-technika/zd%C3%A1-se-%C5%BEe-garmin-vyd%C4%9Bra%C4%8D%C5%AFm-zaplatil-syst%C3%A9my-napaden%C3%A9-ransomwarem-obnovil-de%C5%A1ifrovac%C3%ADm-k%C3%B3dem-aktualizov%C3%A1no/ar-BB178hKu?li=BBOoZca

[155] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 221-231

nebo přihlašovacích údajů k platebním kartám. Často jsou k takovému jednání využívány emaily a na poškozeného se snaží působit, že je něco nutné učinit.[156]

Zpravidla se útočník vydává za důvěryhodnou osobu nebo dokonce společnost a na první pohled působí velice věrohodně. Využívá k tomu například podobné emailové adresy, kterými disponuje skutečná společnost, nebo uvádí v emailu loga této společnosti. Často se útočníci inspirují originálními prvky, které pravá organizace využívá.[157] V takovémto emailu je často uveden odkaz, na který má uživatel kliknout. Tento odkaz přesměruje na podvodnou internetovou stránku, která je na první pohled téměř shodná s originálem. Následně zadané platební (přístupové) údaje jsou následně odeslány útočníkovi.

Útok se dá rozdělit do několika fází:

1. Plánování
2. Příprava zázemí pro útok
3. Útok
4. Sběr informací
5. Zisk z phishingového útoku[158]

Klasickému phishingu odpovídá nejlépe § 209 TZ, který postihuje podvodné jednání. Takové jednání je dokonáno obohacením se. Podle § 209, odst. 6 je příprava trestná a v tom případě i vytvoření takové podvodné stránky a následné získání přihlašovacích údajů je možné posuzovat podle tohoto ustanovení trestního zákoníku. V případě použití malware k získání takovýchto údajů již takové konání posuzujeme i podle § 230 TZ. Co se týká zvláštního paragrafu pro trestnou činnost související s platebními prostředky (§ 234 TZ), je možný dle povahy útoku také souběh s tímto paragrafem. V určitých případech by se mohl pachatel dopustit také jednání podle § 181 poškození cizích práv, kdyby získané přihlašovací údaje nepoužil ke způsobení majetkové škody, ale ke způsobení škody na nemajetkových právech.

Tzv. pharming je jednání velice podobné phishingu, má však dokonalejší a pro uživatele obtížněji zjistitelnou formu. Při útoku dojde k napadení serveru DNS, který převádí adresu serveru na číselnou podobu, a přepsání IP adresy útočníkem na IP adresu falešných stránek, ke kterým se

---

[156] A Guide To Phishing & Ransomware Terminology [online]. [cit. 2020-08-06]. Dostupné z: https://www.ses-escrow.co.uk/blog/guide-phishing-ransomware-terminology

[157] KLIMEK, Libor, Jozef ZÁHORA a Květoň HOLCR. Počítačová kriminalita: v európskych súvislostiach. Bratislava: Wolters Kluwer, 2016. ISBN 978-80-8168-538-5. s. 46

[158] WILSON, Tracy. How Phishing Works [online]. [cit. 2020-08-06]. Dostupné z: https://computer.howstuffworks.com/phishing.htm

uživatel následně připojí. Uživatel si není vědom, že je na jiné stránce, než která je zadaná v okénku prohlížeče, čemuž napomáhá také téměř totožný vzhled falešných stránek, na které uživatele DNS server převede. Aby takové jednání bylo možné, je pachatel nucen uživateli nastavit falešný DNS server (to lze buď v nastavení počítače či v nastavení routeru).[159]

Trestní postih za pharming je obdobný jako za phishing. Posuzování bude záležet na konkrétním způsobu provedení.

Další formou útoku, který má své základy ve phishingu, je spread phishing. Rozdíl mezi klasickým phishingem a spread phishingem spočívá v objektu, na který je útok veden. V případě phishingu je útok veden spíše nahodile a snaží se zasáhnout co největší množství potenciálních obětí (předpoklady návratnosti odpovědí na phishingové emaily jsou v rozmezí 0.01 až 0,1 %). Oproti tomu spread phishing je cílený útok na konkrétní osobu (ať už fyzickou či právnickou). Pro komunikaci s touto osobou útočník často zneužije někoho blízkého potenciální oběti, aby navodil dojem důvěryhodnosti, a za něhož se později vydává. Na rozdíl od předchozího, spíše podvodného jednání, může u tohoto typu útoku dojít i k naplnění skutkové podstaty trestného činu Teroristický útok dle § 311.

Ve světě ICT je možné dopustit se takovéhoto podvodného jednání i prostřednictví telefonu - v tomto případě se útočník dopouští „vishingu“. V případě, že telefon útočník nepoužije jako prostředek hlasové komunikace, ale využívá pouze službu SMS, tak je jeho jednání označováno za „smishing“. Oba případy jsou trestně postihovány stejně jako u phishingu.[160]

5.1.5 Sniffing

Z technického hlediska se jedná o odchyt a následné čtení TCP paketů.[161] Tento odchyt se realizuje pro zjištění pohybu na síti a její následnou diagnostiku a pro hledání případných anomálii, které by se vyskytovaly na síti. Poté je následně například možné identifikovat zařízení, které je napadeno malwarem. Takovýto monitoring je legální a slouží jako prostředek k udržení a správy sítě.

Tato činnost může být považována za kriminální akt, pokud útočník jedná bez vědomí a souhlasu uživatele. Následně se díky takovému jednání může dopustit trestného činu podle § 182

---

[159] KLIMEK, Libor, Jozef ZÁHORA a Květoň HOLCR. Počítačová kriminalita: v európskych súvislostiach. Bratislava: Wolters Kluwer, 2016. ISBN 978-80-8168-538-5. s. 50

[160] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 263-266

[161] Transmission Control Protocol slouží k vytvoření spojení mezi počítači připojenými do sítě

Porušení tajemství dopravovaných zpráv, nebo kdyby byl příslušník určitého stavu – v tomto případě zaměstnanec provozovatele komunikačních služeb, tak by se dopustil kvalifikované skutkové podstavy dle § 182 odst. 5. V těchto případech je jedno, zda se takového jednání dopouští například administrátor sítě, pokud by jednal bez vědomí a souhlasu poškozeného.[162]

5.1.6 DoS, DDoS, DRDoS útoky

Tento specifický typ útoku cílí na funkčnost konkrétního serveru. Zkratka DoS vychází ze slov „denial of service“, které se dají přeložit jako odepření služby. Jednání, kterého se pachatel dopouští, spočívá v neobyčejně vysokém množství požadavků na jeden server v krátkém časovém úseku, které následně server zahltí a způsobí jeho zpomalení, chvilkovou nedostupnost nebo vyřazení pro všechny ostatní uživatele.

Společným prvkem pro všechny tyto útoky je, že vlastník útočícího zařízení nemusí mít ponětí o tom, že je součástí takového útoku. Může se to například stát po zasažení takového zařízení malwarem, který po sobě zanechá backdoors (již výše zmíněno), které umožňuje opětovně vzdálený přístup. Takto infikovaná zařízení se mohou řetězit a vytvořit botnet (také již výše zmíněno), prostřednictvím kterého pak pachatel útočí ze všech zařízení na cílený server.[163]

Rozdíly mezi těmito útoky spočívají především v rozdílném způsobu provedení. Útok DoS je veden z jednoho zařízení a pro napadaný server je poměrně jednoduché bránit se tím, že tomuto zařízení odepře přístup. Oproti tomu u útoku DDoS (Distributed Denial of Service) jsou útoky vedeny současně z několika počítačových systémů často umístěných po celém světě. Třetím, lehce odlišným typem jsou útoky DRDoS (Distributed Reflected Denial of Service), kde požadavek služby nepřichází primárně z útočícího počítače, ale na toto zařízení přijde podvržený požadavek na spojení s předem určeným cílem útoku. Tento požadavek je odesílán od iniciátora útoku neboli útočníka.

Mezi základní metody útoků způsobujících následné odepření služby patří:

1) Ping-Flood – díky příkazu „ping“ je možné zjistit rychlost odezvy a celkovou kondici konkrétního počítačového systému. Smysl tohoto útoku spočívá ve velkém množství těchto dotazů na server a ten následně „odpovídá“. V případě, že chce útočník svůj útok

[162] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 294

[163] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 396

učinit ještě škodlivějším, nastaví u příkazu ping možnost záplava (flood) a dotaz se odesílá bez toho, aby čekal na odpověď serveru.

2) SYN-Flood – funguje na podobném principu jako předchozí útok, avšak netestuje se kondice serveru, ale snaží se o navázání spojení, na které útočník následně neodpoví a server stále čeká a drží slot pro toto spojení – to může mít za následek vyčerpání slotů pro spojení.
3) IP spoofing – princip útoku je dost podobný, avšak při následné odpovědi serveru změní svou IP adresu určenou pro odpověď na jinou IP adresu než vlastní.
4) Smurf attack – tento útok využívá chybnou konfiguraci systému, který má povoleno rozesílání paketů všem zařízením, které jsou v síti zapojeny.

Byť většina útoků, o kterých se zmiňuji, je cílených a promyšlených, tak k takovému „útoku“ může dojít i bez úmyslu způsobit někomu škodu. K obdobné situaci dochází například při různých akcích začínajících v určitou chvíli nebo při „dead-line“ přihlášek do výběrových řízení, aukcí, univerzitních zkoušek atp. Server spuštěný v určitý čas je pak zaplaven žádostmi o spojení a není schopen reagovat na všechny žádosti.

Trestní postih za tuto skupinu útoků je značně komplikovaný, především kvůli nedobře zvolené implementaci ustanovení Úmluvy o kyberkriminalitě do českého právního řádu. Podle ustanovení trestního práva hmotného je nutné nejdříve získat přístup k počítačovému systému a následně data potlačit. Avšak v případě DoS útoku nedochází k získání přístupu, tudíž není naplněna skutková podstata trestného činu podle § 230 TZ. Při rekodifikaci trestního práva byly normy týkající se kybernetické kriminality nesprávně včleněny do našeho právního řádu a dvě skutkové podstaty jsou obsaženy v jedné. Z toho vyplývá, že podle § 230 TZ DoS a DDoS útoky nejsou trestné.[164]

5.2 Útoky spočívající ve vytváření a šíření škodlivého obsahu

Do této skupiny řadíme útoky, které využívají zařízení (například počítač nebo mobilní telefon) jako prostředek útoku na uživatele v kyberprostoru.

Budapešťská úmluva se ve svém třetím oddíle zabývajícím se trestnými činy souvisejícími s obsahem zaměřuje především na dětskou pornografii. K této úmluvě byl v lednu 2003 uzavřen

[164] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 295-302

dodatkový protokol, kterým se smluvní strany zavázaly kriminalizovat šíření rasistického a xenofobního materiálu s využitím počítačových systémů.[165]

Teorií je do této skupiny trestných činů zahrnuta také kyberšikana, kybergrooming, spam, hoax a další.

5.2.1 Dětská pornografie

Tato právní úprava cílí primárně na kriminalizaci chování, které směřuje k podněcování a svádění dětí k sexuálnímu zneužívání. Protiprávním jednáním v souvislosti s dětskou pornografií je i vytváření odkazů na stránky s dětskou pornografií.

Aby měly škodlivý obsah, musí tyto pornografické materiály zobrazovat osobu mladší 18 let. Trestné je také, pokud osoba vyhlíží jako dítě nebo se jeví být dítětem, kde není rozhodující její reálný věk. Dokonce není právně relevantní, jestli je chování skutečné nebo jen předstírané.[166]

Zajímavým je v tomto ohledu také paradox, že v České republice je dovoleno mít pohlavní styk s osobou starší 15 let, avšak snímek zachycující takovýto akt je považován za protiprávní. V tomto ohledu je úmysl zákonodárce poměrně jasný – snaží se chránit mladistvé před dosažením plné zletilosti před pornoprůmyslem a jejich případným zneužitím, avšak působí značně paradoxně, že provádět samotný akt je dle právního řádu v pořádku, ale například zachycení na mobilní prostředek by již bylo trestné.

Trestní zákoník, v návaznosti na ochranu dítěte před sexuálním zneužíváním plynoucí zejména z mezinárodních smluv, především z Budapešťské Úmluvy o počítačové kriminalitě a z Opčního protokolu k Úmluvě o právech dítěte proti prodeji dětí, dětské prostituci a dětské pornografii, upravuje znění skutkových podstat a sazeb za účelem účinnějšího potrestání pachatelů.[167]

Problémem z hlediska dostupnosti a dalšího rozšiřování dětské pornografie je chování rodičů na internetu. Konkrétně sdílení fotek obnažených dětí prostřednictvím sociálních sítí či různých serverů pro ukládání a sdílení fotografií. Není jasné, zda si rodiče uvědomují důsledky šíření takových snímků v prostředí kyberprostoru, zejména to, že materiály mohou být dále používané

---

[165] Dostupé zde: Dodatkový protokol k Úmluvě o počítačové kriminalitě [online]. [cit. 2020-08-09]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931bf

[166] GŘIVNA, Tomáš a Radim POLČÁK, ed. Kyberkriminalita a právo. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4. s. 119-120

[167] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 284

komunitou pedofilů a sdíleny na jejich fórech. Jedním z takových serverů, který slouží k ukládání a následnému sdílení fotografií je český server www.rajce.net, který však má ve svých podmínkách stanovena pravidla pro sdílení v čl. 13: *„Obsah zobrazující nahé osoby, zejména mladší 18 let, je na Rajče povoleno umisťovat pouze do soukromých alb s heslem.“,* avšak uživatelé tato pravidla nerespektují.[168]

Diskutabilním tématem z hlediska dětské pornografie se zdá být také její virtuální zobrazení. Novela trestního zákoníku č. 330/2011 Sb. přinesla trestnost děl, které zobrazují nebo využívají osobu, jež se jeví být dítětem. Ještě před touto novelou se k tomuto tématu vyjádřil Herczeg, který uvedl, že: *„[u] animovaného dětského porna chybí konkrétní dítě, které bylo zneužito, a z účelu a smyslu přijaté novely trestního zákona (ochrana před komerčním sexuálním zneužíváním dětí) lze dovodit, že držení virtuální (animované či kreslené) dětské pornografie pro vlastní potřebu by nemělo být postihováno jako trestný čin přechovávání dětské pornografie dle § 205a TZ. Virtuální dětská pornografie by totiž mohla být pro řadu pedofilů alternativou, která by jim umožnila realizovat své potřeby na úrovni masturbačních fantazií, a tím by se snížilo riziko, že své potřeby skutečně realizují.“*[169]

Z hlediska sexuologů převládá názor, že existence virtuální (animované) dětské pornografie by mohla být nápomocna k dostatečné stimulaci pedofilních jedinců, kteří by potom své tužby nemuseli ventilovat v reálném světě a tím ohrožovat zdravý vývoj dětí.[170] Dalším důvodem pro legalizaci počítačově vytvořené dětské pornografie by mohl být účel právní úpravy a úmysl zákonodárce, kterou je chránit děti před zneužíváním. V případě virtuální dětské pornografie k takovému zneužívání nedochází.

Trestní odpovědnosti v oblasti dětské pornografie odpovídají § 192 a 193. V § 192 je upravena výroba a jiné nakládání s dětskou pornografií, kde kvalifikovanou skutkovou podstatou je, kdo takové jednání způsobí prostřednictvím veřejně přístupné počítačové sítě. Oproti tomu § 193 se zaměřuje na samotnou tvorbu a využití dítěte a § 193a kriminalizuje účast na pornografickém představení, ve kterém vystupuje dítě. V § 193b se zákonodárce zaměřil na jednání pachatele, které

---

[168] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 305-306

[169] HERCZEG, Jiří. Virtuální dětská pornografie: Zločin bez oběti? In: VANDUCHOVÁ, M; GŘIVNA, T. Pocta Otovi Novotnému k 80. narozeninám. 1. vyd. Praha: Aspi, a.s., 2008, ISBN: 978-80-7357-365-2. s. 42

[170] Například: https://www.idnes.cz/zpravy/domaci/povolme-animovane-detske-porno-rika-sexuolog-weiss.A071009_115203_domaci_nad nebo https://www.idnes.cz/hry/magazin/sexuolog-trojan-rozhovor-pornografie-ve-virtualni-realite.A150603_160429_bw-magazin_anb

sleduje setkání s dítětem mladším 15 let s úmyslem spáchat taxativně vymezený trestný čin nebo jiný sexuálně motivovaný trestný čin.

5.2.2 Kybergrooming

Kybergrooming je psychická manipulace oběti prostřednictvím ICT s cílem jejího sexuálního využití.[171] Pro kybergrooming je typické použití technik sociálního inženýrství za účelem vyvolání pocitu důvěry u oběti a vytvoření obvykle i dlouhodobého vztahu. Následně se snaží útočník vybranou oběť od svého okolí izolovat.

Psychická manipulace v rámci kybergroomingu probíhá obvykle delší dobu – od cca 3 měsíců po dobu několika let. Tato doba je přímo závislá na způsobu manipulace a na důvěřivosti oběti. Existují případy, kdy predátor manipuloval dítě po dobu 2–3 let, než došlo k osobnímu setkání a sexuálnímu zneužití. Je třeba rovněž zohlednit hranici zletilosti dítěte – útočník může s dítětem komunikovat v době, kdy bylo nezletilé, k útoku však dojde až po završení zletilosti (je zjevné, že trestní sazby za sexuální zneužití zletilého a nezletilého dítěte jsou velmi rozdílné).[172]

Kybergrooming zpravidla prochází několika etapami:

1) snaha získání důvěry oběti a izolace této oběti od svého okolí,
2) snaha získání si oběti prostřednictvím dárků či laskavostí,
3) vytvoření závislého vztahu mezi útočníkem a obětí (především díky izolaci oběti od okolí a následné vytvoření kamarádského vztahu s útočníkem),
4) realizace osobního setkání,
5) útok v oblasti sexuální či jiný útok.[173]

S rychlým rozvojem internetu a stále větší přístupnosti sociálních a dalších sítí i pro děti předškolního věku se problém kybergroomingu stává stále aktuálnějším. Je třeba proti němu bojovat šířením osvěty a upozorňováním na takové problémy. Jedním z takových projektů v zahraničí je vytvoření desetileté virtuální dívky se jménem Sweetie, která je z Filipín. Za tímto projektem stojí nizozemská společnost Terre des Hommes Netherlands a jejich virtuální potenciální oběť obdržela během deseti dnů působení na internetu zprávy od přibližně dvaceti tisíc

[171] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 397

[172] KOPECKÝ, Kamil. Nebezpečí zvané kybergrooming I. [online]. [cit. 2020-08-11]. Dostupné z: https://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/

[173] Víte co je KYBERŠIKANA? [online]. [cit. 2020-08-11]. Dostupné z: https://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

mužů. Tisíc z nich jí během konverzace nabídlo výměnou za online sex určitou peněžitou částku.[174]

V našich končinách v poslední době proběhly dva projekty týkající se zneužívání dětí na internetu. Prvním z nich byla dokumentární série Černota, druhým, s celkem širokým dosahem, je dokumentární film V síti, na základě kterého bylo v mnoha případech zahájeno trestní stíhání s predátory a k dnešnímu dni již padlo několik rozsudků.[175]

Trestní postih za kybergrooming závisí na fázi a intenzitě, jakou probíhá. Zajímavým je však §193b, který kriminalizuje již návrh setkání s nezletilou osobou s úmyslem dopustit se trestného činu.

5.2.3 Kyberšikana

Šikana v reálném světě zahrnuje ponižování, zesměšňování, urážení a ubližování, ať už po stránce fyzické či po stránce psychické. Obdobně se útočník může chovat i ve virtuálním světě s tím rozdílem, že oběť se může jen velice těžce bránit, protože oproti reálnému světu nestačí se od takového jednání vzdálit. K tomu, abychom tradiční šikanu odlišili od kyberšikany, jsou zapotřebí informační a komunikační technologie ať už k distribuci materiálů, které mají povahu šikany (například nahrané napadení, zesměšňující fotka etc.) nebo k využití těchto technologií k napadání.[176]

Zrádným v případě kybernetické šikany může být faktické neprojevení následků šikany ve světě mimo kyberprostor. Často si příbuzní vůbec nemusí všimnout, že se něco děje. Nebývá také výjimkou, že kybernetická šikana je spojena i se šikanou mimo prostředí ICT.

Častým projevem kyberšikany je tzv. kyberstalking, kdy útočník prostřednictvím ICT pronásleduje svou oběť s cílem ji nějak poškodit. Obvykle se tak děje prostřednictvím telefonátů, SMS, emailů a různých sociálních sítí.[177] Dále útočník svou oběť zesměšňuje na sociálních sítích nebo prostřednictvím veřejných diskuzních fór. Vytváří falešné profily oběti nebo ji prostřednictvím falešných profilů kontaktuje. Velice častým projevem kyberšikany je sdílení

[174] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 307

[175] Více viz: https://www.youtube.com/watch?v=NZr6gf2YhM0

[176] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 309

[177] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 399

nelichotivých či erotických fotografií (často od bývalých partnerů po rozpadu vztahu), rozšiřování lží a pomluv a zveřejňování soukromé konverzace.[178]

Bohužel, s rozšiřujícím trendem šikany v kyberprostoru jsou již zaznamenány případy, kdy takovéto jednání mělo za následek sebevraždu poškozeného. Mezi známé případy patří příběh Amandy Todd, kdy po internetu kolovalo video, které sama oběť nahrála předtím, než spáchala sebevraždu a pomocí tabulek s textem popisovala svůj příběh. Amanda se několikrát přestěhovala a změnila školu, ale útočníci si jí stejně skrze sociální sítě našli a dál o ní rozšiřovali pomluvy a rozesílali její fotografie.[179]

Kyberšikana se nemusí nutně týkat jen nezletilých. Velice často jsou oběťmi šikany v kyberprostoru také veřejně známé osobnosti či politici. Judikatura se vyjádřila na téma veřejně známých osobností, že musí snášet větší tlak ze strany veřejnosti, avšak je na soudu, co je ještě v konkrétním případě v toleranci.[180] Dalšími oběťmi jsou právnické osoby, u nichž dochází ke kybernetické šikaně v rámci konkurenčního boje a snahy o diskreditaci dalšího soutěžitele.[181]

Z pohledu trestního práva není kybernetická šikana (ani klasická šikana) trestným činem. V úvahu přicházejí trestné činy § 175 Vydírání nebo § 354 Nebezpečné pronásledování, ve kterém je v odst. 1 písm. c) uveden jako prostředek elektronické komunikace. Další možnosti ochrany jsou prostřednictvím soukromého práva – například v případě pomluvy.

5.2.4 Extremismus a násilí

Dalšími škodlivými jevy v kyberprostoru jsou extremismus a násilí. Extremismus je popisován jako *„vyhraněné ideologické postoje, které vybočují z ústavních, zákonných norem, vyznačují se prvky netolerance, a útočí proti základním demokratickým ústavním principům, jak jsou definovány v českém ústavním pořádku.*“[182]

Právní základ regulace počítačové kriminality z hlediska extremismu byl na mezinárodní úrovni přijat s dodatkovým protokolem k Úmluvě o počítačové kriminalitě, který kriminalizoval rasistické a xenofobní chování páchané prostřednictvím počítačové sítě.

---

[178] Co je to kyberšikana a jak ji poznat [online]. [cit. 2020-08-11]. Dostupné z: https://www.vimkamklikam.cz/bezpeci-deti/co-je-to-kybersikana-a-jak-ji-poznat

[179] Amanda Todd 1996 - 2012 [online]. [cit. 2020-08-11]. Dostupné z: https://www.puresight.com/Real-Life-Stories/amanda-todd.html

[180] Judikatura viz: https://nalus.usoud.cz/Search/GetText.aspx?sz=1-367-03

[181] Kybernetická šikana – fenomén dnešní doby [online]. [cit. 2020-08-11]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/kyberneticka-sikana-fenomen-dnesni-doby

[182] Co je extremismus [online]. [cit. 2020-08-11]. Dostupné z: https://www.mvcr.cz/clanek/co-je-extremismus.aspx

Často se v prostředí internetu vyskytují webové stránky, které na první pohled vypadají nevinně a informují o historických událostech. Avšak fakta bývají zkreslená a značně ideologicky přizpůsobená. K další radikalizaci celkem dobře slouží různá diskuzní fóra a sociální sítě, které umožňují díky teoretické anonymitě pohodlné sdružování podobně smýšlejících lidí téměř bez reálného ohrožení, že budou nějak postiženi.[183]

Takovéto jednání může být posuzováno například dle § 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob nebo dle § 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod. Obě tyto skutkové podstaty mají v sobě zahrnutou i možnost šíření takového chování prostřednictvím počítačové sítě.

5.2.5 Ostatní

Z hlediska škodlivého obsahu na internetu můžeme považovat za nežádoucí i další chování. Jedním z takových počínání je například spam. Spamem se rozumí v širším slova smyslu veškeré nevyžádané zprávy, které jsou zasílané elektronicky, hromadně a ve valné většině bez vyžádání.

Scam je označení pro emaily, které jsou známé také jako Nigerijské dopisy,[184] kdy jsou pod různými záminkami po oběti požadované různé administrativní a další poplatky.[185]

Dalším jednáním, které se vyskytuje na internetu a tvoří škodlivý obsah, je tzv. hoax. Jeho cílem *je svým obsahem vyvolat dojem důvěryhodnosti. Informuje např. o šíření virů nebo útočí na sociální cítění adresáta. Může obsahovat škodlivý kód nebo odkaz na internetové stránky se škodlivým obsahem*.[186]

5.3 Útoky spočívající v porušování práv duševního vlastnictví

Útoky spadající do této kapitoly by se dali nazvat souhrnným pojmem počítačové pirátství. O definici počítačového pirátství se pokusil ve své diplomové práci Michal Bernat následovně:

---

[183] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5. s. 398

[184] Nigerijské dopisy jsou specifický druh podvodu, kdy se podvodník snaží vylákat ze své oběti peníze pod různorodými záminkami - veškerá komunikace však probíhá na dálku přes dopisy nebo e-maily a k přímému kontaktu mezi podvodníkem a obětí vůbec nedojde.

[185] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 236 - 239

[186] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník Kybernetické bezpečnosti [online]. [cit. 2020-08-05]. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf s. 76

„Počítačové pirátství zahrnuje veškerou protiprávní činnost, která je realizována pomocí výpočetní techniky a jejím důsledkem je porušování práv k duševnímu vlastnictví“[187]

K tématu práva duševního vlastnictví a jeho obsahu uvádí Jan Kolouch: *„Právo duševního vlastnictví představuje majetek nehmotné povahy, tzv. „nehmotné statky“, které jsou výsledkem tvůrčí činnosti člověka. Toto právo je nezávislé na hmotném substrátu (může být, proto užíváno kdykoliv a kdekoliv na světě) za podmínky, že je jedinečné, neopakovatelné a dostatečně originální.“*[188]

Na mezinárodní úrovni je duševní vlastnictví definováno v Úmluvě o zřízení Světové organizace duševního vlastnictví, a to v článku 2, odst. viii), konkrétně jako *práva k literárním, uměleckých a vědeckým dílům, k výkonům výkonných umělců, ke zvukovým záznamům a k rozhlasovému vysílání, k vynálezům ze všech oblastí lidské činnosti, k vědeckým objevům, k průmyslovým vzorům a modelům, k továrním, obchodním známkám a známkám služeb, jakož i obchodním jménům a obchodním názvům, na ochranu proti nekalé soutěži a všechna ostatní práva vztahující se k duševní činnosti v oblasti průmyslové, vědecké, literární a umělecké.*[189]

Právo duševního vlastnictví dělíme na oblast autorského a oblast průmyslového práva.

5.3.1 Průmyslová práva

Mezi průmyslová práva řadíme patenty, užitné vzory, topografie, průmyslové vzory, ochranné známky a označení původu výrobku. Orgánem v České republice, který poskytuje ochranu a vede rejstříky průmyslových práv, je Úřad průmyslového vlastnictví.

Z hlediska legislativy jsou významné následující zákony:

1) zákon č. 527/1990 Sb., o vynálezech a zlepšovacích návrzích,
2) zákon č. 478/1992 Sb., o užitných vzorech (také č. 527/1990 Sb.),
3) zákon 207/2000 Sb., o ochraně průmyslových vzorů,
4) zákon č. 441/2003 Sb., o ochranných známkách (dříve zákon 137/1995 Sb.),

---

[187] BERNAT, Michal. Fenomén počítačového pirátství. 2008. Diplomová práce. Masarykova univerzita. Vedoucí práce JUDr. Radim Polčák, Ph.D. s. 17

[188] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 277

[189] Úmluva o zřízení Světové organizace duševního vlastnictví [online]. [cit. 2020-08-11]. Dostupné z: https://www.upv.cz/cs/pravni-predpisy/mezinarodni/mezinarodni-smlouvy-spravovane-wipo.html

5) zákon 452/2001 Sb., o ochraně označení původu a zeměpisných označení (také 375/2007).[190]

Trestně právní ochraně odpovídá §269 Porušení chráněných průmyslových práv.

Z hlediska kybernetické kriminality jsou průmyslová práva méně významná. Na internetu jsou porušována především v souvislosti s administrativně-informativní činností a ochranou duševního vlastnictví.[191] Oproti tomu druhá kategorie práv duševního vlastnictví, tj. autorská práva, jsou v kyberprostoru daleko rozšířenější a tudíž významněji porušována.

5.3.2 Autorské právo

Porušování autorského práva v prostředí internetu je globálním problémem, jehož řešení je v nedohlednu. Z podstaty internetu jako nejrychlejšího a nejrozšířenějšího média na světě je nutnost pro autora šířit své dílo právě prostřednictvím internetu. Jak ale zamezit tvoření jeho nelegálních kopií? Když vývojáři například počítačových her vymyslí novou ochranu, jak nespustit bez originální kopie jejich dílo, tak do několika dnů různé hackerské skupiny dají volně k dispozici crack, který právě takové spuštění umožnuje. Obdobně obsah nového hudebního alba lze bez vědomí vydavatele zdarma stáhnout z internetu ještě dřív, než je zakoupené originální CD doručeno poštovní službou.

5.3.2.1 **Předmět autorského práva**

Předpisem, ze kterého vychází komplexní právní úprava, je Autorský zákon. V tomto právním předpisu je v § 1 stanoveno, co je předmětem autorského práva. Jsou to:

a) práva autora k jeho autorskému dílu,

b) práva související s právem autorským:

1. práva výkonného umělce k jeho uměleckému výkonu,

2. právo výrobce zvukového záznamu k jeho záznamu,

3. právo výrobce zvukově obrazového záznamu k jeho záznamu,

4. právo rozhlasového nebo televizního vysílatele k jeho vysílání,

---

[190] Ochrana průmyslového vlastnictví v České republice [online]. [cit. 2020-08-11]. Dostupné z: https://www.mzk.cz/sites/mzk.cz/files/ochrana_prumysloveho_vlastnictvi_cr.pdf

[191] JAKL, Ladislav, ed. Průmyslová práva na internetu: soubor vědeckovýzkumných statí. Praha: Metropolitní univerzita Praha, 2010. ISBN 978-80-86855-61-5.

5. právo zveřejnitele k dosud nezveřejněnému dílu, k němuž uplynula doba trvání majetkových práv,

6. právo nakladatele na odměnu,

c) právo pořizovatele k jím pořízené databázi,

d) ochrana práv podle tohoto zákona,

e) kolektivní správa práv autorských a práv souvisejících s právem autorským (dále jen „kolektivní správa“).

Z právního hlediska je zákonem chráněno autorské dílo a jako takové je definováno v § 2 Zákona o právu autorském takto:

(1) Předmětem práva autorského je dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam (dále jen "dílo"). Dílem je zejména dílo slovesné vyjádřené řečí nebo písmem, dílo hudební, dílo dramatické a dílo hudebně dramatické, dílo choreografické a dílo pantomimické, dílo fotografické a dílo vyjádřené postupem podobným fotografii, dílo audiovizuální, jako je dílo kinematografické, dílo výtvarné, jako je dílo malířské, grafické a sochařské, dílo architektonické včetně díla urbanistického, dílo užitého umění a dílo kartografické.

(2) Za dílo se považuje též počítačový program, fotografie a výtvor vyjádřený postupem podobným fotografii, které jsou původní v tom smyslu, že jsou autorovým vlastním duševním výtvorem. Databáze, která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem a jejíž součásti jsou systematicky nebo metodicky uspořádány a jednotlivě zpřístupněny elektronicky či jiným způsobem, je dílem souborným. Jiná kritéria pro stanovení způsobilosti počítačového programu a databáze k ochraně se neuplatňují.

(3) Právo autorské se vztahuje na dílo dokončené, jeho jednotlivé vývojové fáze a části, včetně názvu a jmen postav, pokud splňují podmínky podle odstavce 1 nebo podle odstavce 2, jde-li o předměty práva autorského v něm uvedené.

(4) Předmětem práva autorského je také dílo vzniklé tvůrčím zpracováním díla jiného, včetně překladu díla do jiného jazyka. Tím není dotčeno právo autora zpracovaného nebo přeloženého díla.

(5) Sborník, jako je časopis, encyklopedie, antologie, pásmo, výstava nebo jiný soubor nezávislých děl nebo jiných prvků, který způsobem výběru nebo uspořádáním obsahu splňuje podmínky podle odstavce 1, je dílem souborným.

(6) Dílem podle tohoto zákona není zejména námět díla sám o sobě, denní zpráva nebo jiný údaj sám o sobě, myšlenka, postup, princip, metoda, objev, vědecká teorie, matematický a obdobný vzorec, statistický graf a podobný předmět sám o sobě.[192]

V § 3 AZ jsou stanoveny výjimky, na které se ochrana podle tohoto zákona nevztahuje ve veřejném zájmu. Jedná se o úřední díla (například právní předpis, rozhodnutí, opatření obecné povahy, veřejná listina, sbírka listin), výtvory tradiční lidové kultury, není-li pravé jméno autora známo, a státní symboly podle zákona č. 352/2001 Sb.

5.3.2.2 **Obsah autorského práva**

Pro určení, co se podle zákona rozumí dílem, je nutné si stanovit, jaká konkrétní práva jsou zákonem chráněna. Tato práva jsou stanovena v § 10 AZ a jsou jimi výlučná práva osobnostní a výlučná práva majetková.

Osobnostní práva jsou dále upravena v § 11 AZ. Jsou jimi právo rozhodovat o zveřejnění díla, osobování si autorství a způsobu jakým bude autorství uvedeno, právo na nedotknutelnost vlastního díla a právo na autorský dohled. Dále je uvedeno v § 11, odst. 4, že těchto práv se autor nemůže vzdát, jsou nepřevoditelná a zanikají smrtí. V odst. 5 stejného § je zakotveno právo domáhat se ochrany autorských práv po smrti autora například osobou blízkou.

Majetková práva upravuje § 12 AZ, kde nejvýznamnějším právem je užití díla. Užitím se pro účely tohoto zákona rozumí práva na rozmnožení, rozšíření, pronájem, půjčování a vystavování originálu nebo rozmnoženiny díla. Dalším právem je sdělování díla veřejnosti, které zahrnuje práva na provozování díla živě nebo ze záznamu, vysílání díla rozhlasem nebo televizi, přenos a provozování rozhlasového a televizního vysílání díla.

5.3.2.3 **Volná užití**

V určitých případech taxativně stanovených zákonem je možnost použít určitým způsobem autorské dílo bez svolení autora. Takové užití však nesmí být v rozporu s běžným užitím díla a nesmí jím být dotčeny oprávněné zájmy autora.[193]

Tato volná užití jsou upravena v § 30 AZ:

---

[192] Zákon č. 121/2000 Sb.; Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)

[193] Výjimka z ochrany autorského díla - Volná užití (III.) [online]. [cit. 2020-08-12]. Dostupné z: https://www.pravoit.cz/novinka/vyjimka-z-ochrany-autorskeho-dila-volna-uziti-iii

(1) Za užití díla podle tohoto zákona se nepovažuje užití pro osobní potřebu fyzické osoby, jehož účelem není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu, nestanoví-li tento zákon jinak.

(2) Do práva autorského tak nezasahuje ten, kdo pro svou osobní potřebu zhotoví záznam, rozmnoženinu nebo napodobeninu díla.

(3) Nestanoví-li tento zákon dále jinak, užitím podle tohoto zákona je užití počítačového programu či elektronické databáze i pro osobní potřebu fyzické osoby či vlastní vnitřní potřebu právnické osoby nebo podnikající fyzické osoby včetně zhotovení rozmnoženiny takových děl i pro takovou potřebu; stejně je užitím podle tohoto zákona zhotovení rozmnoženiny či napodobeniny díla architektonického stavbou i pro osobní potřebu fyzické osoby či vlastní vnitřní potřebu právnické osoby nebo podnikající fyzické osoby (§ 30a) a pořízení záznamu audiovizuálního díla při jeho provozování ze záznamu nebo jeho přenosu (§ 20) i pro osobní potřebu fyzické osoby.

(4) Rozmnožena nebo napodobenina díla výtvarného zhotovená pro osobní potřebu fyzické osoby podle odstavce 1 musí být jako taková vždy zřetelně označena.

(5) Rozmnožena nebo napodobenina díla zhotovená pro osobní potřebu fyzické osoby podle odstavce 1 nesmí být použita k jinému než tam uvedenému účelu.

Další případy, které jsou vyňaty z ochrany autorského práva, jsou upraveny v § 31 až 39 AZ. Jedná se například o citaci, při které je nutné respektovat, aby byl zachován smysl a obsah citovaného díla, a o úřední a zpravodajskou licenci, kde musí být dílo užito jen v míře nutné pro účely zpravodajství.[194]

Pro zjištění, zda může být dílo předmětem volného užití, existuje tzv. třístupňový test, který vychází z Revidované Bernské úmluvy. Tento test spočívá ve splnění všech tří bodů, aby mohlo být s dílem volně nakládáno. Tyto bodu jsou:

1) výjimka uvedena v Autorském zákoně,
2) dílo je užíváno běžným způsobem,
3) užíváním díla nejsou dotčeny oprávněné zájmy autora díla.[195]

[194] ČERMÁKOVÁ-VLČKOVÁ, Adéla a Vladimír SMEJKAL. Autorská díla v hromadných sdělovacích prostředcích. Praha: Linde, 2009. ISBN 978-80-7201-744-7. s. 97-100

[195] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 286

5.3.3 Útoky v souvislosti s autorským právem

Pro útoky v prostředí internetu se nejčastěji používá souhrnný pojem pirátství, které zahrnuje pirátství softwarové a audiovizuální. Aby mohlo být jednání označeno za pirátství, je nutné, aby došlo k porušení autorského práva nebo práv s právem autorským souvisejících. Tato forma útoku se s rozšiřující dostupností a oblíbeností internetu značně rozšířila.[196]

5.3.3.1 Porušování autorských práv v oblasti ICT

Na základě poznatků z kriminalistické praxe je možné rozčlenit útoky v oblasti ICT na následující skupiny nelegálního jednání:

1) nelegální zásah do software,
2) nelegální výroba počítačových programů,
3) nelegální šíření software,
4) nelegální užívání počítačových programů.

Nelegální zásahy do software se dají učinit několika různými způsoby. Prvním z nich je plagiátorství, které ve svém jednání zahrnuje úpravu díla bez souhlasu autora a následné uvedení takového díla jako vlastního. Nelegální počin je také překlad originálního díla do jiného jazyka bez souhlasu autora a následné vydání takového díla. Zakázány jsou také další úpravy software, jejichž cílem je změna funkčnosti nebo zpřístupnění pomocí změny licenčních omezení. Do této skupiny lze zařadit i nabalování různého malware a virů k již existujícímu programu, aby se společně s ním šířily.

Druhá skupina nelegálního jednání se týká výroby software, dokumentace a dalších softwarových produktů, ke kterým pachatel nemá platnou licenci. Domácí výroba zahrnuje kopírování software pro osobní účely nebo i pro komerční účely bez získání potřebné licence a velmi často jeho následný prodej. Posledním způsobem páchání trestné činnosti patřícím do této skupiny je zneužití oficiálních kopírovacích služeb k vytvoření tzv. bezpečnostní kopie legálního software tím, že pachatel předloží jako původní originální kus už nelegální kopii nebo legální kopii použije vícekrát.

Skupina zahrnující jednání, jehož cílem je nelegálně šířit software, je tvořena pašováním a prodejem nelegálního software, prodejem software bez svolení autora, půjčováním software

[196] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 286-287

a nelegálním šířením software prostřednictvím internetu. Za nelegální není považován pronájem výpočetní techniky s již nainstalovaným softwarem. Nejčastěji dochází k půjčování software mezi mládeží, ale to již je kvůli stahování z internetu na ústupu. Při šíření software prostřednictvím internetu spadá trestní odpovědnost i na provozovatele serveru určenému k ukládání dat, pokud mohl a měl vědět, že šíření ukládaných dat je nelegální nebo se o této protiprávnosti dozvěděl a neučinil potřebné kroky vedoucí k odstranění dat.

Co se týká nelegálního užívání softwaru, tak jej můžeme rozdělit na dvě skupiny. Na užívání legálně získaného programu v rozporu s licenčním ujednáním a na užívání nelegálně získaného software, ke kterému dochází jak u jednotlivců, tak i ke komerčním účelům u právnických osob.[197]

5.3.3.2 **Porušování autorských práv s využitím prostředků ICT**

Mezi nejčastější způsoby porušování autorských práv souvisejícím s audiovizuálním pirátstvím patří šíření audiovizuálních děl pomocí internetu, umisťování takových děl na internet a šíření děl v rozporu s licenčními podmínkami.[198] K nelegálním činnostem v prostředí počítačových sítí dochází několika způsoby uvedenými v následujících odstavcích.

5.3.3.2.1. **Umístění a stažení díla**

Ještě před rozmachem internetu a zvýšením jeho rychlosti probíhalo nelegální rozšiřování děl prostřednictvím půjčování a případně kopírování na další nosiče. Na základě toho se nositelé autorských práv dožadovali ochrany před ušlým ziskem, které se dočkali trochu krkolomně prostřednictvím poplatku z každého prodaného CD a DVD a dalších médií a zařízení, které lze použít pro kopírování. Zároveň byly zavedeny technologické prvky, které bránily kopírování (například rootkit od společnosti Sony zmíněný v kapitole 5.1.3.6.).

S příchodem širokopásmového internetového připojení nastal velký rozmach porušování autorských práv. K rozšíření již nedocházelo pomocí jedné kopie, kterou mohl v jednu chvíli použít jen jeden člověk, ale data mohla být sdílena v jednu chvíli s téměř neomezeným počtem

[197] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 491-493

[198] KOLOUCH, Jan a Petr VOLEVECKÝ. Trestně právní ochrana před kybernetickou kriminalitou. Praha: Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-402-1. s. 108

uživatelů po celém světě. K takovému sdílení slouží především datová úložiště (file hosting) a peer-to-peer sítě.[199]

Společenská škodlivost takového jednání je podle výzkumu, který provedli v roce 2013 L. Aguiar a B. Martens, minimálně diskutabilní. Vyšlo totiž najevo, že ti, kteří nelegálně stahují hudbu, jsou až dvakrát aktivnějšími zákazníky z hlediska nákupu hudby než ti, kteří vlastní pouze originální nahrávky. Autoři zároveň došli k závěru, že nárůst šíření nelegální hudby na internetu je přímo úměrný nárustu prodeje legálních kopií.[200][201]

K trestnímu postihu za takové jednání slouží § 270 TZ, který směřuje vůči pachateli – tudíž vůči tomu, kdo nelegální obsah na internet uložil. Osobu, která si nelegální obsah z internetu stáhla, však nelze potrestat podle autorského zákona ani trestního zákoníku, byť této osobě musí být naprosto jasné, že obsah, který stahuje, je nelegální. K trestní odpovědnosti provozovatelů serverů s nelegálním obsahem je směrodatný zákon č. 480/20014 Sb., o některých službách informační společnosti, kde podle § 6 není provozovatel povinen dohlížet na obsah uložených dat a ani aktivně hledat případná protiprávní data na jeho serveru uložená. Z toho vyplývá, že jediným trestně odpovědným v celém řetězci je samotný pachatel.

5.3.3.2.2. **Torrenty**

Tzv. torrenty se v posledních několika letech staly dominantními v prostředí porušování autorských práv. Torrenty využívají ke sdílení dat technologii P2P, která slouží ke komunikaci mezi klienty bez nutnosti prostředníka – serveru. K stahování prostřednictvím torrentů je nutné mít naistalovaný program (nejznámější jsou uTorrent a BitTorrent), který lze bez problému volně stáhnout. Dále je potřeba mít soubor, který odkazuje přímo na obsah určený ke stažení. Tento soubor má koncovku .torrent a obsahuje tzv. tracker, který slouží jako prostředí komunikace mezi klienty.

Důležitým aspektem při stahování přes torrenty je, že stahování funguje oboustranně. Když uživatel stahuje nějaký soubor, tak tento soubor zároveň v části, kterou má již staženou sdílí pro

---

[199] DONÁT, Josef a Jan TOMÍŠEK. Právo v síti: průvodce právem na internetu. V Praze: C.H. Beck, 2016. ISBN 978-80-7400-610-4. s. 91-92

[200] AGUIAR, Luis a Bertin MARTENS. Digital music consumption on the internet: Evidence from clickstream data. Working Paper No. JRC79605, 2013 [online]. [cit. 2020-08-20]. Dostupné z: https://www.copyrightevidence.org/evidence-wiki/index.php/Aguiar_and_Martens_(2013)

[201] ZAVRŠNIK, Aleš. Kyberkriminalita. Přeložil David BLAŽEK. Praha: Wolters Kluwer, 2017. Právní monografie. ISBN 978-80-7552-758-5. s. 34

ostatní uživatele. Tito uživatelé se dělí na seedery a leachery. Rozdíl mezi nimi spočívá v kompletnosti dat, která sdílejí, přičemž seeder sdílí kompletní soubor a leacher jen části.[202]

K trestnímu postihu za takové jednání slouží § 270 TZ. Zde je nutné zdůraznit, že v případě nelegálního stahování prostřednictvím P2P jsou soubory zároveň sdíleny a je tak naplněna skutková podstata trestného činu.

5.3.3.2.3. **Warez**

Warezem se rozumí forma počítačového pirátství, v níž prostředí ICT slouží k urychlení nelegálního šíření děl, která porušují autorské právo. Warez se zaměřuje na počítačové hry (gamez), aplikace (appz), cracky (crackz) a filmy (moviez). Činnost většinou zahrnuje získání originálního software, následné odstranění ochrany proti kopírování a poté rozšíření napříč internetem.[203]

Uživatelé setkávají na tzv. warez fórech, které slouží jako „bezpečné" místo pro jejich komunikaci a následné šíření warezu.

Přímo související problém s warezem je tzv. linking, v němž uživatelé často odkazují na nelegální soubory uložené pomocí file hostingu. Takovéto odkazy se právě často vyskytují na warez fórech. Linky však mají většinou omezenou životnost vzhledem k vymazávání dat ze strany provozovatele file hostingu.[204]

5.3.3.2.4. **Embedded linky**

Jedná se o technické řešení týkající se umístění obsahu jiných internetových stránek prostřednictvím vložení určitého kódu. Tento kód odkazuje na data uložená na jiném serveru a zároveň je možné tato data uživatelem zobrazit na stránkách, kde byl tento kód vložen bez nutnosti navštívit server, na kterém jsou data skutečně uložena.[205]

K trestnosti této problematiky nejlépe poslouží nález Nejvyššího soudu v Praze, který se k trestnosti takového jednání vyjádřil následovně:

---

[202] KLIMEK, Libor, Jozef ZÁHORA a Květoň HOLCR. Počítačová kriminalita: v európskych súvislostiach. Bratislava: Wolters Kluwer, 2016. ISBN 978-80-8168-538-5. s. 38-43

[203] Warez [online]. [cit. 2020-08-13]. Dostupné z: https://cs.wikipedia.org/wiki/Warez

[204] KLIMEK, Libor, Jozef ZÁHORA a Květoň HOLCR. Počítačová kriminalita: v európskych súvislostiach. Bratislava: Wolters Kluwer, 2016. ISBN 978-80-8168-538-5. s. 35-36

[205] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 288

Přečinu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 270 odst. 1, odst. 2 písm. c) tr. zákoníku se dopustí ten, kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi a tohoto činu se dopustí ve značném rozsahu. O spáchání citovaného přečinu jde i v případě, že pachatel uloží na server odkazy (tzv. embedded linky), jejichž pomocí neoprávněně zpřístupní třetí osobě obsah cizího autorského díla prostřednictvím veřejně přístupné počítačové sítě (internetu). K této otázce se Nejvyšší soud již vyjádřil ve své judikatuře (viz rozhodnutí uveřejněné pod č. 7/2014 Sb. rozh. tr.), a konstatoval, že za neoprávněný zásah do zákonem chráněných práv ve smyslu § 270 odst. 1 tr. zákoníku lze považovat i takové jednání pachatele, který na Internetu v prostoru vyhrazeném pro své internetové stránky umístí odkazy (tzv. embedded linky) umožňující neoprávněný přístup k rozmnoženinám děl (např. filmových a televizních) umístěných na externích serverech tak, že kdokoli k nim může mít prostřednictvím takové internetové stránky přístup, aniž by k tomu měl souhlas nositelů autorských a souvisejících práv, a využije tzv. hostingu s možností uložení dat na serveru. V takovém případě totiž pachatel (umístěním tzv. embedded linku) umožnil přístup k rozmnoženině díla, a to jako osoba odlišná od osoby, která je vlastníkem této rozmnoženiny nebo jinou oprávněnou osobou, což je činnost, jíž je nutné považovat za porušení autorských práv k jednotlivým dílům a porušení práva na sdělování díla veřejnosti ve smyslu § 18 odst. 1, 2 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších právních předpisů. Jestliže tedy soudy nižších stupňů dospěly k závěru, podle něhož to byl obviněný J. T., kdo na hostitelské servery umístil odkazy ke stažení rozmnoženin filmových děl, pak takový závěr nemohou zpochybnit ani námitky obviněného, že příslušné internetové stránky zakládal před mnoha lety jen pro rodinné příslušníky.[206]

Uvedený nález Nejvyššího soudu lze považovat za důležitý s ohledem na efektivní ochranu autorských práv, zejména z důvodu příčinné souvislosti mezi jednáním pachatele, který provozuje webové stránky s cílem porušovat autorská práva a následkem takového jednání, kterým je právě ono porušení autorských práv.

---

[206] Usnesení Nejvyššího soudu v Praze ze dne 15.7.2015. [online]. [cit. 2020-08-17]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/CreateWordDocBody?openAgent&unid=97EEE035ACF94A98C1257F3C00203029&

5.4 Tradiční kriminalita v novém kabátě

Tato skupina zahrnuje útoky, které byly pro společnost známy již dříve, avšak s příchodem ICT se tyto útoky zčásti přesunuly i do prostředí kyberprostoru.

5.4.1 Sabotáže

Slovo sabotáž je odvozeno od francouzského slova „sabot“, které v překladu znamená dřevák či kopyto. Toto odvození pochází pravděpodobně z roku 1801, kdy ve Francii byly úmyslně poškozovány první programovatelné tkalcovské stavy právě vhozením dřeváků do stroje a tím došlo k první počítačové sabotáži.

Jedním z prvních útoků spadajících do počítačové kriminality na území tehdejšího Československa bylo poškození záznamů Úřadu důchodového zabezpečení uložených na magnetických páskách spáchané nespokojenými zaměstnanci. Dalším zajímavým případem bylo vypnutí sítě rozhlasových vysílačů s cílem zabránit oznámení o vniku vojsk Varšavské smlouvy na území Československa spáchaným vedoucím Ústřední správy spojů. Tento čin byl vzhledem k tehdejšímu režimu souzen až po revoluci.[207]

Sabotáž z pohledu trestního práva hmotného je upravena v § 314 TZ a její základní skutková podstata je následující:

(1) Kdo v úmyslu poškodit ústavní zřízení nebo obranyschopnost České republiky anebo poškodit mezinárodní organizaci zneužije svého zaměstnání, povolání, postavení nebo své funkce nebo se dopustí jiného jednání k tomu, aby

a) mařil nebo ztěžoval plnění důležitého úkolu mezinárodní organizace, orgánu veřejné moci, ozbrojených sil nebo bezpečnostního sboru, hospodářské organizace nebo jiné instituce, nebo

b) způsobil v činnosti takového orgánu anebo takové organizace nebo instituce poruchu nebo jinou závažnou škodu.[208]

Z této skutkové podstaty jasně vyplývá, že k tomu, aby se jednalo o sabotáž z pohledu trestního práva hmotného, je nutné, aby útok na počítač, jeho část či jakékoliv zařízení ICT byl veden s cílem poškodit ústavní zřízení nebo obranyschopnost ČR nebo mezinárodní organizaci. Z toho

[207] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s.104 - 108

[208] Zákon č. 40/2009 Sb.

vyplývá, že například ne každý útok na zařízení uchovávající data bude posuzován podle § 314 TZ.

5.4.2 Kyberterorismus

Pojem kyberterorismus vychází z původní trestné činnosti, která se objevila v novém kabátě, respektive v novém prostředí. K vymezení pojmu terorismus lze využít definici z roku 1980: *„Terorismus je propočítané použití násilí nebo hrozby násilím, obvykle zaměřené proti nezúčastněným osobám, s cílem vyvolat strach, jehož prostřednictvím jsou dosahovány politické, náboženské nebo ideologické cíle. Terorismus zahrnuje i kriminální zločiny, jež jsou ve své podstatě symbolické a jsou cestou k dosažení jiných cílů, než na které je kriminální čin zaměřen.“*[209]

Důvodů expanze terorismu do prostředí ICT je více, ale zejména se jedná o možnost páchat škody na velkou vzdálenost a se značnou efektivitou vzhledem k postupně stále větší závislosti společnosti i státu na prostředí ICT. Kyberterorismus můžeme v zásadě rozdělit do dvou kategorií. V prvním případě se jedná o útok na informační a telekomunikační nástroje, které zahrnují státní a vojenskou infrastrukturu. Druhá skupina je definována útoky na obsah, které spočívají především v psychologické válce, ideologickém působení atp.[210]

Z mezinárodního obranného hlediska je kybernetický prostor pojímán jako 5. operační doména, prostřednictvím které může probíhat nejen válečný konflikt (dalšími doménami jsou země, voda, vzduch a kosmický prostor). Dále lze rozlišovat, kde nastane dopad kybernetického útoku – zda pouze v prostředí kyberprostoru (například útok na servery, data uložená na internetu) nebo ve fyzickém světě (například pozměnění navigačních přístrojů ve veřejné letecké dopravě s cílem způsobit nehodu).[211]

---

[209] Definice pojmu terorismus [online]. [cit. 2020-07-31]. Dostupné z: https://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx

[210] DIBLÍKOVÁ, Simona. Analýza trendů kriminality v České republice v roce 2015 [online]. [cit. 2020-07-31]. Dostupné z: http://www.ok.cz/iksp/docs/437.pdf s. 75

[211] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 115

5.4.3 Podvodné webové stránky

Podvodné webové stránky vykazují znaky klasického podvodného jednání, které má za cíl pod falešnou záminkou či uvedením druhé osoby v omyl z této osoby vylákat peníze nebo ji jiným způsobem způsobit škodu na majetku.

Často je při takovém počínání na internetu využíváno již výše zmíněné sociální inženýrství, snažící se nalákat potencionální oběti na výhodnější ceny nebo na možnost výhry. Pro dosažení výhod má případná oběť poskytnout citlivé informace (email, telefonní číslo, adresu nebo hesla), které jsou následně zneužity pro další případné útoky. Druhým způsobem, jak pro sebe podvodným jednáním získat finanční prospěch, je požadování určité částky za registraci nebo rovnou prodej zboží za výhodné ceny, které následně nebude doručeno.[212]

Jednoduchý návod, jak poznat podvod na internetu, vydalo Evropské spotřebitelské centrum, které je zřízeno za součinnosti Evropské komise a jednotlivými státy. Podle tohoto návodu je vhodné dodržovat několik pravidel, jako je například vyhledání informací o společnosti na internetu, přečtení recenzí ostatních uživatelů, zhodnocení prezentace obchodníka na internetu, neprovádění platby předem u neprověřeného prodejce, zvýšená pozornost u plateb přes Western Union, kontrola obchodního rejstříku v zemi prodejce, přečtení obchodních a smluvních podmínek, kontrola internetové domény (například doména na Kokosových ostrovech nepůsobí příliš důvěryhodně) a případná kontrola pomocí Google street view, zda opravdu existuje sídlo společnosti na dané adrese.[213]

V České republice je podobné jednání postihováno dle § 209 TZ jako podvod. Takové jednání je dokonáno, když se pachatel na úkon oběti obohatí. Dle § 209 odst. 6) je příprava trestná. V případě, že by takovýmto jednáním byly odcizeny a následně použity přístupové údaje, tak by se pachatel dopustil trestného činu dle § 230 Neoprávněný přístup k počítačovému systému a nosiči informací.

---

[212] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 266-267

[213] ESC radí, jak poznat podvod na internetu [online]. [cit. 2020-08-17]. Dostupné z: https://evropskyspotrebitel.cz/nakupy-online/esc-radi-jak-poznat-podvod-na-internetu/

6 Vybrané zahraniční instituty v oblasti kybernetické bezpečnosti

Jak již bylo několikrát zmíněno v předchozích částech této práce, kybernetická kriminalita má typicky mezinárodní charakter a proto dosáhnout efektivní ochrany lze jedině pomocí harmonizace právních řádů do takové podoby, aby jednání v kyberprostoru bylo ve všech státech posuzováno jako legální či nelegální podle podobného vzorce, a podobně i následně sankciováno.

Tvorba vnitrostátního právního řádu je suverénním právem každého státu. Jediný způsob, jak toto suverénní právo směřovat do takové míry, aby došlo ke kýžené harmonizaci, je dobrovolné přistoupení států ke smlouvě či organizaci a zavázání se takovým mezinárodním dokumentem řídit. Takovou organizací je například EU a dokumentem výše zmíněná Úmluva o počítačové kriminalitě.

V této kapitole se zaměřím na přístup vybraných států v oblasti kybernetické kriminality, konkrétně porušování autorského práva ve Francii a ochrany nezletilých ve Velké Británii, a porovnám efektivitu takové úpravy s právním řádem České republiky.

6.1 Francie a legislativa z pohledu autorského práva

Ve Francii se pokusili omezit a v lepším případě co nejvíce zabránit internetovému pirátství prostřednictvím zákona HADOPI.[214] Na jeho základě byl založen speciální úřad, jehož předmětem činnosti je monitorovat a zjišťovat ilegální stahování materiálu z internetu, který podléhá autorským právům. Takovéto stahování bylo po zjištění zaznamenáno a uživatel, který ilegální materiály stáhl, byl následně upozorněn. Tato varování byla celkově tři a následně měl úřad pravomoc odpojit uživatele, který ignoroval tyto výzvy od internetu až na období jednoho roku.[215]

První verze uvedeného zákona zakotvila pravomoc úřadu k odsouzení pachatele po třech výzvách k odpojení od internetu bez jakéhokoliv rozhodnutí soudu. Takovou možnost shledal francouzský ústavní soud jako protiústavní vzhledem k rozporu se zásadou presumpce neviny a také proto, že porušuje Deklaraci práv člověka a občana z roku 1789, dělbu moci a svobodu slova. Jako reakce na to vznikla druhá verze tohoto zákona, ve kterém již byla pravomoc rozhodovat o odpojení od internetu v rukou soudu. Díky tomu již nemohlo dojít k situaci, kdy by pachateli hrozil

[214] Zkratka anglického názvu: High Authority for Copyright Pretection and Dissemination of Works on the Internet law)

[215] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf s. 289

dvojí trest za jeden skutek (jeden by vyměřil úřad a druhý soud za porušení například norem trestního práva v oblasti autorských práv). [216]

Po dvou letech fungování tohoto úřadu bylo zaznamenáno přes 3 miliony IP adres, které se dopustily stahování nelegálního materiálu porušujícího autorská práva. Z tohoto počtu bylo více než na milion IP adres odesláno první varování. Druhé varování již obdrželo jen lehce přes 100 tisíc uživatelů. Posledního varování se za 2 roky fungování úřadu dočkalo pouze 340 „pirátů". Ani třetí varování nezabralo celkem ve 14 případech, kterých se ujaly úřady, a po 2 letech byla poprvé jednomu uživateli vyměřena pokuta ve výši 150 eur.[217]

V červenci roku 2013 na základě návrhu francouzského ministra kultury byla odstraněna možnost odpojení uživatele od internetu z tohoto zákona. Za celou dobu existence zákona byl k takovému trestu v délce 15 dní odsouzen jediný člověk. Zároveň byla zachována pokuta ve výši 1500 eur při hrubé nedbalosti. Navíc zmínil, že fungování aparátu čítajícího 60 zaměstnanců vyjde státní pokladnu na 12 milionů euro a z milionu rozeslaných emailů, téměř statisíce doporučených dopisů je nakonec stíháno jen 134 případů, což způsobuje, že celý systém je neekonomický a neefektivní.[218]

Za rok 2019 podle nejnovější zprávy úřad řešil celkový počet 9 milionů případů, což je oproti roku 2018 pokles o 5 miliónů. Za celou svou existenci úřad rozdal pokuty ve výši 87 tisíc eur, a naopak náklady na provoz tohoto úřadu se vyšplhaly do výše 82 miliónů eur.[219]

Jako myšlenka, jak bojovat i internetovým pirátstvím, může být zákon vnímán zajímavě, nicméně data za jedenáct let platnosti ukazují téměř nulovou efektivitu tohoto předpisu. Zároveň podle výše zmíněné studie L. Aguiara a B. Martense (2013) nezpůsobuje internetové pirátství pokles prodeje originálních děl (alespoň tedy v hudebním průmyslu).

---

[216] HADOPI law [online]. [cit. 2020-08-20]. Dostupné z: https://en.wikipedia.org/wiki/HADOPI_law

[217] Francouzský zákon HADOPI po dvou letech poprvé trestá [online]. [cit. 2020-08-20]. Dostupné z: https://www.zive.cz/bleskovky/francouzsky-zakon-hadopi-po-dvou-letech-poprve-tresta/sc-4-a-165434/default.aspx

[218] France backs away from Hadopi [online]. [cit. 2020-08-20]. Dostupné z: https://www.theregister.com/2012/08/06/hadopi_under_fire/

[219] Hadopi po 11 letech aneb Francie ukazuje, že hon na filmové piráty nemá smysl [online]. [cit. 2020-08-20]. Dostupné z: https://www.root.cz/clanky/hadopi-po-11-letech-aneb-francie-ukazuje-ze-hon-na-filmove-piraty-nema-smysl/

6.2 Velká Británie a ochrana nezletilých v kyberprostoru

Nejvýznamnějšími zákony v Anglii a Walesu z hlediska ochrany dětí na internetu a postihování dětské pornografie jsou Protection of Children Act z roku 1978 a Criminal Justice Act z roku 1988.

V The Sexual Offences Act z roku 2003, zejména v paragrafech 48 až 50, jsou uvedeny trestné činy v sexuální oblasti vůči dítěti. V paragrafu 15 tohoto zákona je trestný čin, který odpovídá § 193b TZ Navazování nedovolených kontaktů s dítětem. Tento trestný čin je z hlediska The Sexual Offences Act jinak označován jako „grooming" a dopustí se ho pachatel starší 18 let, který s osobou naopak mladší 18 let komunikoval alespoň dvakrát či se s ní dokonce setkal. Dle tohoto zákona je trestné i cestovat se záměrem se s takovou osobou potkat, a to kdekoliv na světě. Pro trestnost takového jednání se vyžaduje úmysl. Dle paragrafu 15 (2) je zdůrazněno, že k takovému jednání může dojít kdekoliv na světě. Pachateli, který se takového jednání dopustí hrozní trest odnětí svobody v délce až 10 let.[220]

Zajímavou právní úpravu mají ve Velké Británii ohledně pořizování, šíření a držení fotografií nebo pseudofotografií dětí. Tato právní úprava je obsažena v Protection of Children Act z roku 1978 a v paragrafu 1 a dá se proti ní bránit, pokud žalovaná osoba prokáže, že má legitimní důvod pro distribuci nebo ukazování fotografií či jejich vlastnictví nebo, že fotografie neviděl, nevěděl o nich nebo neměl podezření, že jsou nemravné. V paragrafu 1A jsou nastavena speciální pravidla, pokud je na fotografiích zachycena osoba, která je starší 16 let a je v manželském vztahu, registrovaném partnerství nebo spolu žijí v jedné domácnosti jako partneři.[221]

Významnou organizací v boji proti zneužívání dětí na internetu i mimo něj je Child Exploitation and Online Protection command, která funguje v rámci struktury Národní kriminální agentury (NCA). Tato agentura sleduje nelegální aktivity v prostředí internetu a pomocí jejich stránek je možnost učinit oznámení.[222] Mezi lety 2006 až 2010 díky vlastnímu vyšetřování v kyberprostoru a následnému předání orgánům činným v trestním řízení došlo k více než 1000 zatčení.[223]

---

[220] Sexual Offences Act 2003 [online]. [cit. 2020-08-20]. Dostupné z: https://www.legislation.gov.uk/ukpga/2003/42/section/15

[221] Protection of Children Act 1978 [online]. [cit. 2020-08-21]. Dostupné z: https://www.legislation.gov.uk/ukpga/1978/37/section/1A

[222] Child Exploitation and Online Protection command [online]. [cit. 2020-08-21]. Dostupné z: https://www.ceop.police.uk/safety-centre/

[223] Child Exploitation and Online Protection Command [online]. [cit. 2020-08-21]. Dostupné z: https://en.wikipedia.org/wiki/Child_Exploitation_and_Online_Protection_Command

Oproti zákonné úpravě v České republice byl až do roku 2003 rozdíl ve věku, který byl pro dětskou pornografii stěžejní. Ve Velké Británii až do roku 2003 mohla být zobrazena osoba nad 16 let bez toho, aby to bylo považováno za dětskou pornografii (stejná věková hranice je stanovena pro legální intimní styk). V tomto roce byla hranice posunuta na 18 let, aby byla v souladu s mezinárodním právem.

Zajímavým rozdílem je také porovnání trestného činu podle § 193a TZ, podle kterého je trestná účast na pornografickém představení, ve kterém účinkuje dítě. Tomuto ustanovení odpovídá paragraf 47 Sexual Offences Act (z roku 2003), které však trestnost tohoto jednání vztahuje ke slíbené či uskutečněné platbě za takové představení. V tom případě, pokud by bylo představení s volným vstupem, pak by takové jednání nebylo možné podle tohoto paragrafu postihnout.[224]

[224] Sexual Offences Act 2003 [online]. [cit. 2020-08-21]. Dostupné z: https://www.legislation.gov.uk/ukpga/2003/42/section/47

7 Současný stav kybernetické kriminality

V současné době narůstá počet protizákonných aktivit páchaných v prostředí kyberprostoru. Platné právo jen složitě reaguje na stále rozvíjející a téměř každou chvíli se měnící prostředí internetu a informačních technologií.[225]

Evropská komise reagovala již v roce 2017 na zvyšující se rizika spojená s kybernetickou kriminalitou a v její prognóze bylo zmíněno riziko v podobě internetu věci. Internet věci je pojem vytvořený již v roce 1999 a znamená *celosvětovou síť propojených objektů (věcí), které jsou jednoznačně adresovatelné s tím, že tato síť je založena na standardizovaných komunikačních protokolech umožňujících výměnu a sdílení dat a informací, jejichž analýzou bude možné docílit vyšší přidané hodnoty.*[226] S tímto novodobějším fenoménem Evropská komise spojuje riziko v podobě desítek miliard zařízení připojených k internetu do roku 2020.

Další riziko spatřuje v mnohem větším využití kybernetických nástrojů při práci vnitrostátních orgánů při plnění jejich povinností a rostoucí závislost státu na prostředí kyberprostoru a informačních technologiích. Na základě toho bylo navrženo posílení Agentury Evropské unie pro bezpečnost sítí a informací (ENISA) a vytvoření určitého rámce, podle kterého budou jednotlivé státy přistupovat ke kybernetické bezpečnosti a zavedení společné diplomatické reakce EU jako celku na nepřátelské útoky v kyberprostoru.

Dále je zmíněn až 300 % nárůst použití ransomware mezi roky 2015 až 2016 a až pětinásobný vzrůst dopadů kybernetické kriminality na hospodářství mezi lety 2013 až 2017.[227]

V blízké budoucnosti se podle Kuchty bude kybernetická kriminalita upínat především na nehmotné informace, očekává se zvýšený počet útoků na mobilní zařízení a zařízení připojená do sítě zaměstnavatele, propojení útoků se sociálními sítěmi, zvýšený počet teroristických a špionážních útoků, zneužití internetu k šíření fake news, jakož i intenzivnější střet mezi anonymitou uživatele a ochranou soukromí. Internet bude stále nejlepším možným mediem pro porušování autorských práv.[228]

---

[225] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 766

[226] Internet věcí [online]. [cit. 2020-08-21]. Dostupné z: https://i2ot.eu/internet-of-things/

[227] Stav Unie v roce 2017: Komise zesiluje svoji reakci na kybernetické útoky [online]. [cit. 2020-08-21]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/cs/MEMO_17_3194

[228] Časopis pro právní vědu a praxi: Aktuální problémy počítačové kriminality včetně její prevence, Josef Kuchta. 2016. Brno: Právnická fakulta Masarykovy univerzity v Brně, 1993-. ISSN 1210-9126.

7.1 Kybernetická kriminalita v České republice

I přesto, že v posledních letech dochází v České republice k postupnému poklesu trestné činnosti, v dílčí oblasti kybernetické kriminality je statistika spíše na vzestupu a počet deliktů naopak pravidelně stoupá. V roce 2018 bylo zaznamenáno 6 815 trestných činů, což je o 1 161 více nežli v roce předchozím.[229] Na základě nejnovějšího srovnání zjistíme, že za rok 2019 v oblasti kybernetické kriminality byl zaznamenán nárůst na celkový počet 8 417 skutků, přičemž obecná kriminalita za posledních osm let rapidně poklesla o více než 40 procent. Růst kybernetické kriminality není specifikem našeho státu, ale naopak kopíruje trendy ve světě.

Hlavními projevy této kriminality jsou nejen trestná činnost typická z běžného světa, která se aklimatizovala na prostředí kyberprostoru, ale také čistě kybernetické kriminalita jako útoky na počítačové a informační systémy.[230] Největší nárůst byl zaznamenán u mravnostních trestných činů, které zahrnují trestnou činnost v oblasti dětské pornografie a ohrožování výchovy dítěte včetně například navazování nedovolených kontaktů s dítětem. Významným aspektem zde je, že mladiství nejsou jen obětmi takové činnosti, ale často také samotnými pachateli.

Oblíbenou činností se stává využívání virtuálních měn (například bitcoinů) k převádění finančních prostředků pocházejících z nelegální činnosti. Díky anonymitě virtuálních měn jsou právě k takové činnosti často využívané a z pohledu orgánů činných v trestné činnosti prakticky nevystopovatelné.

Nárůst byl zaznamenán také v souvislosti s nenávistnými projevy na různých komunikačních a sdělovacích platformách. Tyto projevy mají často rasistický či xenofobní podtext.

Předpokladem je, že útoky v kyberprostoru budou stále mít za cíl získání majetkového prospěchu prostřednictvím phishingových útoků. Nadále budou hrozbou útoky na platební

[229] Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2018 [online]. [cit. 2020-08-21]. Dostupné z: https://www.mvcr.cz/soubor/zprava-o-situaci-v-oblasti-vnitrni-bezpecnosti-a-verejneho-poradku-na-uzemi-cr-v-roce-2018.aspx s. 47

[230] Kybernetická kriminalita v ČR stoupá, loni to bylo 8417 činů [online]. [cit. 2020-08-21]. Dostupné z: https://www.ceskenoviny.cz/zpravy/kyberneticka-kriminalita-v-cr-stoupa-loni-to-bylo-8417-cinu/1852630

instituce a DDoS útoky. Ohroženými jsou také zdravotnické organizace, které disponují osobními údaji.[231]

7.2 Úvahy de lege ferenda

Při psaní této práce a procházení veškeré materie, se kterou jsem měl možnost přijít do styku, jsem narazil na několik, dle mého názoru neideálně zpracovaných oblastí týkajících se kybernetické kriminality a jejich příslušné právní úpravy.

7.2.1 Trestní odpovědnost právnických osob

První z legislativních nedokonalostí se týká trestní odpovědnosti právnických osob. Ta u nás byla zavedena zákonem č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, s účinností od 1. 1. 2012. Tento zákon využívá taxativní výčet trestných činů, které mohou být spáchány právnickou osobou uvedenou v § 7 tohoto zákona. Výčet byl novelou s účinností k 1. 12. 2016 změněn a byla použita opačná generální klauzule ve stejném § tohoto zákona, která naopak uvádí trestné činy, kterých se právnická osoba dopustit nemůže. V § 8 jsou uvedeny podmínky přičitatelnosti trestní odpovědnosti právnické osobě. Oproti původní úpravě se právnická osoba již může dopustit TČ dle § 205 TZ Krádež či dle § 207 Neoprávnění užívání cizí věci. Stále se však nemůže dopustit některých trestných činů uvedených právě v § 7 TOPO, což i přes pochopitelnost například u TČ opilství nebo TČ proti branné povinnosti neodpovídá rovnému postavení trestní odpovědnosti jak fyzických, tak právnických osob při existenci § 8 TOPO, který stanovuje, jaké jednání je právnické osobě přičitatelné.

7.2.2 Postihnutelnost DoS a DDoS kyberútoků

Dalším problémem, na který jsem narazil, je postihnutelnost DoS a DDoS útoků z hlediska českého právního řádu. Je to způsobeno především nevydařenou transformací požadavků vyplývajících z Kapitoly II, oddílu 1, článku 4 Úmluvy o počítačové kriminalitě, kde je uvedeno následující:

[231] Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2018 [online]. [cit. 2020-08-21]. Dostupné z: https://www.mvcr.cz/soubor/zprava-o-situaci-v-oblasti-vnitrni-bezpecnosti-a-verejneho-poradku-na-uzemi-cr-v-roce-2018.aspx s. 48

Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem, pokud je spácháno úmyslně, neoprávněné poškození, vymazání, snížení kvality, pozměnění nebo ***potlačení počítačových*** *dat.*

Tento požadavek byl do českého právního řádu promítnut prostřednictvím § 230 TZ následovně:

(2) Kdo ***získá přístup*** *k počítačovému systému nebo k nosiči informací a:*

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, ***potlačí****, sníží jejich kvalitu nebo je učiní neupotřebitelnými,*

Na základě takového promítnutí se staly DoS či DDoS útoky takřka nepostihnutelnými, protože při nich nedochází k získání přístupu k počítačovému systému. Možným případným řešením by bylo začlenění samostatné skutkové podstaty, která by dopadala na útoky DoS a DDoS.

7.2.3 Virtuální dětská pornografie

Poslední nedokonalostí, kterou bych rád zmínil, je spíše téma k úvaze pro odborníky z řad psychologie a kriminalistiky. Je jí trestnost virtuální dětské pornografie. Pokud bereme jako fakt, že se s určitou pravděpodobností ve společnosti vyskytuje tato parafilní porucha, kterou dokonce pracovní skupina pro přípravu manuálu DSM-5, který obsahuje mentální poruchy, označuje za další sexuální orientaci,[232] pak musí vyvstat otázka, jak lze tento problém vzhledem k nutné ochraně dětí řešit. Moderní technologie nabízí řešení, které se na první pohled nejeví jako skvělé a velké části společnosti může připadat až nemravné. Je jím legalizace virtuálního dítěte, které by mohlo posloužit k ukojení potřeby člověka trpícího touto poruchou. Tato varianta se z mého pohledu jeví jako společensky neškodná (při zachování této potřeby pro pedofila a případného šíření v rámci léčení, a byť to může znít i jako utopie, tak například dostupnosti na základě doporučení ošetřujícího lékaře) a může znamenat zvýšení ochrany pro skutečně žijící děti, které by jinak mohly být ohroženy. Avšak současná právní úprava obsahuje v § 192 TZ odst. (1) *Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu****, jež se jeví být dítětem****, bude potrestán odnětím svobody až na dva roky.*

[232] Pedofilie [online]. [cit. 2020-08-21]. Dostupné z: https://cs.wikipedia.org/wiki/Pedofilie

Problematickou v tomto případě je zvýrazněná část, jež zahrnuje do skutkové podstaty právě i materiály, které zobrazují virtuální dítě. Je na odbornících v rámci psychologie, aby zhodnotili dostatečnost takového stimulu pro pedofila, a na zákonodárci, aby tento názor vyslyšel a virtuální dětskou pornografii ze skutkové podstaty trestného činu případně vyňal.

Závěr

Při psaní své diplomové práce jsem měl možnost seznámit se s velkým množstvím odborné literatury a informací týkajících se problematiky kybernetické kriminality. Už ze začátku byla impulzem při výběru tohoto tématu především jeho aktuálnost a také osobní zkušenost s prostředím kyberprostoru a původní domněnka, že o velkém množství škodlivého jednání v tomto prostředí mám přinejmenším alespoň povědomí.

Kyberprostor je již běžnou součástí života každého z nás a jeho role v našem životě bude čím dál výraznější. S jeho rostoucí rolí je potřeba také tento prostor efektivně právně regulovat a případné porušení těchto norem trestat a následné sankce vymáhat. Za tímto účelem jsou pořádány mezinárodní konference, na nichž je téma kybernetické kriminality pravidelně diskutováno.

Ve své práci jsem se v první řadě zaměřil na historii počítače a na zařízení a vynálezy, o kterých můžeme mluvit jako o předchůdcích počítače. Následně má pozornost směřovala k nejrychlejšímu a nejvýraznějšímu médiu dnešní doby a tím je internet. Díky jeho rozvoji jsou dnešní technologie na takové úrovni a zaujímají v našem životě tak důležité místo. V poslední části první kapitoly jsem se zaměřil na kyberprostor a jeho odlišnost od internetu a samotný pojem kybernetické kriminality.

Následující kapitola byla zaměřena na právní rámec upravující kyberprostor a vše co se ho týká. Byla zmíněna jak soukromoprávní, tak i veřejnoprávní úprava, která je předmětem této práce. Z tohoto důvodu jsem se zaměřil na veřejnoprávní předpisy, a to především na dva v kyberprostoru dominantní – Trestní zákoník a Zákon o kybernetické bezpečnosti. Při procházení platné legislativy jsem narazil na několik nedostatků a některé z nich jsem zmínil v kapitole zabývající se tím, jak by právo mělo vypadat v budoucnu. Další část této kapitoly byla zaměřena na mezinárodní právní úpravu. Tato právní úprava by měla v ideálním případě být jakýmsi minimálním požadavkem na vnitrostátní úpravy všech zemí.

Třetí kapitola této práce pojednává o specifických znacích, kterými se kybernetická kriminalita projevuje a které mají s velkou pravděpodobností za následek i popularitu této kriminality, která vede ke každoročnímu nárůstu uskutečněných trestných činů.

Další kriminologický aspekt, na který jsem se zaměřil, byl subjekt trestného činu. Rozdělil jsem pachatele na několik skupin podle jejich schopností nebo trestné činnosti, které se dopouštějí. Druhou částí této kapitoly byla oběť trestného činu a snaha definovat uživatele, kteří jsou náchylnějšími stát se obětí kybernetické kriminality.

Jádrem této diplomové práce se stal podle předpokladů výčet kybernetické kriminality. Tento seznam jsem rozdělil do čtyř skupin podle dělení uvedeného v Úmluvě o počítačové kriminalitě. Tento seznam byl lehce upraven podle učebnice kriminologie a měl by podat ucelený pohled na nelegální činnost páchanou v kyberprostoru. V této kapitole jsem definoval jednání, kterým se pachatel dopouští trestné činnosti. U některých skutkových podstat byly uvedeny konkrétní případy, které se staly na území České republiky nebo v zahraničí. U některých jednání je uveden také postih odpovídající ustanovením TZ.

Šestá kapitola je věnována porovnání vybraných institutů v České republice s úpravou zahraničních zemí. Jako první jsem si vybral Francii a autorské právo, na jehož právní úpravu jsem narazil během hledání zdrojů týkajících se autorského práva v kyberprostoru. Druhou zahraniční zemí je Velká Británie, a to zejména kvůli liberálnějšímu pojetí práva a jejímu pohledu na ochranu nezletilých v kyberprostoru.

Závěrečná kapitola se snaží reflektovat současný stav kybernetické kriminality a směr, kterým se trestná činnost bude vyvíjet, přičemž jsem zjistil, že počet kybernetických trestných činů má posledních několik let stále vzrůstající tendenci a prognózy do budoucna hovoří o stále větším nebezpečí z kybeprostoru, ať už se jedná o kyberterorismus či příchod IoT, který souvisí s inteligentními domácnostmi či dokonce inteligentními budovami. Ve druhé části jsou uvedena statistická data z hlediska kybernetické kriminality páchané na území České republiky. Třetí část obsahuje myšlenky de lege ferenda, nad kterými jsem se zamýšlel během psaní této diplomové práce.

Seznam zkratek

ICT – Informační a komunikační technologie (stejně tak IKT)

TZ – trestní zákoník

AZ – Autorský zákon

P2P – peer-to-peer

TČ – Trestný čin

TOPO – Trestní odpovědnost právnických osob

IoT – Internet of things (internet věcí)

Seznam použitých zdrojů

1 Seznam použité literatury

ČERMÁKOVÁ-VLČKOVÁ, Adéla a Vladimír SMEJKAL. Autorská díla v hromadných sdělovacích prostředcích. Praha: Linde, 2009. ISBN 978-80-7201-744-7.

DIANIŠKA, Gustáv. Kriminológia. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2009. Právnické učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 978-80-7380-198-4.

DONÁT, Josef a Jan TOMÍŠEK. Právo v síti: průvodce právem na internetu. V Praze: C.H. Beck, 2016. ISBN 978-80-7400-610-4.

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

GŘIVNA, Tomáš a Radim POLČÁK. Kyberkriminalita a právo. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.

GŘIVNA, Tomáš, Miroslav SCHEINOST, Ivana ZOUBKOVÁ, et al. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5.

HERCZEG, Jiří. Virtuální dětská pornografie: Zločin bez oběti? In: VANDUCHOVÁ, M; GŘIVNA, T. Pocta Otovi Novotnému k 80. narozeninám. 1. vyd. Praha: Aspi, a.s., 2008, ISBN: 978-80-7357-365-2.

HOLCR, Květoň a Jaroslav FENYK. Kriminológia. Bratislava: Iura Edition, 2008. ISBN 978-80-8078-206-1.

CHATFIELD, Tom. Digitální svět: 50 myšlenek, které musíte znát. Vyd. 1. [Praha]: Slovart, 2013. 208 s. ISBN 978-80-7391-720-3

JAKL, Ladislav, ed. Průmyslová práva na internetu: soubor vědeckovýzkumných statí. Praha: Metropolitní univerzita Praha, 2010. ISBN 978-80-86855-61-5.

JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

KLIMEK, Libor, Jozef ZÁHORA a Květoň HOLCR. Počítačová kriminalita: v európskych súvislostiach. Bratislava: Wolters Kluwer, 2016. ISBN 978-80-8168-538-5.

KOLOUCH, Jan a Petr VOLEVECKÝ. Trestně právní ochrana před kybernetickou kriminalitou. Praha: Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-402-1.

KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf

MAISNER, Martin. Zákon o kybernetické bezpečnosti: komentář. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8.

MATĚJKA, Michal. Počítačová kriminalita. Praha: Computer Press, 2002. ISBN 80-7226-419-2.

NAUMANN, Friedrich. Dějiny informatiky: od abaku k internetu. Praha: Academia, 2009. Galileo. ISBN 978-80-200-1730-7.

POLČÁK, Radim. Právo informačních technologií. Praha: Wolters Kluwer, 2018. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-045-8.

POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice.

POŽÁR, Josef. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

SCHEINOST, Miroslav, Martin CEJP, Petr POJMAN a Tomáš DIVIÁK. Trendy vývoje organizovaného zločinu a jeho vybraných forem. Praha: IKSP, 2018. ISBN 978-80-7338-171-4.

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.
SMEJKAL, Vladimír, Tomáš SOKOL a Martin VLČEK. Počítačové právo. Praha: C.H. Beck, 1995. Právo a hospodářství (C.H. Beck). ISBN 80-7179-009-5.
SMEJKAL, Vladimír. Internet a §§§. Praha: Grada, 2001. ISBN 80-247-0058-1.
SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a-nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.
ŠÁMAL, Pavel. Trestní zákoník: komentář. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5.
TOMÁŠEK, Jan. Úvod do kriminologie. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-746-7.
VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3.
YAR, Majid. Cybercrime and society. London: SAGE, 2006. ISBN 1-4129-0753-5. Dostupné také z: http://www.loc.gov/catdir/enhancements/fy0659/2005934725-d.html
ZAVRŠNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017. Právní monografie. ISBN 978-80-7552-758-5.

2 Odborné časopisy

LÁTAL, Ivo, Počítačová (informační) kriminalita a úloha policisty při jejím řešení. Policista, 1998, č.3.
von HENTIG, Hans. The Criminal and His Victim. Studies in the Sociobiology of Crime: Yale University Press, New Haven 1948.
Josef Kuchta. Časopis pro právní vědu a praxi: Aktuální problémy počítačové kriminality včetně její prevence, Brno 2016: Právnická fakulta Masarykovy univerzity v Brně, 1993-. ISSN 1210-9126.
GŘIVNA, Tomáš. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. Acta Universitatis Carolinae. Iuridica. 2008, 2008(4), 21-34. ISSN 0323-0619.

3 Seznam použitých internetových zdrojů

http://news.bbc.co.uk/2/hi/technology/4072704.stm
http://www.ok.cz/
https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf s. 97
https://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/
https://computer.howstuffworks.com/phishing.htm
https://cs.qwe.wiki/wiki/Convention_on_Cybercrime
https://cs.wikipedia.org
https://dc.czechnationalteam.cz/index.html

https://dictionary.cambridge.org/dictionary/english/cyberspace
https://ec.europa.eu/commission/presscorner/detail/cs/MEMO_17_3194
https://en.wikipedia.org/
https://evropskyspotrebitel.cz/nakupy-online/esc-radi-jak-poznat-podvod-na-internetu/
https://history-computer.com/
https://i2ot.eu/internet-of-things/
https://is.mendelu.cz/
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931bf (dodatkový protokol – počitačové krim)
https://spomocnik.rvp.cz/clanek/21714/BARLOWOVA-DEKLARACE-NEZAVISLOSTI-KYBERPROSTORU.html
https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html
https://video.aktualne.cz/dvtv/matka-ji-prodala-pedofilum-znasilnily-me-stovky-muzu-hlavou/r~70ac19fef90e11e982ef0cc47ab5f122
https://wikisofia.cz/
https://www.ceop.police.uk/safety-centre/
https://www.ceskenoviny.cz/zpravy/kyberneticka-kriminalita-v-cr-stoupa-loni-to-bylo-8417-cinu/1852630
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=SnCoQlkS
https://www.copyrightevidence.org/evidence-wiki/index.php/Aguiar_and_Martens_(2013)
https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html
https://www.czso.cz/
https://www.digitalnipevnost.cz/viki/keylogger-keystroke-logger
https://www.e15.cz/kryptomeny/ceske-pocitace-zaplavil-program-ktery-tezi-kryptomeny-bez-vedomi-uzivatelu-1341752
https://www.fi.muni.cz/usr/jkucera/pv109/2003/xcerveny.htm
https://www.finextra.com/newsarticle/13864/banks-told-to-beware-enemy-within
https://www.history.com/news/who-invented-the-internet
https://www.idnes.cz/
https://www.internetembezpecne.cz/internetem-bezpecne/malware/botnet/
https://www.internetworldstats.com/stats.htm
https://www.irozhlas.cz/zpravy-domov/nemocnice-benesov-kyberneticky-utok-ransomware-vykupne-ochrana-osobnich-udaju_2001140615_cha
https://www.kaspersky.com/resource-center/threats/adware
https://www.legislation.gov.uk
https://www.malwarebytes.com/malware/
https://www.msn.com/cs-cz/zpravy/v%C4%9Bda-a-technika/zd%C3%A1-se-%C5%BEe-garmin-vyd%C4%9Bra%C4%8D%C5%AFm-zaplatil-syst%C3%A9my-napaden%C3%A9-ransomwarem-obnovil-de%C5%A1ifrovac%C3%ADm-k%C3%B3dem-aktualizov%C3%A1no/ar-BB178hKu?li=BBOoZca
https://www.mvcr.cz
https://www.mzk.cz/sites/mzk.cz/files/ochrana_prumysloveho_vlastnictvi_cr.pdf
https://www.nortonsecurityonline.com/security-center/evolution-of-computers.html
https://www.pbs.org/nerds/timeline/pre.html
https://www.policie.cz/clanek/vite-co-je-kybersikana.aspx
https://www.pravniprostor.cz
https://www.pravoit.cz/novinka/vyjimka-z-ochrany-autorskeho-dila-volna-uziti-iii

https://www.psp.cz/sqw/text/orig2.sqw?idd=133551
https://www.psp.cz/sqw/text/tiskt.sqw?O=5&CT=410&CT1=0#prilohy(důvodová zpráva)
https://www.puresight.com/Real-Life-Stories/amanda-todd.html
https://www.root.cz/clanky/hadopi-po-11-letech-aneb-francie-ukazuje-ze-hon-na-filmove-piraty-nema-smysl/
https://www.ses-escrow.co.uk/blog/guide-phishing-ransomware-terminology
https://www.statista.com/statistics/617136/digital-population-worldwide/
https://www.theregister.com/2012/08/06/hadopi_under_fire/
https://www.unodc.org
https://www.upv.cz/cs/pravni-predpisy/mezinarodni/mezinarodni-smlouvy-spravovane-wipo.html
https://www.vice.com/en_us/article/qkjzwp/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster
https://www.vimkamklikam.cz/bezpeci-deti/co-je-to-kybersikana-a-jak-ji-poznat
https://www.youtube.com/watch?v=NZr6gf2YhM0
https://www.zive.cz/bleskovky/francouzsky-zakon-hadopi-po-dvou-letech-poprve-tresta/sc-4-a-165434/default.aspx

4 Seznam použitých právních předpisů

Zákon č. 45/2013 Sb., Zákon o obětech trestných činů a o změně některých zákonů, ve znění pozdějších předpisů
Zákon č. 141/1961 Sb., Zákon o trestním řízení soudním, ve znění pozdějších předpisů
Zákon č. 121/2000 Sb.; Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů
Zákon č. 127/2005 Sb.; Zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) ve znění pozdějších předpisů
Zákon č. 181/2014 Sb.; Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů ve znění pozdějších předpisů
Zákon č. 40/2009 Sb., Trestní zákoník, ve znění pozdějších předpisů
Zákon č. 89/2012 Sb.; Zákon občanský zákoník, ve znění pozdějších předpisů

5 Kvalifikační práce

BERNAT, Michal. Fenomén počítačového pirátství. 2008. Diplomová práce. Masarykova univerzita. Vedoucí práce JUDr. Radim Polčák, Ph.D.
DOUBRAVA, Jiří. Počítačová kriminalita (trestněprávní a kriminologické aspekty). Olomouc, 2011. Diplomová práce. Univerzita Palackého v Olomouci Právnická fakulta.
PETRJÁNOŠ, David. Trestněprávní úprava internetové kriminality. Brno, 2017. Diplomová práce. Právnická fakulta Masarykovy univerzity obor Právo. Vedoucí práce Doc. JUDr. Josef Kuchta, CSc.
KALINEC, Zdeněk. Vybrané aspekty kybernetické kriminality. Brno, 2015. Bakalářská práce. Právnická fakulta Masarykovy univerzity obor Právo. Vedoucí práce Doc. JUDr. Marek Fryšták, Ph.D.
KRUPIČKA, Jiří. Trestněprávní a kriminologické aspekty internetové kriminality. Praha, 2010. Rigorózní práce. Právnická fakulta Univerzity Karlovy v Praze. Vedoucí práce Prof. JUDr. Jiří Jelínek, CSc.

6 Seznam použité judikatury

Nález: https://nalus.usoud.cz/Search/GetText.aspx?sz=1-367-03
Usnesení:
http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/CreateWordDocBody?openAgent&unid=97EEE035ACF94A98C1257F3C00203029&

Abstrakt

Fenomén kybernetické kriminality se v dnešní době již nedá považovat za něco neznámého a široké veřejnosti skrytého. Přesto většina laické společnosti má povědomí pouze o zlomku protiprávního jednání, ke kterému v kyberprostoru dochází. To má za následek, že podstatná část uživatelů internetu jedná v kyberprostoru v rozporu s platnou legislativou, ať již tak činí vědomě či nikoliv.

Kybernetickou kriminalitu nelze považovat za méně nebezpečnou, než jiné druhy kriminality. Naopak díky její dostupnosti, globálnosti a teoretickému odstupu pachatele od samotného trestného činu je tato kriminalita rok od roku na vzestupu a její dopady jsou stále závažnější především kvůli závislosti dnešní společnosti na informačních a komunikačních technologiích.

Cílem této diplomové práce je čtenáři představit svět kybernetické kriminality a nabídnout obecný pohled na jednotlivé aspekty této kriminality.

V úvodu této práce jsou blíže popsány jednotlivé termíny, se kterými se při procházení této práce bude čtenář setkávat a je zde zkráceně popsaná historie vzniku počítače a internetu.

Nezbytnou součástí této práce je představení legislativního rámce v oblasti právní úpravy kybernetické kriminality. V této části jsou zmíněny zákony, které se v prostředí kyberprostoru aplikují a změny v mezinárodních úpravách, které vnitrostátní úpravu ovlivňují.

Třetí část diplomové práce se zabývá specifickými rysy kybernetické kriminality, které jsou pro tento druh trestné činnosti příznačné a jejich existence dělá z této kriminality fenomén.

Obsáhlejší kapitolou v rámci celé práce je část zabývající se subjektem trestného činu neboli pachatelem a jeho obětí. V této kapitole jsou nejdříve uvedena obecná specifika pachatele a oběti trestného činu a následně jsou již popsány specifičtí pachatelé, kteří se vyskytují v kyberprostoru.

Nejobsáhlejší kapitolou celé práce je část, která se snaží čtenáři dát téměř kompletní výčet jednotlivých druhů trestné činnosti v prostředí kyberprostoru. Tyto trestné činy jsou řazeny do čtyř oddílů, které odpovídají dělení dle mezinárodní úpravy. U některých trestných činu jsou zmíněny i nejznámější případy zejména kvůli reálnější představě čtenáře o závažnosti této kriminality.

V šesté kapitole jsou vybrány jednotlivé zahraniční instituty v rámci obrany proti kybernetické kriminalitě a jejich následná efektivita. Těmito zeměmi jsou Francie a její snaha o vyřešení problémů kolem porušování autorského práva a Velká Británie s její úpravou dětské pornografie.

Poslední kapitola této práce obsahuje dvě části. První část se zaměřuje na současný stav kybernetické kriminality v rámci České republiky a následující prognózy. Druhá část je zaměřena na otázky, jak by právo v této oblasti mělo vypadat a na jednotlivé nefunkční a neupravené instituty v české právní úpravě.

Abstract

Today, the phenomenon of cybercrime can no longer be considered something obscured or unknown to the general public. Yet the majority of general population is aware of only a fraction of the offenses committed in cyberspace. As a result, a substantial proportion of Internet users act in violation of valid legislation in cyberspace, whether they do so knowingly or not.

Cybercrime cannot be considered less dangerous than other forms of crime. On the contrary, due to its availability, globality and possible distance of the offender from the crime itself, this kind of criminal behaviour is on the rise year by year and its effects are becoming more severe, mainly due to the dependence of today's society on information and communication technologies.

The aim of this thesis is to provide an introduction to the cybernetic world crime and offer a general view of the various aspects of this criminal activity.

The introduction of my thesis deals with detailed description of the basic terminology present throughout the whole thesis and contains a brief description of the history and origins of the computer and Internet.

An essential part of my thesis is the presentation of the legislative framework in the field of cybercrime regulation. This section mentions the laws that apply in the cyberspace environment and changes in the international regulations that affect the national legislation.

The third part of the thesis deals with specific features of cybercrime that are characteristic for this type of criminal activity and the occurrence of which makes this criminality a phenomenon.

A more extensive chapter in the entire thesis is the part dealing with the subject of a crime, namely the perpetrator and their victims. In this chapter, the general characteristics of a perpetrator and a victim are provided first. Subsequently, specific offenders who are found in cyberspace are described.

The most extensive chapter of the whole thesis is the part that aims to provide an almost complete list of individual types of crimes that occur in the cyberspace environment. These crimes are divided into four sections that correspond with the international regulation. In certain instances a well known examples of criminal cases are mentioned, in order to provide a better notion of the severity of this criminality.

The sixth chapter features individual foreign institutes in the field of defense against cybercrime and their effectiveness. The countries mentioned are France and it‘s efforts to solve problems related to copyright infringement law and the United Kingdom with its regulation of child pornography. The last chapter of this work contains two parts. The first part focuses on the current state of cybercrime in the Czech Republic and it’s prognosis. The second part focuses on

the matters how law in this area should be constituted and on individual non-functional and unregulated institutes in Czech law system.

Klíčová slova / Key words

Kybernetická kriminalita, Kriminologie, Trestní právo

Cybercrime, Crimonology, Criminal law