UNIVERZITA KARLOVA

Právnická fakulta

Jana Ševčíková

Kriminologické aspekty kybernetické kriminality

Pachatelé a oběti kybernetické kriminality

Diplomová práce

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

Katedra trestního práva

Datum vypracování práce (uzavření rukopisu): 31.5.2020

Prohlašuji, že jsem předkládanou diplomovou práci vypracovala 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 142 364 znaků včetně mezer.

Jana Ševčíková

diplomantka

V Praze dne 31.5.2020

Obsah

Úvod

Kybernetická kriminalita je poměrně novým fenoménem, kterému je v dnešní době v odborné literatuře a v rámci kriminologických výzkumů věnována stále větší pozornost. Tato skutečnost je pravděpodobně nejvíce zapříčiněna zvyšujícím se nápadem kybernetické kriminality, který je způsoben jednak přesunem některých tradičních trestných činů, např. podvodů z tzv. off-line světa do kyberprostoru, ale také množstvím nových ryze kybernetických trestných činů[1].

Téma této diplomové práce analyzující kybernetickou kriminalitu z kriminologického pohledu jsem si zvolila v návaznosti na studium několika volitelných předmětů z oblasti kriminologie, psychologie a kybernetické kriminality, které jsem absolvovala jak na Právnické fakultě Univerzity Karlovy, tak v rámci zahraničního pobytu v Belgii na Katholiek Universiteit Leuven v akademickém roce 2018/2019. V rámci studia jsem měla možnost se seznámit se specifiky kybernetické kriminality, které znesnadňují boj proti této kriminalitě, ať už se jedná o problematiku obtížné trestněprávní klasifikace některých jednání, vysokou míru latence této kriminality, potenciální závažný dopad na zvláště zranitelné oběti, anonymitu pachatele ztěžující jeho odhalení a mnohé další.

Při studiu těchto předmětů a odborné literatury jsem si však také uvědomila, že kriminologické výzkumy a právní teorie se kybernetické kriminalitě dosud věnovaly z poměrně obecného hlediska – v největší míře jsou zaměřeny na popis kriminálních jednání, ke kterým v kyberprostoru dochází (včetně možné právní kvalifikace), případně jsou věnovány popisu specifik kybernetické kriminality odlišujících ji od jiných druhů kriminality. Vědecké výzkumy a statistiky pak poskytují především obecné informace o četnosti a dynamice této trestné činnosti. Naopak výrazně menší pozornost je věnována podrobnějším otázkám, např. charakteristice pachatelů a obětí, přičemž pokud se již s takovými výzkumy setkáme, jsou často zaměřeny buď na velmi obecný výzkumný vzorek nebo pouze na některé skupiny, např. děti nebo seniory[2]. Tyto skupiny bývají obecně považovány za rizikové, ale přesto existuje velké množství určitých druhů kybernetické trestné činnosti (např. podvody, hacking, kyberstalking), u nichž lze předpokládat, že viktimizovány mohou být osoby bez ohledu na věk. Lze připustit, že pokud se jedná o kybernetické trestné činy, které existují také v tzv. off-line světě (např. nenávistné trestné činy, stalking, podvody), lze ohledně osobnosti pachatele a oběti čerpat také

[1] Ministerstvo vnitra ČR. *Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2018,* Praha, 2019, s. 47 [online]. [cit. 2020-03-14]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx

[2] Roubalová a kol. Institut pro kriminologii a sociální prevenci. *Oběti kriminality. Poznatky z viktimizační studie*, 2019, Praha, s. 93, [online]. [cit. 2020-03-14]. Dostupné z: http://www.ok.cz/iksp/docs/449.pdf

ze zdrojů věnujících se pachatelům a obětem těchto trestných činů spáchaným mimo kyberprostor, přesto však s sebou spáchání trestného činu prostřednictvím internetu může nést specifika, která se projeví u obětí či pachatelů v kyberprostoru odlišně.

Domnívám se tedy, že základní obecná charakteristika kybernetické kriminality byla v odborné literatuře již bohatě popsána a nyní je zde prostor pro podrobnější zaměření na konkrétní trestné činy a jejich pachatele a oběti, který by mohl přinést nový posun v boji s kybernetickou kriminalitou, a to jak v oblasti prevence, tak represe. K úspěšnosti výzkumů by navíc mohla přispět také skutečnost, že se v poslední době také zvyšuje povědomí a zájem veřejnosti o problematiku nebezpečnosti internetu, důkazem může být např. i úspěch dokumentárního snímku V síti Víta Klusáka a Barbory Chalupové upozorňující na fenomén kybergroomingu.

Cílem této práce je analyzovat a shrnout poznatky z oblasti kriminologie pachatelů a obětí kybernetické trestné činnosti a zjistit, zda tito pachatelé a oběti vykazují specifika ve srovnání s pachateli a oběťmi trestné činnosti, k níž nedochází v kyberprostoru. První část této práce bude zaměřena na objasnění základních pojmů, které budou v rámci práce blíže zkoumány. Druhá část této práce bude zaměřena na stručné vymezení pojmu kybernetické kriminality a pachatele této trestné činnosti ze všeobecného pohledu – budou zkoumány poznatky o pachatelích kybernetické kriminality bez zaměření na konkrétní druh této trestné činnosti. Na základě stejného přístupu bude zpracována také třetí část této práce, která se věnuje obětem kybernetické kriminality a jejich specifikům. Ve čtvrté části budou zkoumána specifika konkrétních jednání z oblasti kybernetické kriminality, a to hate crimes, podvodných jednání a kyberstalkingu přičemž pozornost bude zaměřena opět nejvíce na pachatele a oběti této trestné činnosti a dopady této trestné činnosti. Výběr těchto konkrétních jednání byl proveden s cílem zaměřit se na jednání co nejvíce různorodá, která umožňují komparaci mezi pachateli a oběťmi těchto různých druhů trestné činnosti a vystihující heterogennost kybernetické kriminality.

1. Základní pojmy

Úvodem je nezbytné stručně vymezit základní pojmy, na které je tato diplomová práce zaměřena, tedy především pojem kybernetické kriminality, pachatelů a obětí této trestné činnosti. Při vymezení těchto pojmů bude vycházeno z obecně přijímaných kriminologických a zákonných definic.

1.1. Kybernetická kriminalita

Kybernetická kriminalita představuje termín zastřešující velké množství různých kriminálních jednání a o její přímé definici nepanuje v rámci odborné literatury shoda. Nejobecněji lze kybernetickou kriminalitu popsat jako trestnou činnost, ke které dochází v kyberprostoru[3]. Kyberprostorem se rozumí *„veškerý virtuální prostor, především svět internetu, jiných sítí a mobilních technologií“*, přičemž tento prostor slouží ke komunikaci, zábavě, práci, vyhledávání i ukládání informací a poskytuje tak široké možnosti pro páchání různorodé trestné činnosti[4].

K vytvoření bližší představy o formách kybernetické kriminality, tedy konkrétních jednáních jejích pachatelů, přispívají různé systémy klasifikace kybernetické kriminality. Pro účely této práce se jeví jako nejvhodnější vymezit kybernetickou kriminalitu prostřednictvím třístupňové klasifikace založené na rozlišování mezi druhy jednání, kterých se pachatelé dopouští, případně podle vztahu počítače či počítačového systému k trestnému činu, jež nebyl přímo spáchán v kyberprostoru[5]. Tato klasifikace a její modifikace jsou používány ve Velké Británii, Kanadě, ale také na mezinárodní úrovni. Rozdělení trestných činů je následující:

a) **počítač nebo počítačový systém je „obětí“ kriminální aktivity pachatele**, tj. je terčem jeho kriminálního jednání, příkladem mohou být případy hackingu, šíření malware a DDoS útoky (tzv. *„computer crimes“*);
b) **počítač nebo počítačový systém je nástrojem ke spáchání tradičního trestného činu,** který je možné spáchat i v tzv. off-line světě, tedy bez využití informačních technologií, např. trestného činu výroby a distribuce pornografie, kyberstalkingu,

[3] Válková, H., Kuchta, J., Hulmáková, J. a kol. *Základy kriminologie a trestní politiky*. 3. vydání. Praha: C.H. Beck, 2019, s. 542.
[4] Gřivna, T., Scheinost M., Zoubková I. a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019, s. 388.
[5] Clough, J. *Principles of Cybercrime.* Cambridge: Cambridge University Press, 2015. Pozn. přístup k publikaci byl poskytnut v rámci studia předmětu Cybercrime na KU Leuven v letním semestru 2018/2019 z University Publishing Online.

mravnostní kriminality, porušování autorských práv, nenávistných trestných činů, podvodů a kyberšikany (tzv. *„computer facilitated crimes“*);

c) **počítač nebo počítačový systém je nosičem informací důležitých pro trestní řízení o jiném trestném činu:** jedná se o případy, kdy počítače či počítačového systému nebylo využito ke spáchání trestného činu přímo, ale může poskytnout důležité informace o spáchání trestného činu; příkladem může být situace, kdy je počítač nosičem e-mailové komunikace mezi pachatelem vraždy a osobou, která jej k vraždě navedla (tzv. *„computer related crimes“*).

Lze se domnívat, že toto vymezení pojmu kybernetické kriminality nejlépe pokrývá všechny druhy trestné činnosti, která je dnes za kybernetickou kriminalitu považována a rovněž v případě výskytu nových kriminálních jednání v kyberprostoru bude pravděpodobně možné tato jednání do jedné z výše uvedených skupin zařadit. V právní teorii, mezinárodních smlouvách a vnitrostátních právních úpravách kybernetické kriminality se setkáme s podrobnějšími klasifikacemi trestněprávních jednání založenými na definicích skutkových podstat těchto jednání[6], vzhledem k obecnému zaměření této diplomové práce a také čerpání z cizojazyčných zdrojů se však výše uvedená univerzální klasifikace jeví jako vhodnější.

Závěrem lze poznamenat, že pojem „kybernetická kriminalita“ nebo „kyberkriminalita“ postupně v odborné terminologii nahradil pojmy „počítačová kriminalita“ a „informační kriminalita“[7], které vystihovaly tehdejší chápání tohoto druhu kriminality spojené nejčastěji právě s počítačem. Dnes se ale jeví jako vhodnější vymezit toto jednání právě pomocí přídavného jména odvozeného od slova „kyberprostor“, v němž k útokům pachatelů dochází a který spojuje různorodé trestné činy z této oblasti, přičemž kromě počítače může trestnému činu dodávat onen „aspekt kybernetiky“ přítomnost jakéhokoliv jiného zařízení, které umí prostřednictvím protokolu komunikovat s jinými zařízeními[8], např. mobilního telefonu, tabletu apod.

1.2. Pojem pachatele

Při definování pachatele kybernetické kriminality bude pro účely této práce použito kriminologické pojetí pachatele, dle kterého se pachateli rozumí *„osoby, které se dopustily činů označených zákonem jako trestné činy, ale i některé osoby, které orgány činné v trestním řízení*

[6] srov. např. Kolouch, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016, s. 37.
[7] Gřivna, T., Scheinost M., Zoubková I. a kol., 2019, op. cit., s. 389.
[8] Smejkal, V. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, s. 19.

trestně nestíhají"[9]. Pachateli kybernetické kriminality mohou být jak fyzické, tak právnické osoby, přičemž požadavek na trestní odpovědnost právnických osob jako pachatelů kybernetické kriminality zakotvuje kromě českých právních předpisů také právní úprava Evropské unie[10]. Vzhledem k omezenému rozsahu této práce bude pozornost věnována pouze fyzickým osobám jako pachatelům kybernetické kriminality. Pokud se jedná o pachatele, který je fyzickou osobou, lze předpokládat, že pachateli mohou být nejen osoby dospělé, ale také mladiství a osoby trestně neodpovědné pro nedostatek věku, např. u trestných činů tzv. kyberšikany[11].

1.3. Pojem oběti

Pojem oběti je definován zákonem č. 45/2013 Sb., o obětech trestných činů a změně některých zákonů v § 2 odst. 2 (dále také jako „zákon o obětech trestných činů"), podle kterého se obětí 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"*. Tato definice odpovídá také kriminologickému členění různých forem viktimizace, o němž bude pojednáno v kapitole věnované obětem kybernetické kriminality. Dle odst. 3 téhož ustanovení zákona o obětech trestných činů se navíc v případě, že byla oběti trestným činem způsobena smrt považují, *„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",* z této definice vyplývá teoretické dělení obětí na oběti přímé (první kategorie) a nepřímé (druhá kategorie zahrnující pozůstalé oběti přímé). V této práci bude pozornost věnována pouze přímým obětem kybernetické kriminality.

Z různorodosti kriminálních jednání, kterých se pachatelé kybernetické kriminality dopouští, lze usuzovat na široké spektrum obětí kybernetické kriminality. Mezi oběťmi kybernetické kriminality pravděpodobně budou zastoupeny osoby různých věkových kategorií, úrovně vzdělání apod. Ve vztahu k některým druhům kybernetické kriminality se jeví jako vhodné upozornit také na institut zvláště zranitelné oběti, kterou definuje zákon o obětech trestných činů v § 2 odst. 4 jako osobu, která *„splňuje podmínky odst. 2 a 3 téhož zákona a zároveň je:*

[9] Gřivna, T., Scheinost M., Zoubková I. a kol., 2019, op. cit., s. 95.
[10] Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12.srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV, [online]. [cit. 2020-03-10]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32013L0040
[11] Smejkal, V., 2018, op. cit., s. 687.

- *dítětem;*
- *osobou vysokého věku nebo osobou s různými druhy postižení, pokud mohou tyto skutečnosti bránit jejímu úplnému a účelnému uplatnění ve společnosti;*
- *obětí trestného činu obchodování s lidmi nebo trestného činu teroristického útoku;*
- *obětí taxativně vyjmenovaných trestných činů (např. trestného činu proti lidské důstojnosti v sexuální oblasti, trestného činu, který zahrnoval nátlak, násilí či pohrůžku násilím, trestného činu spáchaného pro příslušnost k některému národu, rase, etnické skupině, náboženství, třídě nebo jiné skupině osob nebo oběť trestného činu spáchaného ve prospěch organizované zločinecké skupiny), jestliže je v konkrétním případě zvýšené nebezpečí způsobení druhotné újmy zejména s ohledem na její věk, pohlaví, rasu, národnost, sexuální orientaci, náboženské vyznání, zdravotní stav, rozumovou vyspělost, schopnost vyjadřovat se, životní situaci, v níž se nachází, nebo s ohledem na vztah k osobě podezřelé ze spáchání trestného činu nebo závislost na ní.“*

V následujících částech textu věnujících se konkrétním trestným činům z oblasti kybernetické kriminality bude věnována pozornost také otázce, zda a případně s jakou četností může kybernetický trestný čin zasáhnout také oběti označované jako tzv. zvláště zranitelné oběti.

2. Pachatel kybernetické kriminality

Hlavním cílem kriminologie při studiu pachatelů konkrétní trestné činnosti je vytvoření tzv. obrazu pachatele, založeného především na studiu jeho osobnosti, motivace a příslušnosti k určité sociální skupině[12]. Zjištění těchto skutečností umožňuje vysvětlit a pochopit jednání pachatele a zvolit vhodnou metodu jeho resocializace na základě individuálního přístupu. Pochopení osobnosti pachatele má význam také pro prevenci konkrétní trestné činnosti – pokud předem analyzujeme profil osob, u nichž existuje vyšší míra pravděpodobnosti, že se dopustí spáchání určité trestné činnosti, je možné na ně různými nástroji působit tak, aby bylo trestné činnosti předejito. Poznatky o osobnosti pachatele můžeme čerpat také z oblasti forenzní psychologie zaměřující se na osobnost konkrétních pachatelů zejména s ohledem na objasnění jejich motivace, která je rozhodující pro určení subjektivní stránky trestného činu[13].

Kybernetická kriminalita je označována za jeden z nejdynamičtějších druhů trestné činnosti, který je spojen se stále se zvyšujícím nápadem trestných činů [14] a současně s předpokladem vysoké míry latence tohoto druhu kriminality[15]. Hlavním důvodem rozvoje této trestné činnosti je bezesporu rychlý vývoj informačních a komunikačních technologií a s ním spojená dostupnost internetu pro velkou část světové populace, ale také přesun tradičních kriminálních jednání, ke kterým dříve docházelo pouze v tzv. off-line světě, do kyberprostoru (např. podvodů, stalkingu, mravnostní kriminality)[16].

Z klasifikace kybernetické kriminality (srov. kapitola 1.1.) je již na první pohled zřejmé, že jednání jejích pachatelů jsou velmi různorodá, a liší se nejen mezi jednotlivými kategoriemi, ale také v rámci jednotlivých kategorií. Proto se lze domnívat, že rovněž pachatelé této trestné činnosti představují z hlediska svých vlastností, motivů a dalších znaků velmi heterogenní skupinu. Stejně jako se zvyšuje počet kybernetických trestných činů a konkrétních forem této trestné činnosti, mění se také představa o profilu pachatele kybernetické kriminality. V následující části kapitoly bude pozornost věnována právě dřívějším představám a zjištěním o pachatelích kybernetické kriminality. Tyto představy budou následně komparovány s výsledky novějších výzkumů a názory současných autorů věnujících se studiu pachatelů kybernetické kriminality.

---

[12] Gřivna, T., Scheinost M., Zoubková I. a kol., 2019, op. cit., s. 95.
[13] Čírtková, L. *Forenzní psychologie*. 3., upr. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013, s. 80.
[14] Ministerstvo vnitra, *Zpráva o situaci v oblasti vnitřní bezpečnosti,* 2019, op. cit., s. 47.
[15] Smejkal, V. Kybernetická kriminalita – fenomén dneška. *Právní prostor.* [online]. 2015 [cit. 2020-03-10]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska
[16] Ministerstvo vnitra ČR. *Zpráva o situaci v oblasti vnitřní bezpečnosti,* 2019, op. cit., s. 47.

2.1. Vývoj představy o pachatelích kybernetické kriminality

Dle *Panzavolty* [17] byly poznatky a představy o pachatelích v době počátků kriminologických výzkumů o pachatelích kybernetické kriminality, tj. přibližně ve druhé polovině 80. let a v 90. letech, především tohoto charakteru:

- pachateli jsou vysoce inteligentní jedinci s odborným vzděláním nebo alespoň hlubším zájmem a znalostí informačních technologií;
- pachatelé se dopouštějí trestné činnosti jako jednotlivci (tj. trestné činy nejsou ve velké míře páchány v rámci organizované trestné činnosti);
- pachatelů kybernetické kriminality existuje poměrně malé množství i vzhledem k odbornosti nezbytné k provedení útoku (tutéž domněnku vyjadřoval rovněž *Clough* a odůvodňoval ji někdejší nižší dostupností informačních technologií – počítače a jiná podobná technická zařízení byla dříve užívána především ve výzkumu nebo byla přístupná pouze vládě a finančním institucím a *„schopnost dopustit se kybernetického trestného činu byla velmi omezena na osoby s přístupem k potřebným zařízením a potřebnou expertízou“* [18]);
- pachatelé nepředstavují vážnou hrozbu z hlediska rozsahu způsobené škody (kybernetická trestná činnost ve své tehdejší podobě nebyla vnímána jako tak závažná a také existovalo méně forem kybernetické kriminality).

Výše uvedené charakteristiky lze doplnit také dříve uznávaným názorem, že kybernetické útoky jsou páchány zejména mladými „počítačovými génii“, kteří testují své schopnosti a zjišťují, jakou škodu jsou schopni spáchat [19]. *Musil* navíc uvádí, že jeden z výzkumů zaměřených na pachatele počítačové kriminality provedený v roce 1992 prokázal, že pachateli jsou zejména programátoři, tj. pachatelé specialisté, oproti běžné populaci vzdělaní v oblasti informačních technologií [20]. Z výše uvedeného lze tedy usoudit, že stereotypem pachatele kybernetické kriminality byl dříve mladý pachatel disponující alespoň určitým stupněm vzdělání v oblasti informačních technologií a kybernetická kriminalita byla vnímána jako hrozba mnohem méně než v současné době.

[17] Přednášky a konzultace v rámci předmětu *Cybercrime* na Katholiek Universiteit Leuven vedeného profesorem Michelem Panzavoltou v letním semestru akademického roku 2018/2019.
[18] Clough, J., 2015, op. cit., s. 4.
[19] Csonka, P. *The council of Europe's convention on cyber-crime and other European initiatives*. Revue internationale de droit pénal, 2006, s. 476. Pozn. přístup k publikaci byl poskytnut v rámci studia předmětu Cybercrime na KU Leuven v letním semestru 2018/2019.
[20] Musil, S. *Počítačová kriminalita: nástin problematiky: kompendium názorů specialistů*. Praha: Institut pro kriminologii a sociální prevenci, 2000, s. 249; pozn.: k pojmu počítačová vs. kybernetická kriminalita srov. bod 1.1.

V současné době je však již známo výrazně větší množství forem kybernetické trestné činnosti, nápad tohoto druhu kriminality se prudce zvýšil a výše uvedené předpoklady byly novými kriminologickými výzkumy doplněny či pozměněny v tyto poznatky:

- pachatelé se často sdružují do organizovaných zločineckých skupin;
- internet poskytuje prostor k páchání široké a různorodé škály trestné činnosti (postupně přibývají různé formy kybernetické kriminality, kterých se pachatelé dopouští);
- škoda způsobená kybernetickými trestnými činy může být velmi vysoká a pachatelé představují i z důvodu aspektu jejich organizovanosti mnohem větší hrozbu než dříve[21];
- pachateli nejsou pouze osoby se vzděláním či zvláště pokročilými znalostmi v oblasti informačních technologií;
- trestných činů se často dopouští pachatelé jako profesionální hackeři, kyberteroristé nebo „kyberšpioni“, kteří jsou využívání a zaplaceni různými korporacemi nebo dokonce vládami[22].

Předně si lze všimnout, že oproti předchozím předpokladům je nyní jako poměrně relevantní aspekt kybernetické kriminality vnímána zvyšující se organizovanost pachatelů, která vytváří podmínky pro páchání stále závažnější trestné činnosti. Bylo pozorováno, že si v současné době pachatelé kybernetické kriminality vybírají cíle svých útoků tak, aby ze své činnosti získali stále větší profit[23]. Organizovanost pachatelů také ztěžuje již tak velmi nesnadné a specifické vyšetřování kybernetické kriminality.

Další změnu lze zaregistrovat v souvislosti s formami kybernetické kriminality. Bylo zaznamenáno, že kybernetická kriminalita podléhá tzv. trendům, to znamená, že v rámci jejího vývoje jsou evidovány stále nové formy této trestné činnosti, které se od jednoho pachatele následně rozšiřují k dalším. Pachatelé se konkrétní formy trestné činnosti dopouští v určitém souvislém období a v některých případech tyto formy kybernetické kriminality následně ustoupí novým druhům kybernetické kriminality[24]. *Europol* ve své Roční analýze rizik internetové trestné činnosti pro rok 2019 upozorňuje na to, že kybernetické trestné činy je vždy třeba vnímat v jejich určité *„present form“* čili současné podobě, ale zároveň je nutné mít na paměti rychlý vývoj této trestné činnosti a tzv. *„future projections“* čili potenciální nové formy

[21] Přednášky a konzultace v rámci předmětu Cybercrime na KU Leuven vedeného profesorem Michelem Panzavoltou v letním semestru akademického roku 2018/2019.
[22] Csonka, P., 2006, op. cit., s. 476.
[23] Europol. *Internet organised crime threat assessment 2019*, s. 4. [online]. [cit. 2020-03-10]. Dostupné z: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019
[24] Požár, J. Vybrané trendy kybernetické kriminality. *Acta Informatica Pragensia* [online]. 2015, 4 (3): 366-348. [cit. 2020-03-10]. Dostupné z: https://aip.vse.cz/pdfs/aip/2015/03/11.pdf

této trestné činnosti, se kterými se setkáme v budoucnu[25]. Lze se však domnívat, že predikovat vývoj forem kybernetické trestné činnosti vyžaduje mnoho znalostí jak z oblasti informačních technologií, tak práva a zůstává otázkou, zda je vůbec možné učinit odhad, který by odpovídal reálnému vývoji. Kybernetické trestné činy jsou tedy v důsledku jejich střídajících se trendů velmi obtížně preventabilní.

Třetí znak kybernetické kriminality, který je dnes vnímán oproti minulosti odlišně, lze spatřovat v charakteristice pachatele této trestné činnosti. Ten již není vnímán jako osoba nutně vzdělaná v oblasti informačních technologií, ale připouští se, že u některých forem kybernetické trestné činnosti nejsou žádné zvláštní znalosti pachatele v oblasti informačních technologií vyžadovány. Lze si představit například pachatele podvodů prostřednictvím e-mailu, kdy pachateli postačí uživatelská znalost počítače a elektronické komunikace. V následující části kapitoly bude pozornost upřena právě na bližší obecnou charakteristiku pachatelů kybernetické kriminality založenou na poznatcích současných výzkumů.

2.2. Obecná charakteristika pachatele kybernetické kriminality

Jak bylo uvedeno výše, formy kybernetické trestné činnosti jsou velmi různorodé, a proto lze předpokládat, že i spektrum pachatelů bude pestré. Právě z důvodu heterogennosti forem kybernetické trestné činnosti je třeba mít na paměti, že zjištěné údaje o pachatelích nemohou pravděpodobně dopadat na každého pachatele a při profilování pachatele je proto vhodnější pracovat s výsledky výzkumů zaměřených na konkrétní kybernetický trestný čin, pokud byly takové výzkumy provedeny.

Prvním znakem, na kterém se shoduje většina výzkumů, je pohlaví pachatele – pachatelem kybernetické kriminality je obvykle muž[26]. Lze soudit, že to může být zapříčiněno i skutečností, že dle statistik kriminality je stíhaných pachatelů mezi muži konstantně více než mezi ženami. Nelze však říci, že by byla oblast kybernetické kriminality doménou mužských pachatelů, ženy si lze v pozici pachatelek snadno představit např. u trestných činů kyberšikany či kyberstalkingu, ale také podvodů v podobě tzv. romance scams (viz dále bod 4.3.2.2.).

Kriminologické výzkumy se dále zaměřují na otázku věku pachatele, přičemž z jejich výsledků vyplývá, že nejčastějšími pachateli jsou osoby do věku 35 let[27]. Odhady se ovšem různí ve vztahu k odlišným formám kybernetické trestné činnosti, z policejních statistik

[25] Europol, 2019, op. cit., s. 6.
[26] Hadzhidimova, L. I., Payne, B. K. 2019. The profile of the international cyber offender in the U.S. *International Journal of Cybersecurity Intelligence & Cybercrime*: *2(1),* 40-55. [online]. [cit. 2020-05-22]. Dostupné z: https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1012&context=ijcic
[27] Válková, H., Kuchta J., Hulmáková J. a kol., 2019, op. cit. s. 527.

mapujících kybernetickou kriminalitu v období let 2011–2019 vyplývá, že např. u mravnostních trestných činů dochází k nárůstu podílu pachatelů nedosahujících věku 18 let, přičemž těchto pachatelů do 18 let věku je u mravnostních kybernetických trestných činů více než u ostatních kybernetických trestných činů dohromady[28]. Kriminalitu páchanou osobami nižšího věku lze přisuzovat zejména předpokládané pokročilejší úrovni jejich digitální gramotnosti, která je u nich pravděpodobně vyšší než například u seniorů. Lze však mít za to, že v následujících letech či desetiletích již nebude předpoklad o spíše nižším věku pachatele kybernetické kriminality na místě, jelikož většina průměrné populace bude disponovat alespoň základní úrovní digitální gramotnosti, která je nezbytná pro spáchání některého trestného činu z oblasti kybernetické kriminality.

Z hlediska vzdělání jsou pachatelé kybernetické kriminality dle statistik spíše inteligentní osoby s vyšším vzděláním. Vzhledem k tomu, že spáchání některých trestných činů z oblasti kybernetické kriminality vyžaduje pokročilou znalost v oboru informačních technologií (DDoS útoky, malware apod.), lze předpokládat, že potenciální pachatel bude příslušným vzděláním disponovat, existuje však řada jiných nelegálních praktik na internetu, např. podvodné e-maily, kyberstalking, pro které nejsou vyšší vzdělání či inteligence pachatele vyžadovány. Ve vztahu ke vzdělání a odborným znalostem lze pachatele členit na amatéry a profesionály[29] (dále také viz bod 2.3.2.).

Tři výše popsaná hlediska, tedy pohlaví, věk a vzdělání či odbornost pachatele, jsou jedinými hledisky, o kterých jsou v rámci kriminologických výzkumů kybernetické kriminality činěny obecné závěry. V dnešní době je totiž čím dál více zřejmé, že obecnou charakteristiku pachatele kybernetické kriminality není možné vytvořit[30]. To je zapříčiněno zejména výše popsaným množstvím forem této kriminality, kdy je zřejmé, že pachatelé se dopouští trestné činnosti s velmi rozmanitou motivací, ke spáchání různých trestných činů je potřeba různé vzdělání pachatelů apod., a tedy nelze generalizovat odhady o pravděpodobném věku, vzdělání, pohlaví, pohnutkách, duševním stavu pachatele a jiných jeho charakteristikách. Tuto skutečnost lze ilustrovat například komparací pachatele kybergroomingu, který prostřednictvím seznamky přesvědčuje nezletilé dítě k poskytnutí intimních fotografií a pachatele trestného činu porušení autorských práv. Už jen pravděpodobný motiv pachatelů je zcela odlišný, vedle sexuálního

[28] Centrum prevence rizikové virtuální komunikace. Statistika kybernetické kriminality za rok 2019. [online]. [cit. 2020-03-10]. Dostupné z: https://www.e-bezpeci.cz/index.php/z-jinych-webu/1749-statistika-kybernetricke-kriminality-za-rok-2019

[29] Gřivna, T., Scheinost M., Zoubková I. a kol., 2019, op. cit., s. 392.

[30] Gřivna, T., Scheinost M., Zoubková I. a kol., 2019, op. cit., s. 392, Válková, H., Kuchta J., Hulmáková J. a kol., 2019, op. cit., s. 606.

motivu stojí motiv majetkový a také ohledně osobnosti pachatelů bude pravděpodobně možné učinit zcela jiné závěry. Lze proto uzavřít, že v porovnání s obecnými výzkumy kybernetické kriminality se k naplnění cílů kriminologie jako vhodnější jeví zaměření výzkumné činnosti na pachatele konkrétních forem této trestné činnosti.

2.3. Kategorizace pachatelů kybernetické kriminality

Vytvoření obecné charakteristiky pachatele kybernetické kriminality je sice obtížné a jak bylo uzavřeno výše také téměř nemožné, v odborné literatuře se však setkáme alespoň s obecnou kategorizací pachatelů založenou na různých kritériích. Zařazení neznámého pachatele do určité kategorie osob, o nichž již existují konkrétní výzkumné poznatky může přispět k úspěšnosti vyšetřování. Také lze předpokládat, že pachatelé určité trestné činnosti dodržují podobné vzorce chování, což může být rovněž užitečné pro predikci jejich dalšího chování. Lze poznamenat, že jsou sestavovány také kategorizace pachatelů konkrétní trestné činnosti z oblasti kybernetické kriminality, např. pachatelů kyberstalkingu či nenávistných trestných činů (více viz kapitola 4.). V následující části této kapitoly budou představeny a analyzovány obecné kategorizace podle některých autorů věnujících se problematice kybernetické kriminality.

2.3.1. Kategorizace pachatelů kybernetické kriminality dle *Smejkala*

Kybernetická kriminalita je *Smejkalem* popisována jako tzv. „dematerializovaný zločin" – jedná se podle něj o trestné činy, které jsou založeny na nepoctivosti jejich pachatelů zneužívajících znalost počítačových systémů[31]. V následující části bude pozornost věnována jeho kategorizaci pachatelů kybernetické kriminality do šesti různých skupin, přičemž informace o těchto skupinách budou doplněny dalšími poznatky.

První skupinu představují tzv. pachatelé bílých límečků, tato kategorie vychází z klasické Sutherlandovy teorie o kriminalitě osob s vysokým sociálním statutem, které zneužívají svého postavení k páchání kriminality. Tito pachatelé jsou obvykle nadprůměrně inteligentní a jejich trestná činnost není spojena s násilím – dopouští se nejčastěji podvodů a nezákonných manipulací[32]. Lze si všimnout, že označení určité skupiny pachatelů kybernetické kriminality jako bílých límečků je zmiňováno napříč odbornou literaturou věnující se kybernetické kriminalitě[33]. Vyšší sociální postavení je pro pachatele příhodné zejména ve fázi

[31] Smejkal, V., 2018, op. cit., s. 688-689.
[32] Čírtková, L., 2013, op. cit., s. 282.
[33] Dvořák, M. Phishing, pharming a jejich trestněprávní postih. Trestněprávní revue 4/2018, s. 84. [online]. [cit. 2020-03-01]. Dostupné prostřednictvím https://www.beck-online.cz/, Požár, J., 2015, op. cit.

vyšetřování trestné činnosti, kdy v důsledku sociálních stereotypů představují skupinu osob, která není vždy na první pohled považována za podezřelou.

Druhou skupinu pachatelů tvoří tzv. průnikáři**,** osoby s patrnými anarchistickými rysy dopouštějící se zpravidla zavirování počítačů, průniků do vládních počítačových sítí a DDoS útoků. Tato kategorie pravděpodobně také nejvíce odpovídá původnímu stereotypu pachatele kybernetické kriminality, který byl popsán v části 2.1.

Třetí skupinou jsou organizovaní zločinci, kteří počítače využívají zejména ke skryté komunikaci, praní špinavých peněz, výrobě padělků a nelegálních druhů pornografie apod. Kvůli jejich organizovanosti je rozsah jejich trestné činnosti a zřejmě také výše škody jejich trestnou činností způsobená vyšší než u samostatných pachatelů. Pachatelé se sdružují do skupin za účelem páchání různé kybernetické trestné činnosti, doloženy jsou případy organizovanosti u hackingu, výroby a šíření malware, DDoS útoků, vydírání, trestných činů souvisejících s porušováním práv duševního vlastnictví, obchodování s lidmi, praní špinavých peněz[34] ale také např. kybergroomingu. Vyšetřování kybernetických trestných činů v rámci organizované kriminality je patrné také ze statistik Policie ČR a Národní centrály proti organizovanému zločinu[35]. Specifikům organizované trestné činnosti z oblasti kybernetické kriminality bude věnována část 2.6.

Čtvrtá skupina pachatelů je označována jako profesionálové, jejich činnost má podobu průniků do počítačových systémů, odhalování utajovaných informací apod., přičemž ji vykonávají profesionálně, tedy za účelem získání obživy. Lze se domnívat, že se u této skupiny pachatelů také často setkáme s jejich zapojením do organizované trestné činnosti.

Následující pátou skupinu představují tzv. kyberteroristé, pachatelé sofistikovaných útoků[36] při kterých k provedení útoku používají informační technologie. Kyberterorismus je novým a velmi nebezpečným fenoménem, jelikož pachatelé při svých útocích často cílí na významné informační systémy či systémy elektronických komunikací a jejich útok tak může mít výrazný dopad na velkou skupinu osob. *Kolouch* uvádí, že se pachatelé kyberteroristických útoků obvykle dopouští jako příslušníci malých skupin, které nejsou na rozdíl od tradičních teroristických skupin vojensky organizované[37]. Jedním z druhů kyberterorismu může být také

[34] United Nations Office On Drugs and Crime. *E4J University Module Series, Module 13: Cyber organized crime activities*. [online]. [cit. 2020-03-01]. Dostupné z: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html

[35] Policie ČR. Statistika kyberkriminality. *Zveřejněné informace 2019.* [online]. [cit. 2020-03-12]. Dostupné z: https://www.policie.cz/clanek/statistika-kyberkriminality.aspx

[36] Kuchta, J. *Aktuální problémy počítačové kriminality včetně její prevence*. Časopis pro právní vědu a praxi 1/2016, s. 5. [online]. [cit. 2020-03-01]. Dostupné prostřednictvím https://www.beck-online.cz/

[37] Kolouch, J., 2016, op. cit., s. 323.

tzv. kybernetická válka, kdy se v postavení pachatelů kybernetických útoků mohou objevit státy[38]. I vzhledem k této skutečnosti lze předpokládat, že motivace pachatelů – kyberteroristů – může být velmi specifická, např. nábožensky či politicky orientovaná.

Šestá a poslední skupina je nazvána jako osoby nepřemýšlející o svém jednání a následcích a jedná se osoby zpravidla blízké věku dětí a mladistvých, neuvědomující nebo nepřipouštějící si trestnost svého jednání. Lze se domnívat, že do této skupiny budou patřit například pachatelé trestných činů spočívajících v porušování autorských práv, pachatelé kybergroomingu a v některých případech i např. osoby podílející se na šíření poplašných zpráv.

Tato podrobná kategorizace podporuje tvrzení, že pachatelé tvoří velmi pestrou skupinu. Je možné se setkat s osobami vysoce postavenými a uznávanými, a naopak s osobami s kontroverzními anarchistickými sklony. Organizované zločinecké skupiny jsou vyčleněny samostatně, což jen podtrhuje závažnost a specifičnost jejich trestné činnosti. Navíc se lze domnívat, že velké množství pachatelů pokryje poslední šestá kategorie, jelikož vzhledem k tomu, že internet poskytuje pachateli anonymní prostředí, pachatel si velmi často neuvědomuje možné následky svého jednání.

Kromě výše uvedené kategorizace lze uvést jinou *Smejkalovu* kategorizaci pachatelů, kterou formuloval dříve v rámci své publikační činnosti:

a) cizí státy vedoucí tzv. kybernetickou válku,
b) teroristé,
c) zaměstnanci zneužívající přístup k určitým informacím nebo zařízení k páchání trestné činnosti.
d) organizované skupiny[39].

Lze si povšimnout, že ve srovnání s první kategorizací zde *Smejkal* upozorňuje na mezinárodněprávní aspekty kybernetické kriminality, která může být v mezinárodních vztazích využívána jako politický nástroj a její projevy je dle mezinárodního práva veřejného možné chápat jako zásahy do suverenity států či porušení zákazu použití síly v mezinárodním právu[40]. Tento aspekt kybernetické kriminality jiní autoři v kategorizace samostatně obvykle nezmiňují. Lze se domnívat, že jej mohou vnímat jako podkategorii pachatelů – teroristů, ale ani v takovém případě by nevystihovali veškeré formy mezinárodní kybernetické kriminality, jelikož se nemusí vyskytovat pouze ve formě klasifikované jako terorismus. Lze předpokládat, že druhá

[38] Smejkal, V. in Jelínek, J. *Terorismus-základní otázky trestního práva a kriminologie*. Praha: Leges, 2017, s. 90.
[39] Smejkal, V., 2015, op. cit.
[40] Přednáška Mgr. Tomáše Brunera v rámci povinně volitelného předmětu Kybernetické kriminality a kybernetické bezpečnosti v zimním semestru 2019/2020.

Smejkalova kategorizace může být pro určité základní vymezení pachatelů užitečná, nejedná se však o kategorizaci komplexní, která by postihovala veškeré formy kybernetické kriminality. Individuální pachatele pokrývá v zásadě jen třetí skupina – zaměstnanci – přičemž se lze domnívat, že se bude jednat zejména o trestné činy spočívající ve zneužití přístupu do počítačového systému nebo informací, které mají díky své pracovní pozici zaměstnanci k dispozici, a tedy některé kybernetické trestné činy zůstanou zcela stranou této kategorizace, např. mravnostní kriminalita, nenávistné trestné činy a další.

2.3.2. Kategorizace dle *Kuchty*

Dělení pachatelů na amatéry a profesionály dle *Kuchty* je založeno na jejich vztahu k informacím, které jsou předmětem trestné činnosti. Za profesionály jsou označeny osoby zneužívající přístup k informacím či počítačovým systémům, který mají k dispozici obvykle díky svému zaměstnání. Trestnou činnost provádí s motivem majetkového zisku, jde většinou o zaměstnance, konkrétně pracovníky managementu nebo programátory. Naopak skupinu amatérů představují osoby, které do informačních systémů pronikají náhodně bez předchozích informací nebo přístupů k těmto systémům. Vedle těchto skupin zmiňuje zřejmě k jejich specifické motivaci autor teroristy[41]. Lze si všimnout, že označení profesionálové používá v rámci své první klasifikace také *Smejkal* (bod 2.3.2.), avšak k popisu pachatelů, kteří kybernetickou kriminalitu páchají profesionálně, tedy za odměnu pro jiné osoby. Skupina profesionálů podle *Kuchtovy* kategorizace však obsahově koresponduje s druhým *Smejkalovým* dělením, a to se skupinou zaměstnanců (bod 2.3.2.). Vedle těchto skupin zmiňuje zřejmě k jejich specifické motivaci autor teroristy. Jakkoliv se toto dělení může jevit jako poměrně jednoduché, lze se domnívat, že může být užitečným vodítkem například pro určení základní motivace pachatele.

2.4. Kriminogenní faktory kybernetické kriminality

Kriminogenní faktory neboli činitelé přispívající ke kybernetické kriminalitě se částečně překrývají s těmi, které můžeme pozorovat u jiných druhů trestné činnosti. Těmito shodnými faktory je zejména touha po snadném nabytí majetku, absence morálních hodnot, zhroucení životních cílů, zlehčování a tolerance některých jednání ze strany veřejnosti; zlehčování veřejností je patrné zejména u trestných činů souvisejících s porušováním autorských práv, kdy se lidé většinou nad nahráváním nelegálně získaných autorských děl ani nepozastaví a sami je

[41] Válková, H., Kuchta J. Hulmáková J. a kol., 2019, op. cit., s. 528.

využívají[42]. Na rozdíl od jiných druhů kriminality se u kybernetické trestné činnosti nesetkáme s kriminogenními faktory spočívajícími v původu pachatele ze sociálně vyloučené oblasti, špatných či absentujících rodinných vztazích nebo například předchozí trestné činnosti[43].

Kriminogenními faktory, které však byly oproti jiným druhům trestné činnosti ve vyšší míře identifikovány speciálně u kybernetické kriminality jsou jimi patrně zejména:

a) vysoká míra latence: předpokládá se, že velká část trestné činnosti zůstává nezjištěna a nestane se tak ani předmětem trestního stíhání; příčiny tohoto jevu budou zkoumány v bodu 3.1.[44];
b) charakteristická motivace pachatele: viz níže bod 2.5.;
c) pomalu reagující legislativa: jak bylo popsáno výše, kybernetická kriminalita se dynamicky rozvíjí a velmi rychle přibývá nových forem jednání, kterých se pachatelé dopouští, proto v praxi nelze vyloučit situaci, kdy legislativa daný problém vůbec neřeší nebo není vůči konkrétnímu nelegálnímu jednání úplně přiléhavá;
d) příležitosti k organizovanosti pachatelů: viz níže bod 2.6.,
e) anonymita pachatele a pravděpodobná vyšší míra tzv. nevztahových deliktů: viz kapitola 3.3.2.
f) dostupnost internetu a počítačových zařízení: pachatelem alespoň některých kybernetických trestných činů může být prakticky kdokoliv, není třeba mít určité finanční prostředky a vzdělání[45].

Následující část textu bude věnována otázce motivace pachatele kybernetické trestné činnosti, která v některých případech může korespondovat s motivací pachatelů odlišné trestné činnosti, ale také může být zcela specifická právě pro kybernetickou trestnou činnost.

2.5. Motivace pachatelů kybernetické trestné činnosti

Motivace pachatelů kybernetické trestné činnosti je i vzhledem k rozmanitým formám jejich jednání velmi různorodá a závisí obvykle na věku, osobnosti a příležitostech. Naopak technické dovednosti a znalosti nejsou pro motivaci tolik rozhodující[46]. U jednoho pachatele se nejspíše můžeme setkat i s kombinací několika druhů motivace. Tak např. pachatel kybergroomingu získávající při své činnosti pornografický materiál, který se rozhodne později

[42] Kuchta, J., 2016, op. cit., s. 548.
[43] Idem.
[44] Gřivna, T., Scheinost M., Zoubková I. a kol.: op. cit., s. 391.
[45] Kuchta, J., 2016, op. cit., s. 549-550.
[46] Smejkal, V., 2018, op. cit., s. 687.

šířit, bude pravděpodobně motivován jak svým vlastním sexuálním uspokojením, tak vidinou zisku finančních prostředků.

Dle *Kuchty* je za převažující motivaci u pachatelů považována touha po zisku, pomsta (např. u kyberstalkingu [47]), euforie z pocitu beztrestnosti či neodhalitelnosti, touha po dobrodružství vyvolaná u pachatele anonymitou, kterou internet nabízí. Pachatelé mravnostní kriminality jsou motivováni vlastním sexuálním uspokojením.

Se zvláštní motivací se můžeme setkat u pachatelů – zaměstnanců, kteří se jako pachatelé vyskytují v rámci výše diskutovaných kategorizací. Jelikož jejich trestná činnost pramení z příležitostí, které jim poskytuje zaměstnání, mohou být k této činnosti motivováni právě také důvody souvisejícími se zaměstnáním, např. pocitem převahy nad zaměstnavatelem nebo názorem, že firmě nemohou uškodit malé ztráty[48]. *Požár* vyslovuje obavu z nebezpečí spočívajícím právě v lidském faktoru. Dle jeho názoru je třeba zapojit nástroje prevence ve vnitřních strukturách společností, jelikož největší riziko kybernetické kriminality hrozí právě ze strany skupiny disponující citlivými informacemi či přístupy k těmto informacím, tedy především zaměstnanců, administrátorů a podobných osob[49].

Specifická může být také motivace pachatelů dopouštějících se trestné činnosti spočívající v porušování autorského práva. Ti jsou nejčastěji motivováni ziskem z nelegální činnosti, případně zcela zvláštním cílem, který ve svých očích vnímají jako vznešený a sami sebe ani nepovažují za zločince. *Završnik* hovoří o tzv. hackerské kultuře, která prosazuje „volně dostupný software“ a „základní lidské právo na svobodu komunikace a používání software“[50].

V neposlední řadě je v oblasti kriminologických výzkumů velká pozornost věnována motivaci pachatelů kyberšikany, kterou je ve většině případů touha po „zábavě“ pramenící z pocitu nudy, přičemž touha pachatele způsobit oběti újmu nemusí být vůbec přítomna nebo může být pouze okrajovým faktorem motivujícím pachatele k jeho činu. Lze se domnívat, že tato skutečnost bude způsobena i často nízkým věkem pachatelů, kdy kyberšikana je častá u dětí a adolescentů, kteří si nemusí plně uvědomovat následky svého jednání[51].

---

[47] Vakhitova, Z. a kol. Offender – victim relationship and offender motivation in the context of indirect cyber abuse: A mixed-method explanatory analysis. *International review of Victimology 2018*, Vol. 24(3) 347-366. [online]. [cit. 2020-03-02]. Dostupné z: https://www.researchgate.net/publication/321000126_Offender-Victim_Relationship_and_Offender_Motivation_in_the_Context_of_Indirect_Cyber_Abuse_A_Mixed-Method_Exploratory_Analysis

[48] Smejkal, V., 2018, op. cit. sub 3, s. 688.

[49] Požár J., 2015, op. cit.

[50] Završnik, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017, s. 12-13.

[51] Hamuddin, B., Syahdan, S., Rahman, F., Rianita, D., Derin, T. Do They Truly Intend to Harm Their Friends?: The Motives Beyond Cyberbullying among University Students. *International Journal of Cyber Behavior,*

2.6. Organizovaná trestná činnost

Jak bylo uvedeno výše (viz bod 2.1.), pachatelé se ke kybernetické trestné činnosti často sdružují do organizovaných zločineckých skupin. Těmi se dle § 129 zákona č. 40/2009 Sb., trestního zákoníku, rozumí společenství alespoň tří trestně odpovědných osob s vnitřní organizací a strukturou, rozdělením funkcí a dělbou činností, které je zaměřeno na soustavné páchání trestné činnosti. Organizované zločinecké skupiny zmiňuje v rámci typologie pachatelů např. *Smejkal*[52], který je označuje za „nejčastější „uživatele" výnosů páchání kybernetické kriminality". V praxi můžeme identifikovat dva typy organizovaných zločineckých skupin z oblasti kybernetické kriminality:

a) kybernetická trestná činnost je primární činností organizované zločinecké skupiny: pachatelé se zaměřují pouze na páchání této trestné činnosti,
b) kybernetická trestná činnost je sekundární činností této skupiny: tedy je páchána za účelem praní špinavých peněz a uskutečňování převodů majetku získaných jinou trestnou činností a další činnosti[53] .

Lze doplnit, že organizované zločinecké skupiny se mohou trestné činnosti dopouštět na základě motivace vlastní či tzv. „na objednávku". Jedná se o model pojmenovaný *Europolem* jako tzv. *„crime-as-a-service model"*, přičemž na základě tohoto modelu je kybernetická trestná činnost páchána pro jiné osoby, které by samy nebyly schopny z důvodu technologické neznalosti tyto činy spáchat[54].

Otázkou zůstává, proč je právě pro pachatele kybernetické kriminality jejich organizovanost tak typická. Lze se domnívat, že pachatelé právě díky provázanosti internetu a možnostem rychlého vyhledání kontaktů a komunikace velmi jednoduše naleznou osoby s podobným cílem. S těmito osobami si mohou snadno vyměňovat zkušenosti a znalosti z oblasti kybernetické kriminality a mohou se také „spojit" za účelem spáchání závažnějšího trestného činu, než kterého by se dopustili samostatně[55]. K navázání kontaktů může sloužit zejména tzv. dark web nebo uzavřené diskuzní skupiny, a proto není v rámci vyšetřování jejich spolupráce organizované skupiny jednoduché odhalit.

Členové organizovaných zločineckých skupin navíc využívají pro páchání trestné činnosti odlišnosti v legislativě různých států a pro „základnu" svých aktivit často volí státy,

Psychology and Learning (IJCBPL), 2019, 9(4), 32-44. doi:10.4018/IJCBPL.2019100103. [online]. [cit. 2020-05-22]. Dostupné z: https://www-igi-global-com.ezproxy.is.cuni.cz/gateway/article/full-text-html/241849.
[52] Smejkal, V., 2015, op. cit.
[53] Idem.
[54] Europol, 2019, op. cit., s. 23.
[55] Clough, J., 2015, op. cit., s. 5.

jejichž legislativu považují za slabou a pro jejich aktivity nejvíce výhodnou a tolerantní[56]. Lze se domnívat, že právě z tohoto důvodu by bylo velmi vhodné zvýšit v oblasti kybernetické kriminality úroveň mezinárodní spolupráce tak, aby byly ještě více přiblíženy definice skutkových podstat kybernetických trestných činů a také aby byly vyjasněny podmínky jurisdikce a trestního stíhání ze strany jednotlivých států. Vzhledem k neomezené a neohraničené povaze kyberprostoru se však nejedná o jednoduchý úkol.

2.6.1. Odlišnosti organizované kybernetické trestné činnosti

Organizované zločinecké skupiny dopouštějící se kyberkriminality vykazují oproti organizovaným zločineckým skupinám z jiných oblastí kriminality několik odlišností, jejichž znalost může být užitečná při vyšetřování. *Nurse* a *Bada* popsali charakteristické odlišnosti organizované zločinecké skupiny, se kterými se setkáme u pachatelů hackingu, lze však dovozovat, že alespoň znaky uvedené pod písmeny a) a c) je možné vztáhnout také na jiné případy organizované kybernetické kriminality, např. kybergrooming, naopak se znakem dle písmene b) by bylo možné se setkat například u trestných činů spočívajících v zásazích do autorského práva (srov. bod 2.5.):

a) rozdělení rolí v rámci skupiny je méně patrné, skupina nemusí mít konkrétního vůdce;
b) aktivity skupiny mohou být založeny na motivu, který je veřejností vnímán jako „ušlechtilý, a tedy společenský přijatelný“ a ospravedlnitelný (jako příklad autoři uvádí útok organizované skupiny proti Islámskému státu);
c) vzhledem k povaze internetu jako platformy k páchání trestné činnosti je typické rozmístění pachatelů bez geografického omezení a s ním spojená skutečnost, že se může jednat o pachatele, kteří se seznámili prostřednictvím internetu a nikdy se nesetkali[57].

Vyšší tendence k organizovanosti pachatelů byly zaznamenány např. u pachatelů kybergroomingu, kteří se často sdružují za účelem spolupráce zejména pokud je jejich motivací sexuální zneužívání dětí nebo výroba dětské pornografie. Bylo zjištěno, že pachatelé této trestné činnosti si vytváří online databáze se sdílenými informacemi o dětských obětech trestných činů[58].

[56] De Hert, P., González-Fuster G., Koops, B. *Fighting cybercrime in the two Europes. The added value of the EU framework decision and The Council of Europe Convention.* International Review of Penal law (Vol. 77), 2006, s. 518.
[57] Nurse, J. R.C., Bada, M. *The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations*. [online]. [cit. 2020-03-02]. Dostupné z: https://arxiv.org/pdf/1901.01914.pdf.
[58] Kopecký, K. *Kybergrooming. Nebezpečí kyberprostoru (studie),* 2010, s. 8. [online]. [cit. 2020-03-10]. Dostupné z: http://e-nebezpeci.cz/

Závěrem

Z výsledků kriminologických výzkumů zaměřených na obecnou charakteristiku pachatele kybernetické kriminality vyplývá, že vytvoření takové charakteristiky znemožňuje různorodost nelegálních jednání, která jsou za kybernetickou kriminalitu považována. Jako užitečnější pro účely prevence a represe se tak jeví výzkum charakteristických znaků pachatelů jednotlivých kybernetických trestných činů, kterým bude věnována čtvrtá část práce. Lze se však domnívat, že poměrně užitečnou pomůcku pro praxi představují rovněž obecné kategorizace pachatelů kybernetické kriminality, které byly popsány v této části práce, jelikož umožňují pachatelovo jednání lépe popsat v rámci příslušné skupiny. Současně lze předpokládat, že vzhledem k tomu, že se pachatelé velké části kybernetické kriminality dopouštějí v rámci organizovaných zločineckých skupin, jsou poznatky o specifících těchto skupin pro praxi rovněž velmi přínosné.

3. Oběti kybernetické kriminality

Viktimologie je poměrně mladým podoborem kriminologie, který se zaměřuje na trestný čin z perspektivy jeho oběti. Právě z toho důvodu, že k rozvoji viktimologie došlo až v 50. letech dvacátého století[59], je pochopitelné, že viktimologie věnující se konkrétně obětem kybernetické kriminality je teprve v počátcích. Viktimologie zkoumá vlastnosti oběti, vztah mezi obětí a pachatelem, proces viktimizace, roli oběti v procesu odhalování, vyšetřování a soudního projednávání věci, pomoc oběti a ochranu občanů před viktimizací. Poznatky viktimologie umožňují lépe pochopit situaci, v níž se po spáchání trestného činu oběť nachází a zvolit nejvhodnější přístup k oběti zahrnující v některých případech i poskytnutí psychologické pomoci. Poznatky viktimologie jsou významné také pro prevenci trestné činnosti – na základě zjištěných viktimogenních faktorů je možné adresovat nástroje prevence nejvíce ohroženým skupinám osob[60]. První část této kapitoly bude věnována problematice latence kybernetické kriminality, přičemž bližší pozornost bude upřena k důvodům nenahlašování této trestné činnosti ze strany jejích obětí. V dalších částech kapitoly budou zkoumány dopady kybernetické kriminality na oběť, osobnost oběti a vztah oběti a pachatele.

3.1. Problematika latence kybernetické kriminality

Jedním ze základních kriminogenních faktorů kybernetické kriminality popsaných v bodu 2.4. je předpokládaná vysoká míra latence, která je důvodem toho, že statistiky zaznamenávající kybernetickou kriminalitu pravděpodobně neposkytují přesný a důvěryhodný obraz této kriminality. Lze soudit, že této problematice je třeba v souvislosti s viktimologií věnovat zvýšenou pozornost, jelikož v důsledku latence zůstává velké množství trestných činů neobjasněno a mnohým obětem tak není poskytnuta potřebná pomoc ani náhrada škody či nemajetkové újmy. Dalším důvodem zkoumání latence v rámci viktimologie je skutečnost, že právě oběti mohou svým jednáním spočívajícím v nenahlašování trestné činnosti, přispívat ke zkreslení statistických dat o této kriminalitě (viz bod 4.1.1.). V praxi se setkáme s několika možnými příčinami více či méně přispívajícími k latenci kybernetické kriminality. Jejich identifikace je zároveň východiskem pro jejich eliminaci, která může vést k vytvoření reálnějšího obrazu o kybernetické kriminalitě, a tedy i ke zvýšení účinnosti prevence a represe.

Dle *Clougha* je jednou z hlavních příčin zkreslení statistik o kybernetické kriminalitě ve vnitrostátním měřítku skutečnost, že v některých případech policie tyto trestné činy eviduje

[59] Marešová, A. Martinková M. O významu poznávání obětí trestné činnosti. Ministerstvo vnitra ČR. [online]. [cit. 2020-05-22]. Ke stažení: https://www.mvcr.cz/clanek/o-vyznamu-poznavani-obeti-trestne-cinnosti.aspx
[60] Gřivna, T., Scheinost M., Zoubková I. a kol., 2019, op. cit., s. 122.

jako některé z tradičních trestných činů, tedy jako např. podvody, aniž by specifikovala, že se jedná o trestné činy spáchané prostřednictvím internetu. Tuto příčinu lze pravděpodobně vnímat jako nejsnáze řešitelnou, a to řádným poučením osob evidujících kriminalitu dle jejích jednotlivých druhů. Lze doplnit, že problém zkreslení statistik je identifikován také v mezinárodním měřítku, přičemž hlavní příčina tohoto zkreslení tkví v odlišnostech ve vnitrostátních definicích skutkových podstat kybernetické kriminality jednotlivých států, které způsobují, že je velmi obtížné vytvořit souhrnnou evropskou či globální statistiku této kriminality[61].

Dalším z faktorů přispívajících ke zkreslení statistik je vliv médií, které tendují k informování pouze o ojedinělých, avšak zajímavých a šokujících případech kybernetické kriminality a neupozorňují na běžné, ale ve skutečnosti mnohem častější jevy[62]. Je vhodné poznamenat, že vliv médií je v souvislosti s viktimologií vnímán jako problematický i z dalších důvodů. Média se často podílí na šíření poplašných zpráv, zkreslují informace, které ovlivňují jednání veřejnosti a nadměrným upozorňováním na některé moderní fenomény mohou také u některých jedinců vyvolat tzv. syndrom falešné viktimizace, který byl popsán např. u stalkingu (včetně jeho varianty páchané prostřednictvím internetu)[63].

Jak bylo uvedeno výše, latence kybernetické kriminality může být v neposlední řadě zapříčiněna neoznamováním kybernetické trestné činnosti ze strany jejích obětí. Právě tato problematika bude v následující části textu blíže popsána.

3.1.1. Neoznamování kybernetické trestné činnosti

Ačkoli by se tato skutečnost mohla jevit jako paradoxní, jednu z hlavních příčin přispívajících zřejmě ve velké míře k latenci kybernetické kriminality představuje neoznamování této trestné činnosti jejími oběťmi. Důvody neoznamování trestné činnosti mohou pramenit z nevědomosti oběti, ale často jsou také ryze psychologického charakteru. Lze se setkat především s těmito důvody:

[61] Většina evropských stát a další světové státy sice přistoupily k mezinárodněprávním dokumentům, které upravují kybernetickou kriminalitu (zejména Budapešťská úmluva sjednaná Radou Evropy), pokud se však jedná o skutkové podstaty trestných činů, nastavují tyto dokumenty obvykle pouze minimální standardy jednání, které jsou státy zavázány trestně stíhat, v důsledku čehož se výsledné vnitrostátní právní úpravy mezi sebou liší; Clough, J., 2015, op. cit., s. 15.
[62] Clough, J., 2015, op. cit., s. 15.
[63] Čírtková, L., 2013, op. cit., s. 140, přednášky doc. PhDr. Ludmily Čírtkové, CSc. v rámci předmětu Soudní psychologie v zimním semestru akademického roku 2019/2020.

a) oběť si neuvědomuje, že se stala obětí trestného činu (typické pro některé případy majetkové kriminality, kdy např. pachatel čerpá z účtu oběti jednorázově či postupně velmi malé částky, přičemž oběť toto jednání nezaznamená)[64];
b) poškozený[65] má osobní zájem na utajení trestné činnosti (je-li v postavení poškozeného např. banka, pojišťovna či jiná finanční instituce, nenahlašuje trestný čin *„z obavy, že by se o jejich problémech se zabezpečením systému dozvěděla veřejnost a ztratily by důvěryhodnost*“[66], hypoteticky by z podobného důvodu mohly zatajit skutečnost, že se staly terčem kybernetického útoku například i státní instituce, které by nechtěly ztratit důvěru občanů v úroveň zabezpečení, které zajišťují);
c) oběť se obává publicity případu a případně s ní spojené sekundární viktimizace (lze předpokládat zejména u mravnostní kriminality a kyberšikany, kdy může být pro oběť velmi obtížné svěřit se jiné osobě s tak citlivým tématem, natož aby riskovala, že se o jednání dozví další osoby)[67];
d) oběť problém bagatelizuje (pravděpodobně především v případě trestných činů majetkových, kdy škoda způsobená oběti nedosahuje dle jejího subjektivního vnímání příliš vysoké částky);
e) oběť nemá důvěru v policii a její schopnost případ úspěšně vyřešit[68] (lze se domnívat, že výskyt této příčiny bude častější v některých státech či oblastech, kde je důvěra jejich obyvatel v orgány činné v trestním řízení velmi nízká, naopak v jiných státech či oblastech tato příčina nebude zaznamenána vůbec);
f) oběť zažívá pocit studu, nechce přiznat, že se „nechala napálit“[69] (pravděpodobně zvláště u obětí podvodů na internetu či podvodných e-mailů);

[64] Kuchta J., 2016, op. cit., s. 5., Clough, J., 2015, op. cit. s. 14.
[65] Pozn.: V tomto případě je namísto pojmu oběti použit pojem poškozený, jelikož obětí mohou být dle zákona o obětech trestných činů pouze fyzické osoby, naopak poškozeným ve smyslu § 43 zákona č. 141/1961 Sb., trestního řádu, může být také právnická osoba (jedná se pouze o jeden z několika rozdílů mezi pojmy poškozeného a oběti). Ačkoli je tato diplomová práce zaměřena primárně na oběti trestné činnosti, vzhledem k zachycení co nejvíce důvodů neoznamování trestné činnosti lze považovat za vhodné upozornit i na možné důvody na straně právnických osob, a to právě například bank nebo jiných finančních institucí, jelikož ty mohou být terčem kybernetických útoků velmi často. Lze se domnívat, že na pojem poškozený lze odkázat právě u tohoto důvodu nenahlašování kybernetické kriminality pod bodem b), lze si však představit, že pokud jde o důvody pod písm. a), d), e), h), mohla by být v pozici poškozeného také právě osoba právnická, nikoli pouze fyzická.
[66] Smejkal, V., 2018, op. cit., s. 705, Završnik, A., 2017, op. cit., s. 48.
[67] European Crime Prevention Network. *Cybercrime: A theoretical overview of the growing digital threat,* 2016, Brusel. [online]. [cit. 2020-03-07]. Dostupné z: https://eucpn.org/sites/default/files/document/files/theoretical_paper_cybercrime_.pdf; Clough, J., 2015, op. cit., s. 14.
[68] Smejkal, V. 2018, op. cit., s. 705.
[69] Roubalová a kol., 2019, op. cit., s. 93.

g) oběť neví, jak v dané situaci adekvátně reagovat či z důvodu neznalosti není schopna vyhodnotit, že se stala obětí trestného činu[70] (pravděpodobně časté u dětských obětí);
h) oběť považuje nahlášení trestného činu a následnou nutnou spolupráci s policií při vyšetřování za zbytečnou námahu (lze se domnívat, že se bude jednat opět zejména o případy, kdy oběť škodu způsobenou trestným činem nevnímá jako likvidační, jinak by ji ani nedůvěra ve schopnosti orgánů činných v trestním řízení od nahlášení trestného činu pravděpodobně neodradila; také se tato příčina může částečně překrývat s příčinou pod písmenem e), tj. příčinou spojenou s nedůvěrou v policii)[71].

Z výše uvedeného přehledu je patrné, že některé z důvodů mají původ pouze v nedostatečné informovanosti obětí jako uživatelů informačních technologií a bylo by zřejmě možné eliminovat je zvýšením povědomí o bezpečném chování na internetu. Potenciálním obětem je třeba zejména doporučit, aby zvýšily pozornost při provádění plateb přes internet a také kontrolovaly pohyby na svých bankovních účtech tak, aby byly schopny odhalit, že došlo ke spáchání trestného činu. Jako důležité se zdá také rovněž upozornit oběti na skutečnost, že ačkoli mohou subjektivně škodu jim způsobenou pociťovat jako bagatelní, kybernetickou trestnou činnost nelze vnímat izolovaně, ale v rámci možné rozsáhlé činnosti pachatelů nebo dokonce jejich organizovaných skupin, a proto i oznámením trestných činů způsobujících bezvýznamnou škodu mohou oběti přispět k odhalení závažné trestné činnosti. Můžeme poznamenat, že každý druh trestné činnosti vykazuje v otázce latence konkrétní odlišnosti, které mohou mít příčinu ve specifických kategorie obětí touto trestnou činností zasažených (např. jedná-li se o dětské oběti, mohou mít pravděpodobně jiné důvody pro nenahlašování trestné činnosti než senioři).

Na závěr lze doplnit, že kromě problematiky tzv. *„under-reporting“* (nedostatečného oznamování této trestné činnosti) upozorňují někteří autoři také na problematiku tzv. *„over-reporting“*. Jedná se o případy, kdy se oběti mylně domnívají, že se staly obětí kybernetické kriminality a tyto případy nahlašují orgánům činným v trestním řízení. *Završnik* tento jev popisuje jako tzv. „kybernetickou hypochondrii“, kdy *„uživatelé příliš často připisují chybné fungování terminálových zařízení škodlivému softwaru, ačkoliv je chybná funkce pouze důsledkem uživatelovy nedostatečné znalosti fungování zařízení“*[72].

[70] Roubalová a kol., 2019, op. cit., s. 93., Clough, J., 2015, op. cit. sub 1, s. 14.
[71] Roubalová a kol., 2019, op. cit., s. 145.
[72] Završnik, A., 2017, op. cit., s. 48.

3.2. Viktimizace

Následující část kapitoly bude zaměřena na viktimizaci – klíčový pojem viktimologie – a její jednotlivé druhy. Pojem viktimizace označuje proces, při němž se z potenciální oběti stává oběť reálná, přičemž viktimologie zkoumá v souvislosti s tímto procesem především vztah pachatele a oběti, chování oběti a tzv. míru viktimnosti, kterou se rozumí stupeň pravděpodobnosti rizika, že se konkrétní osoba stane obětí trestného činu[73]. V právní teorii se setkáme s klasifikací na primární a sekundární fázi viktimizace založené na rozlišování podnětů, které ji způsobují. Zatímco primární viktimizace představuje újmu způsobenou oběti bezprostředně trestným činem, sekundární viktimizace spočívá v újmě způsobené oběti různými činiteli až po spáchání trestného činu. V odborné literatuře se můžeme setkat také s pojmem terciární viktimizace, která je charakterizována jako stav trvalejšího rázu, kdy oběť není schopna se se zkušeností s trestným činem adekvátně vyrovnat, ačkoli již byla zjednána náprava (např. v podobě odsouzení pachatele a poskytnutí náhrady škody či nemajetkové újmy oběti)[74]. Současně lze doplnit, že ne všechny oběti prožívají všechny fáze viktimizace a také projevy a intenzita jednotlivých fází viktimizace se může u obětí lišit v závislosti na různých faktorech včetně osobnosti oběti, druhu konkrétní trestné činnosti a například způsobu spáchání trestného činu.

3.2.1. Primární viktimizace

K primární viktimizaci dochází u obětí bezprostředně v důsledku spáchání trestného činu, tedy nezávisle na skutečnostech po trestném činu následujících, původcem způsobené újmy je tedy pachatel, případně jeho spolupachatelé. Projevy primární viktimizace jsou nazývány jako tzv. primární rány a mohou být trojího druhu:

a) finanční (majetková) újma,
b) emocionální (psychická) újma,
c) fyzická újma[75].

Lze předpokládat, že oběti kybernetické kriminality mohou být vystaveny téměř všem projevům primární viktimizace vyjma fyzické újmy. Finanční újma může vzniknout např. v souvislosti s podvodnými jednáními na internetu, kdy oběť přijde o peníze, které zaslala pachateli jako zálohu za jím nabízené zboží, které následně pachatel nedoručil. Dále si lze představit například situaci, kdy pachatel uskuteční DDoS útok na počítač oběti a tím počítač

[73] Válková, H., Kuchta J., Hulmáková J. a kol., 2019, op. cit., s. 172-173.
[74] Čírtková, L., 2013, op. cit., s. 102.
[75] Čírtková, L., 2013, op. cit., s. 103.

nenávratně poškodí. V neposlední řadě může mít finanční újma podobu ušlého zisku zapříčiněného např. několikadenním výpadkem v činnosti společnosti, jejíž počítače byly pachatelem zavirovány. Finanční újma způsobená kybernetickou kriminalitou je obtížně vyčíslitelná, příčinou této skutečnosti je především výše diskutovaná problematika latence této kriminality a s ní spojená nevědomost obětí ve vztahu k mnohým případům, a tedy i škodě jimi způsobené. Odhady o výši škody byly v roce 2014 vyčísleny na částku globálně dosahující 300 miliard dolarů ročně[76]. Aby bylo možné získat přesnější údaje o finanční újmě způsobené kybernetickými trestnými činy, zaměřují se viktimologické výzkumy nejčastěji na získání údajů o konkrétních formách této trestné činnosti, např. podvodech na internetu (více viz bod 4.3.).

Hrozba emocionální (psychické) újmy je na první pohled v oblasti kybernetické kriminality patrná zejména u obětí kyberšikany a kybergroomingu, ale není vyloučena ani u podvodných jednání, kdy se oběť v důsledku trestného činu může stát přehnaně nedůvěřivou a ztratit víru v okolní svět. Psychické dopady kybernetické trestné činnosti mohou mít podobu emocionálního traumatu, depresí, akutní stresové reakce, u obětí krádeže identity se mohou projevovat pocity zrady, vzteku, zranitelnosti a bezmocnosti[77]. Narušení víry ve vlastní schopnost oběti je označováno jako tzv. naučená bezmoc a je jedním z nejvíce negativních dopadů primární viktimizace, jelikož zvyšuje riziko opakované viktimizace[78].

Souhrnnou charakteristikou zaznamenanou u obětí kybernetické kriminality je pocit viny, který může taktéž vyústit v řadu úzkostných poruch či deprese. Tento pocit byl shodně identifikován u obětí různých druhů kybernetické kriminality, a to jak u obětí majetkových trestných činů, které se obviňují z nedostatečného zajištění přístupu do svého technického zařízení, které se stalo terčem útoku hackera, tak např. u obětí kybergroomingu, z důvodu sdělení důvěrných informací či zaslání intimních fotografií pachatelům, kteří je později zneužili. V některých případech se mohou pocity viny v kombinaci s dalšími emocionálními ranami u obětí rozvinout až v tzv. post-traumatickou stresovou poruchu[79].

Příkladem ilustrujícím závažnost psychických následků kybernetické kriminality jsou mnohé případy kyberšikany, jejichž oběti se v nejzávažnějších případech uchylují až k sebevraždě. Vznik psychologických potíží u obětí kyberšikany dokládá například případ

[76] Macalíková, J. Policie ČR. *Kybernetické hrozby jsou stále aktuálnější*, 2014 [online]. [cit. 2020-03-07]. Dostupné z: https://www.policie.cz/clanek/kyberneticke-hrozby-jsou-stale-aktualnejsi.aspx
[77] Nurse, J. R. C., Bada, M. *The social and psychological impact of cyber-attacks.* Benson & McAlaney (2019/20) Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press, 21 s. [online]. [cit. 2020-03-07]. Dostupné z: https://arxiv.org/ftp/arxiv/papers/1909/1909.13256.pdf
[78] Čírtková, L., 2013, op. cit. sub 4, s. 121.
[79] Henson, B., Reyns, B. W., Fisher, B. S. *Cybercrime Victimization.* The Wiley Handbook on the Psychology of Violence, 2016, s. 567 [online]. [cit. 2020-03-07]. Dostupné z: https://www.researchgate.net/publication/314826891_Cybercrime_Victimization

známý jako „Hledám kluka z autobusu“, kdy tehdy devítiletá dívka umístila na internet video, ve kterém popisuje, že se zamilovala do chlapce, kterého potkala v autobusu a ráda by jej cestou internetu našla a znovu se s ním setkala. Po umístění na internet video začalo být mezi uživateli internetu sdíleno a velmi rychle se rozšířilo, dívka se setkala se zesměšňováním a parodováním na internetu, ale také v reálném životě, přičemž v důsledku těchto zážitků musela vyhledat psychologickou pomoc[80].

Pokud se jedná o způsobení fyzické újmy v rámci primární viktimizace, její vznik si nelze jako důsledek kybernetické kriminality dost dobře představit. Lze se pouze domnívat, že některá jednání v kyberprostoru mohou být spouštěčem pachatelova agresivního jednání i mimo kyberprostor, například pachatel kyberšikany může začít na oběť útočit v tzv. off-line světě a ke vzniku fyzické újmy může dojít. Stejnou situaci si lze představit také u kybergroomingu, kdy pachatel oběť po navázání pouta přes internet vyláká na osobní schůzku a tam se na ní dopustí sexuálního násilí.

V závislosti na různých faktorech oběti volí odlišné způsoby toho, jak se s primární viktimizací trestné činnosti vypořádat či jak na ni reagovat. Bylo zjištěno, že častou reakcí obětí kybernetické kriminality je zvýšení obezřetnosti při užívání internetu, úprava nastavení ochrany soukromí, změna uživatelských jmen, hesel či zablokování nevyžádaných zpráv, které pravděpodobně u obětí vede ke znovunabytí nebo posílení pocitu bezpečí[81]. Pokud se jedná o oběti z řad mladistvých a dětí, bylo zaznamenáno, že se ve srovnání s případy, kdy by se stali obětí kriminality mimo kyberprostor, častěji obrací na rodiče a přátele, které o trestném činu informují s žádostí o radu[82].

3.2.2. Sekundární viktimizace

Sekundární viktimizace vzniká u oběti po spáchání trestného činu, projevuje se ve srovnání s primární viktimizací pouze v rovině psychické (s možnými přesahy do roviny fyzické, pokud by se jednalo o psychosomatické problémy) a jejími spouštěči jsou vlivy z okolí oběti. Může být způsobena nepatřičnými reakcemi okolí oběti (rodiny, spolupracovníků, přátel oběti či i neznámých osob v podobě pomluvy), nevhodným přístupem orgánů činných v trestním řízení anebo necitlivostí médií při informování o případu[83].

[80] Kolouch, J., 2016, op. cit., s. 312.
[81] Aricak et al. in Armstrong, S. B., Dubow, E. F., Domoff S.E. *Adolescent coping: In-person and Cyber-victimization.* Journal of psychosocial research on cyberspace. Vol 13, No 4, 2019. [online]. [cit. 2020-04-07]. Dostupné z: https://cyberpsychology.eu/article/view/12559/10906
[82] Idem.
[83] Čírtková, Ludmila. *Viktimologie pro forenzní praxi.* Praha: Portál, 2014, s. 61.

Sekundární viktimizaci způsobené kybernetickou kriminalitou není v odborné literatuře věnována příliš velká pozornost, autoři výzkumů připouští, že viktimizace způsobená kybernetickými trestnými činy obecně představuje zatím poměrně neprobádanou oblast[84]. To ale neznamená, že viktimizace obětí této kriminality nepředstavuje závažný problém. Naopak, vzhledem ke skutečnosti, že potenciálními oběťmi mravnostní kriminality na internetu nebo kriminality spojené s výrobou pornografie mohou být ve velké míře děti jako tzv. zvláště zranitelné oběti, je nepochybně třeba věnovat případným následkům, ať už v podobě primární či sekundární viktimizace dostatečnou pozornost. *Kopecký* se v rámci projektu E-bezpečí zabývá izolovaně sekundární viktimizací dětských obětí online vydírání (jedna z praktik kybergroomingu nebo kyberšikany), kdy pachatel dítě nejčastěji vydírá tím, že uveřejní jeho intimní fotografie či videa, které mu dítě dříve dobrovolně poskytlo[85]. Uvádí, že vydírání je na internetu stále častějším jevem a zároveň spousta těchto případů zůstává utajena z důvodu nenahlašování této trestné činnosti. Pokud se však dětské oběti rozhodnou případ nahlásit, jsou ohroženy sekundární viktimizací zejména ze strany policie – reakce policistů může být vůči nim netaktní, lhostejná, necitlivá (policisté oběti vytýkají, že intimní materiály pachateli dobrovolně zaslala, problém oběti bagatelizují). Rovněž hrozí vysoké riziko viktimizace ze strany médií, které často informují právě o případech, v nichž se jedná o dětské oběti.

3.3. Charakteristika oběti kybernetické kriminality

Stejně jako nelze jednoduše nalézt obecnou charakteristiku pachatele kybernetické kriminality, ani u oběti není možné její popis zobecnit. Jako hlavní aspekt zvyšující viktimnost byla identifikována neopatrnost oběti[86], kdy si oběť často ani neuvědomuje potenciální rizika, kterým je na internetu vystavena a podléhá technikám tzv. sociálního inženýrství pachatele. Určité podobnosti mezi oběťmi je možné vysledovat až v rámci zkoumání konkrétních nelegálních jednání, ke kterým na internetu dochází, poznatkům o některých z nich bude věnována pozornost ve čtvrté části této práce.

Ve vztahu k otázce ohrožení tzv. zvlášť zranitelných obětí (bod 1.3.) lze na základě analýzy jednotlivých forem kybernetické kriminality dospět k závěru, že se v oblasti této trestné činnosti můžeme setkat se všemi „typy“ zvláště zranitelných obětí. Dětské oběti přichází

[84] Roubalová a kol., 2019, op. cit., s. 93.
[85] Kopecký, K. *Krátký úvod do sekundární viktimizace dětských obětí online vydírání*. E-bezpečí, 2012. [online]. [cit. 2020-03-15]. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/dalsi-temata/533-sekundarniviktimizace; Pozn: stejné praktiky pachatelů zachytili také autoři dokumentu V síti.
[86] Křivna, T., Scheinost M., Zoubková I. a kol., 2019, op. cit., s. 392.

v úvahu zejména u kybergoomingu a kyberšikany. Pokud se jedná o osoby s různými druhy postižení, lze si opět představit, že se také stanou obětí kyberšikany nebo některých nenávistných trestných činů. Rovněž teroristické útoky se v dnešní době odehrávají ve velké míře také v kyberprostoru, takže o existenci jejich obětí není pochyb. Poslední kategorii zvlášť zranitelných obětí (oběti taxativně vymezených trestných činů) lze také v rámci jednání pachatelů kybernetické kriminality identifikovat – kybergrooming často obsahuje znaky jak nátlaku, tak násilí, či pohrůžek, trestné činy spáchané pro příslušnost k některé výše uvedené skupině jsou tzv. nenávistné trestné činy a organizovaná kriminalita je v rámci kybernetické kriminality také velmi častým jevem.

V následující části kapitoly budou nejprve analyzovány některé aspekty viktimologických výzkumů jako hlavních pramenů informací o obětech trestných činů. Dále bude zkoumán vztah pachatele a oběti jako jeden z aspektů sledovaných v rámci viktimologie kybernetické kriminality. V závěru bude představena problematika sociálního inženýrství jako hlavního nástroje pachatele kybernetické kriminality ke spáchání trestného činu.

3.3.1. Viktimologické výzkumy

Viktimologie vychází ze závěrů výzkumů, které mají nejčastěji podobu anonymních dotazníkových šetření. Výpovědní hodnota viktimologických výzkumů bývá často zpochybňována vzhledem k neproveditelnosti empirického ověření jejich výsledků, dosahu pouze na respondenty určitých věkových skupin a pouze některé trestné činy, zkreslené odpovědi respondentů, nepřesnost ve formulacích dotazníkových otázek a latenci kriminality. *Roubalová* upozorňuje, že viktimologické výzkumy nejsou vhodné k mapování všech druhů kriminality, nejvyšší výpovědní hodnotu mají obzvláště, pokud jde o tradiční trestné činy, tj. krádeže, vraždu, ublížení na zdraví, naopak nejsou vhodné, pokud jde o hospodářskou nebo drogovou kriminalitu, kdy se oběti často o spáchání trestného činu ani nedozví nebo se jedná o tzv. trestné činy bez obětí[87].

Nejrozsáhlejší viktimologické výzkumy jsou v České republice prováděny *Institutem pro kriminologii a sociální prevenci* (dále také jako „IKSP“), přičemž nejnovější z těchto výzkumů byl uskutečněn v roce 2019[88]. Z výše uvedených příčin se tyto výzkumy zaměřují zejména na oběti tzv. tradiční kriminality, avšak právě v posledním provedeném výzkumu byla pozornost poprvé věnována také jevům z oblasti kybernetické kriminality, a to podvodům při

[87] Válková, H., Kuchta J., Hulmáková J. a kol., 2019, op. cit. s. 176., Roubalová a kol., op. cit., s. 18 a 155.
[88] Roubalová a kol., op. cit., s. 9.

internetovém nakupování, podvodným e-mailům a stalkingu. Závěry výzkumu ohledně těchto trestných činů budou zohledněny v části 4. této práce.

3.3.2. Vztah pachatele a oběti

Zodpovězení otázky existence předchozího vztahu mezi pachatelem a obětí je nezřídka rozhodné pro zjištění příčin spáchání konkrétního trestného činu i pochopení role oběti ve vztahu ke spáchání trestného činu. Trestné činy jsou totiž mnohdy páchány na základě již existujícího vztahu mezi pachatelem a obětí, ať už objektivního (např. zaměstnaneckého či sousedského) nebo subjektivního (partnerského). Tato skutečnost byla v největším rozsahu doložena u tradičních trestných činů jako jsou vraždy, sexuálních trestné činy a loupeže[89].

Pachatelé kybernetické kriminality při svém jednání těží zejména z anonymity, kterou jim internet nabízí. Domnívají se, že jim falešná nebo anonymní identita, za níž se při svém jednání skrývají, umožní nejen spáchat trestný čin, ale také uniknout trestní odpovědnosti za tento skutek. Dalo by se tedy očekávat, že pachatelé ve většině případů nebudou jednat na základě předchozího vztahu s obětí. K hypotéze, že mezi pachatelem a obětí kybernetické kriminality obvykle neexistuje předcházející vztah přispívá rovněž skutečnost, že tyto trestné činy mohou mít často nadnárodní rozměr a pachatel se při jejich páchání může nacházet v jiném státě či dokonce na jiném kontinentu než oběť.

Přesto si lze všimnout, že některé kybernetické trestné činy mají ve srovnání s jinými určitou osobní povahu, která napovídá existenci možného předchozího vztahu mezi pachatelem a obětí, např. kyberstalking, kyberšikana či kybergrooming. V porovnání např. s hackingem nebo podvodnými e-maily mají tato jednání zcela odlišný a často intimní ráz a jejich pachatelé obvykle sledují naprosto jiný motiv, nejčastěji sexuálního charakteru. Zdá se tedy, že při zkoumání vztahu pachatele a oběti kybernetické kriminality je třeba vzít v potaz konkrétní formu a povahu kriminálního jednání a motiv jeho pachatele. Následující část textu bude věnována analýze výše uvedené hypotézy o vztahovosti některých kybernetických trestných činů.

3.3.2.1. Vybrané vztahové kybernetické trestné činy

Prvním z nelegálních jednání z kategorie kybernetické kriminality, u nějž lze předpokládat předchozí vztah mezi pachatelem a obětí je kyberšikana, která je chápána jako šikanování oběti pomocí informačních technologií spočívající primárně ve vydírání, obtěžování

[89] Válková, H., Kuchta J., Hulmáková J. a kol., 2019, op. cit. s. 126.

a zastrašování[90]. Ačkoli pojem kyberšikany nenalezneme v trestním zákoníku, pachatel může svým jednáním naplnit znaky skutkové podstaty trestného činu nebezpečného pronásledování, vydírání, podvodu nebo např. pomluvy. Ke kyberšikaně dochází nejčastěji mezi spolužáky, rovněž se můžeme setkat s kyberšikanou zaměřenou proti učitelům. Dle výzkumu občanského sdružení *Aisis* navštěvuje 78 % pachatelů kyberšikany stejnou školu jako jejich oběť. Z výzkumu Univerzity Palackého v Olomouci z roku 2016 věnujícímu se kyberšikaně namířené proti učitelům vyplynulo, že je páchána nejčastěji žáky, které učitel zná a učí (34,92 % případů). Mezi pachateli se v menší míře objevují také žáci, které učitel zná, ale neučí, nebo rodiče žáků. Je vhodné poznamenat, že podle téhož výzkumu zůstává obvykle značná část útoků kyberšikany proti učitelům neobjasněna (až 25 % případů)[91]. Přesto však lze na základě výše uvedených zjištění shrnout, že ke kyberšikaně dochází ve většině případů na základě předchozího (ve většině případů objektivního) vztahu mezi pachatelem a obětí.

Jedním z kriminálních jednání, která jsou na internetu v poslední době zaznamenávána, je tzv. revenge porn neboli šíření videí či fotografií se sexuálním obsahem bez souhlasu osoby, kterou videa či fotografie zachycují, přičemž cílem pachatele je se oběti svým jednáním pomstít nebo ji zesměšnit[92]. Obětí tohoto jednání, které lze zařadit mezi jednání popisovaná jako kyberšikanu, se nejčastěji stávají bývalí partneři pachatelů zpravidla po ukončení vztahu[93]. Navíc požadavek na existenci předchozího vztahu mezi pachatelem a obětí vyplývá z motivu pachatele – lze si jen obtížně představit situaci, kdy by pachatel zamýšlel pomstít nebo zesměšnit osobu, kterou nezná. Jako příklad z praxe z České republiky lze uvést kauzu zvanou jako „Roztahovačky“, kdy pachatelé vytvořili stejnojmennou stránku na Facebooku, na kterou umisťovali intimní fotografie svých bývalých partnerek[94].

Kyberstalking můžeme popsat jako soustavné pronásledování oběti za použití prostředků elektronické komunikace spočívající zejména v obtěžování oběti zasíláním zpráv, e-mailů, telefonáty apod. Od obecné formy stalkingu se kyberstalking liší tím, že pachatel kyberstalkingu obtěžuje oběť pouze prostřednictvím informačních a komunikačních technologií, ale nedochází k mezi nimi k žádnému fyzickému kontaktu. Bylo zjištěno, že mezi

---

[90] Centrum prevence rizikové virtuální komunikace. *Kyberšina. Úvod do problematiky*. E-bezpečí, 2016 [online]. [cit. 2020-03-15] Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/bud-v-bezpeci/78-bud-v-bezpeci-kybersikana/file

[91] Kopecký, K., Szotkowsi, R. Centrum prevence rizikové virtuální komunikace. *Národní výzkum kyberšikany učitelů.* Olomouc, 2016. [online]. [cit. 2020-03-01] Dostupné z: http://www.prevence-info.cz/sites/default/files/users/10/vyzkumnazprava.pdf

[92] Šepec, M. Revenge pornography or non-consentual dissemination of sexually explicit material as a sexual offence or as a privacy violation offence. *International Journal of Cyber Criminology*, Volume: 13 I2019, s. 420. [online]. [cit. 2020-04-06] Dostupné z: http://www.cybercrimejournal.com/MihaSepecVol13Issue2IJCC2019.pdf

[93] Idem.

[94] Kolouch, J., 2016, op. cit., s. 315.

pachatelem a obětí obecné formy stalkingu ve většině případů existuje předchozí vztah, nejčastěji se jedná o vztah partnerský, kdy po jeho ukončení ze strany oběti pachatel nepřestává oběť kontaktovat[95]. Oproti tomu kyberstalking se dle výsledků výzkumů vyznačuje poměrně vyrovnaným poměrem případů založených na předchozím vztahu pachatele a oběti a naopak případů, k nimž dochází mezi zcela neznámými osobami[96]. Lze se domnívat, že je to kvůli skutečnosti, že zatímco stalker v tzv. off-line světě musí mít pro realizaci svého jednání vždy o oběti alespoň základní povědomí založené na předchozím vztahu s obětí (znát její bydliště, místo zaměstnání apod.), přičemž tato znalost je hlubší v případě, kdy se jedná o osoby, mezi nimiž existoval blízký vztah (partnerský, přátelský), kyberstalker může na oběť útočit, aniž by on nebo oběť opustili dům, ve kterém žijí. Kyberstalkerovi totiž postačuje získat kontakt na oběť, prostřednictvím kterého se ní může na internetu spojit (e-mail, účet na sociální síti apod.) a poté je již pro něj oběť jako předmět útoku dosažitelná bez ohledu na to, zda je informován o bližších skutečnostech o jejím životě. Navíc lze podotknout, že mnoho informací o dříve zcela neznámé oběti je možné získat právě z jejích sociálních sítí, kde oběti velmi často neuváženě otevřeně oznamují, kde se zrovna nachází a co dělají, případně jaké mají plány do budoucna. Pachatel může tedy oběť zastrašovat tvrzeními, že ví, kde se nachází, a přitom pouze vycházet z informací, které o sobě oběť sama dobrovolně uveřejnila. Lze uzavřít, že kyberstalking stojí v rámci kategorizace spíše na pomezí vztahových a nevztahových deliktů, jelikož z výše popsaných příčin použití internetových a komunikačních technologií nahrává i trestným činům zcela nezaloženým na předchozím vztahu pachatele a oběti.

3.4. Sociální inženýrství

Pachatelé kybernetické kriminality jsou dle výše popsaných zjištění spíše osoby s vyšší inteligencí a pro navázání vztahu s obětí a zvýšení pravděpodobnosti úspěchu svých útoků používají tzv. sociální inženýrství. Sociální inženýrství neboli sociotechnika představuje soubor postupů a strategií k vylákání osobních nebo citlivých údajů a materiálů, přičemž tyto pachatel dále využívá pro páchání trestné činnosti[97]. Příkladem může být získání hesel prostřednictvím nichž pachatel proniká do počítačových systémů nebo intimních informací či fotografií oběti kybergroomingu, které používá k vydírání oběti v případě, že s ním chce oběť přerušit kontakt.

[95] Čírtková, L., 2013, op. cit., s. 219.
[96] Vakhitova, Z. a kol., 2018, op. cit., s. 351.
[97] Kopecký, K. *Strategie manipulace dětí v online prostředích se zaměřením na tzv. kybergrooming*. Pediatrie pro praxi 2015; 16 (5), s. 209. [online]. [cit. 2020-03-01] Dostupné z: https://www.researchgate.net/profile/Kamil_Kopecky3/publication/280023825_Strategie_manipulace_deti_v_online_prostredich_se_zamerenim_na_tzv_kybergrooming/links/55c494c108aea2d9bdc32508.pdf

Postupy sociálního inženýrství spočívají zejména v uvedení osoby v omyl, lstivém jednání nebo jiném psychické ovlivňování, přičemž byly ve velké míře zaznamenány právě u pachatelů kybernetické kriminality.

Uživatel internetu je mezi možnými terči kybernetické kriminality vnímán jako nejslabší článek, jelikož je v porovnání se stroji vybaven znalostmi, zkušenostmi, ale také emocemi, na které může pachatel vědomě působit a oběti se mohou zejména vlivem emocí dopouštět tzv. „kognitivních chyb úsudku“[98]. *Kolouch* uvádí, že *„jelikož na světě nemůže existovat počítačový systém, který by alespoň v nějaké fázi nebyl závislý na člověku (ať již jde o zprovoznění, nastavení, či údržbu počítačového systému), je nejjednodušší cestou získat potřebné informace právě od člověka“*[99]. Různé metody sociálního inženýrství může pachatel aplikovat v případech, kdy je terčem jeho útoku fyzická osoba, např. jako oběť kybergroomingu, ale také zamýšlí-li např. zaútočit na informační systém obchodní společnosti, tj. metody sociálního inženýrství taktéž směřují vůči fyzické osobě (z důvodů zranitelnosti uvedených výše), ale cílem pachatele je zasáhnout chod celé společnosti, např. banky.

Lze předpokládat, že sociální inženýrství může být nejúčinnější zejména jsou-li jeho metody použity vůči mladším a nezkušeným jedincům, případně i starším osobám se zvýšenou důvěřivostí. V souvislosti s charakteristikou pachatelů můžeme uvést, že větší sklony k sociálnímu inženýrství budou mít pravděpodobně manipulativní jedinci, kteří jsou schopni jednak úspěšně identifikovat cíl útoku, a rovněž jsou způsobilí tyto osoby úspěšně ovlivňovat a přimět je k jednání, které je pro ně prospěšné.

V postupech pachatelů využívajících sociální inženýrství lze vysledovat určitou chronologii jejich jednotlivých kroků. Prvním krokem pachatele je odhalení zranitelného místa v systému, případně konkrétní zranitelné oběti. Tyto informace pachatel obvykle získává průzkumem volně dostupných webových stránek[100]. Pachatel však může při vyhledávání prvotních informací o cíli útoku přistoupit také k tzv. fyzickému útoku, kdy se např. vydává za pracovníka servisní agentury a snaží se získat nejvíce informací přímo na místě, které si vybral jako cíl útoku, např. získat hesla, která mají pracovníci společnosti často poznamenána v bezprostřední blízkosti počítače[101].

[98] Národní centrum kybernetické bezpečnosti. *Sociální inženýrství.* [online]. [cit. 2020-03-01] Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/
[99] Kolouch, J., op. cit., s. 186.
[100] Jirovský, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*, Praha, 2007, s. 196.
[101] Kolouch, J., op. cit., s. 187-188.

Poté, co pachatel potenciální oběť identifikuje, naváže s ní kontakt a snaží se o navázání důvěrného vztahu s obětí, kterou chce následně přesvědčit ke sdělení určitých informací. Za sdělení těchto informací pachatel oběti v některých případech nabízí odměnu v podobě finančního zisku, avšak mnohem častěji dochází k situacím, kdy oběť na základě důvěrného vztahu s útočníkem informace vyzrazuje sama bez finanční motivace, jelikož pachateli se podaří vyvolat v ní dojem, že poskytnutí informací ji „nic nestojí“ a zároveň získá sdělením pocit, že „byla užitečná“[102].

3.4.1. Metody sociálního inženýrství

Pachatelé v rámci sociálního inženýrství používají různé metody útoku, přičemž jednotlivé metody lze aplikovat v různých fázích útoku. Nejčastějšími metodami jsou:

a) zasílání podvodných e-mailů či vytvoření falešných webových stránek (tzv. phishing): odesílatel e-mailu se například vydává za pracovníka banky či jiné společnosti a vyžaduje od oběti sdělení hesla k jejímu internetovému bankovnictví za účelem provedení aktualizací; že se jedná o podvodný e-mail lze obvykle zjistit z hlavičky e-mailu, z níž je patrné, z jaké e-mailové adresy byla zpráva odeslána, oběti však často tyto skutečnosti nekontrolují ani jim nevěnují pozornost; pachatel se také může stavět do role zaměstnavatele či jiné osoby na vedoucí pozici ve společnosti, v jejichž kompetenci je autorizace určitých plateb či jednání a e-maily, které adresují podřízeným zaměstnancům požadují provedení těchto plateb či jednání[103];
b) telefonické hovory: nejčastěji se terčem útoku stávají pracovníci help desku, při útocích bývají úspěšné zejména ženy, které dokážou lépe navodit pocit důvěry a přesvědčit oběť ke sdělení informací[104];
c) prohledávání odpadků v místě útoku: lze si představit situaci, kdy pachatel nalezne důležité dokumenty, které měly být skartovány, a ne vyhozeny do koše s běžným odpadem;
d) vydávání se za servisního technika či jinou osobu za účelem fyzického průniku na místo útoku: většina lidí většinou nemá tendence ověřovat, zda tito lidé jsou skutečně těmi, za které se vydávají[105].

[102] Jirovský, V., 2007, op. cit., s. 201.
[103] Jirovský, V., 2007, op. cit., s. 203-204; Europol, 2019, op. cit., s. 40; přednášky v rámci povinně volitelného předmětu Kybernetické kriminality a kybernetické bezpečnosti v zimním semestru 2019/2020.
[104] Jirovský, V., 2007, op. cit. sub 95, s. 201.
[105] Kolouch, J., 2016, op. cit., s. 187-188.

Sociální inženýrství je obecným pojmem, bylo ale zjištěno, že jeho jednotlivé techniky se mohou lišit ve vztahu ke druhu jednání pachatele. Specifické techniky byly popsány například u pachatelů kybergroomingu. Jedná se o tzv. techniku „kobercového tapetování", strategii vylákání intimních materiálů prostřednictvím fotografie osoby opačného pohlaví a *„webcam trolling"*[106]. Technika tzv. kobercového tapetování spočívá v jednání pachatele, který na konkrétní sociální síti, chatu či jiné platformě, identifikuje skupinu obětí určitého věku (zjistitelné z profilu oběti, je možné vyhledat nastavením filtru) a tyto oběti následně hromadně osloví[107]. Další používanou technikou v případě, že je cílem pachatele vylákat z oběti její intimní fotografie, je zaslání zdánlivě vlastních intimních fotografií (pachatel ale obvykle nepoužívá své vlastní fotografie, protože se často vydává za osobu zcela jiné věkové kategorie), přičemž se tímto jednáním snaží oběti „dodat odvahu" k zaslání jejích intimních fotografií[108]. Poslední zvláštní techniku tzv. *webcam trollingu* pachatelé používají ke zvýšení své důvěryhodnosti v případě, že s obětí uskutečňují videohovor. Namísto skutečného obrazu webkamery, který by zachycoval jejich obraz nainstalují videozáznam osoby, za níž se vydávají, přičemž oběti tvrdí, že jim nefunguje na počítači mikrofon, a proto vidí jen jejich obraz, ale nemohou spolu přímo mluvit[109].

3.4.2. Prevence sociálního inženýrství

Prevence v oblasti sociálního inženýrství je realizována zejména zvyšováním informovanosti o metodách, které mohou pachatelé ke spáchání trestného činu použít. Dle *Europolu*[110] by měly společnosti školit své zaměstnance tak, aby byli schopni odhalit podvodné e-maily a telefonáty, a aby ochránili svou společnost před možnými fyzickými průniky pachatelů do místa útoku, tj. zejména kontrolou návštěv společnosti atd. Nezbytné je přitom zaškolení nejen zaměstnanců, kteří primárně odpovídají za ochranu důležitých informací a materiálů, ale také zaměstnanců na nižších pracovních pozicích (recepční a administrativní pracovníci, jelikož právě jejich nevhodným postupem mohou být informace vyzrazeny[111]).

[106] Kopecký, K., 2015, op. cit., s. 209.
[107] Pozn.: tato technika je zachycena také tvůrci dokumentárního filmu V síti, kdy pachatelé falešné oběti byly pachateli osloveny velmi rychle, patrně na základě uvedeného věku u jejich profilu. Zároveň byli v dokumentu identifikováni pachatelé, kteří komunikovali s různými obětmi stejného věku, tj. bylo patrné, že oslovují více obětí na základě těchto kritérií.
[108] Pozn.: také tato technika byla v dokumentu v síti zachycena – ve většině případů se však jednalo o fotografie či videa samotných pachatelů, která zasílali obětem nebo se sami obnažení prezentovali na webkameře.
[109] Kopecký, K., 2015, op. cit., s. 209.
[110] Europol, 2019, op. cit., s. 11.
[111] Jirovský, V., 2007, op. cit., s. 206.

Lze se domnívat, že většina potenciálních obětí si uvědomuje, že jsou kybernetickou kriminalitou ohroženy, ale nemusí si být vždy vědomy toho, jak nebo čím jsou přesně ohroženy. Seznámení obětí s konkrétními jednáními, s nimiž se mohou ze strany pachatele setkat, tak může významně přispět prevenci kybernetické kriminality. Na závěr lze poznamenat, že problematika sociálního inženýrství je dalším důkazem nezbytné interdisciplinární spolupráce zejména mezi kriminologií, psychologií a sociologií.

Závěrem

Charakteristika typické oběti kybernetické kriminality je stejně obtížná jako charakteristika pachatele – pro každý trestný čin z oblasti kybernetické kriminality bude pravděpodobně typická oběť určitého věku nebo vlastností. Lze si povšimnout, že viktimologie orientovaná pouze na oběti kybernetické kriminality není prozatím příliš rozvinuta, pokud je možné dohledat přesnější informace o některém typu obětí kybernetické kriminality, jedná se ve většině případů o oběti kyberšikany nebo kybergroomingu, což je pochopitelné vzhledem k tomu, že oběťmi jsou nejčastěji děti jako zvlášť zranitelné oběti, přesto však lze považovat za nezbytné, aby se viktimologický výzkum zaměřil rovnoměrněji také na jiné oblasti kybernetické trestné činnosti, jelikož je patrné, že kybernetická kriminalita má velký dopad jak na majetkovou tak nemajetkovou sféru jejích obětí. Je nepochybné, že příprava a provádění viktimologických výzkumů je velmi náročná a aby byl výsledek relevantní, je nezbytné oslovit dostatečný vzorek populace. Přesto se však lze domnívat, že nejen informace o pachatelích, ale také o obětech mohou velkou měrou přispět v oblasti prevence této kriminality, přičemž je to právě preventivní přístup, který je v dnešní době vedle represivního přístupu často zdůrazňován. Důležitost viktimologického výzkumu v této oblasti podtrhuje navíc skutečnost, že se v oblasti kyberprostoru pohybují stále mladší uživatelé, kteří jsou ohroženi zejména mravnostní kriminalitou, jejíž následky mohou být pro další život jejích obětí velmi kritické.

V návaznosti na předchozí dvě kapitoly věnované analýze obětí a pachatelů kybernetické kriminality lze dodat, že nejsou jedinými „osobami“, kterým je a nadále by měla být věnována pozornost kriminologických výzkumů. V posledních měsících lze v odborné literatuře zaznamenat zvýšený výskyt popisu tzv. „by-stander fenoménu“, který není v kriminologii novým pojmem, nicméně v souvislosti s kybernetickou kriminalitou začal být zmiňován a popisován až poměrně nedávno. Psychologie se pomocí „by-stander fenoménu“ snaží popsat jednání osob, které se za různých okolností ocitnou na místě činu, přičemž jsou zkoumány faktory, které ovlivňují jejich chování a mají vliv na vytváření jejich rozhodnutí oběti trestného činu pomoci. Lze se domnívat, že tyto osoby, které jsou svědky trestné činnosti,

mohou být v případě kybernetické kriminality důležitými subjekty pro účely prevence kriminality, případně zabránění v jejím dalším pokračování, pokud trvá delší dobu, např. v podobě dlouhodobé kyberšikany, a proto je nezbytné jejich jednání blíže zkoumat a výsledky výzkumů využít právě k prevenci kriminality. Problematickým aspektem „by-stander fenoménu“ v oblasti kybernetické kriminality je však dle výzkumů ještě nižší ochota pomoci oběti trestného činu, než u tzv. off-line zločinů. Je pochopitelné, že kolemjdoucí vnímá např. fyzické napadení, jehož je svědkem jako závažnější než urážky či kyberšikanu, jichž je svědkem na diskuzních fórech. Tento jev, kdy „by-stander“ vnímá kybernetickou kriminalitu jako méně závažnou, než kriminalitu v tzv. off-line světě, je způsoben také tím, že oběť často nezná, nikdy se s ní nesetkal a nemůže tudíž vyhodnotit, jaký dopad na ni trestný čin má[112]. Lze se tedy domnívat, že nástroje prevence není třeba adresovat pouze potenciálním obětem trestné činnosti, ale patřičně také upozornit, jak postupovat v případě, kdy se osoba stane svědkem kybernetického trestného činu.

[112] Koehler, C., Weber, M. (2018). ”Do I really need to help?!” Perceived severity of cyberbullying, victim blaming, and bystanders’ willingness to help the victim. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 12*(4), Article 4. https://doi.org/10.5817/CP2018-4-4. [online]. [cit. 2020-05-22] Dostupné z: https://cyberpsychology.eu/article/view/11451/10233; Walker, J. A., Jeske, D. (2016). Understanding Bystanders' Willingness to Intervene in Traditional and Cyberbullying Scenarios. *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL), 6*(2), 22-38. doi:10.4018/IJCBPL.2016040102. [online]. [cit. 2020-05-22] Dostupné z: https://www-igi-global-com.ezproxy.is.cuni.cz/gateway/article/full-text-html/158156

4. Pachatelé a oběti vybraných forem kybernetické kriminality

Jak bylo uzavřeno na základě výše uvedených zjištění, vytvořit univerzální profil pachatele a oběti kybernetické kriminality není vzhledem k rozmanitosti forem této trestné činnosti možné. Lze sice vysledovat určité shodné znaky, avšak v obou případech se jedná o kusé charakteristiky neposkytující širší možnosti praktického využití pro oblast prevence či represe. Větší pravděpodobnost identifikace charakteristických pachatelů a obětí však lze předpokládat, budou-li zkoumány jednotlivé formy kybernetické kriminality, přičemž právě třem z nich bude věnována závěrečná část této práce, a to nenávistným trestným činům, kyberstalkingu a podvodným jednáním na internetu.

4.1. Nenávistné trestné činy na internetu

Nenávistné trestné činy na internetu (dále také jako „hate crimes“) představují obdobu nenávistných trestných činů páchaných v tzv. off-line světě. Jednání jejich pachatelů spočívá v nenávistných projevech vůči určité osobě nebo skupině osob, přičemž k těmto projevům dochází nejčastěji na sociálních sítích, webových stránkách politických stran a v internetových diskuzích[113]. Díky rozvoji internetu získaly v posledních letech nenávistné trestné činy novou platformu, která umožňuje sdílení informací s předem neurčeným a velmi širokým okruhem osob. Dostupnost takto sdílených projevů dovoluje páchání trestné činnosti v mnohem větším rozsahu než dříve. V roce 2018 byl v České republice registrován nárůst počtu nenávistných projevů na sociálních sítích a dalších komunikačních platformách, např. v diskusních chatech na zpravodajských serverech[114]. Nenávistné projevy na internetu mohou mít pravděpodobně závažný dopad na psychiku jejich obětí, další rizika této trestné činnosti navíc tkví v potenciálním podnícení dalších osob k páchání této činnosti. Bylo zjištěno, že nenávistné projevy učiněné na internetu vykazují oproti nenávistným projevům v tzv. off-line světě vyšší míru explicitnosti a útočnosti související patrně s tím, že je pachatel ve své pozici „posilněn“ pocitem anonymity a mylného pocitu bezpečí z hlediska případné trestní odpovědnosti[115].

---

[113] Smieško, I. *Internet a trestné činy extrémismu*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2017, s. 50.

[114] Ministerstvo vnitra ČR. *Zpráva o projevech extremismu a předsudečné nenávisti na území České republiky v roce 2018.* Praha, 2019, s. 47. [online]. [cit. 2020-03-01] Dostupné z: https://www.mvcr.cz/clanek/extremismus-vyrocni-zpravy-o-extremismu-a-strategie-boje-proti-extremismu.aspx

[115] Keum, B. T. Qualitative Examination on the Influences of the Internet on Racism and its Online Manifestation. *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL)*, 2017, 7(3), 13-22. doi:10.4018/IJCBPL.2017070102 [online]. [cit. 2020-03-01] Dostupné z: https://www-igi-global-com.ezproxy.is.cuni.cz/gateway/article/full-text-html/190804

4.1.1. Pachatelé nenávistných trestných činů na internetu

Hate crimes nejčastěji představují nevztahové delikty, tj. tyto trestné činy nebývají založeny na předchozím vztahu pachatele a oběti. Pachatel útočí na oběť z toho důvodu, že je jiná než on, a přitom sebe považuje za normální a oběť za nenormální a tento vnitřní pocit založený obvykle na nesnášenlivosti jej motivuje k nenávistnému útoku[116]. Pro naplnění znaků skutkové podstaty trestných činů z nenávisti přitom není podstatné, zda oběť trestného činu odlišnost, pro kterou na ni pachatel útočí, skutečně vykazuje, nebo se tak pachatel pouze domníval. To znamená, že i kdyby pachatel útočil na internetu na neznámou osobu, která by ve skutečnosti napadenou charakteristikou nedisponovala, stále by se dopouštěl trestného činu.

Ze Zprávy o extremismu na území České republiky z roku 2018 vyplývá, že pachatelé nenávistných projevů na internetu nemusí mít vazbu na extremistickou scénu a mnoho z nich se mylně domnívá, že u nich z tohoto důvodu nemůže za jejich jednání vzniknout trestní odpovědnost. Tento pocit neodpovědnosti je zřejmě u pachatelů umocněn také pocitem anonymity, kdy příspěvky na internetu mohou zveřejňovat pod smyšlenou identitou. Pokud jde o otázku věku pachatele, dle údajů Ministerstva vnitra představují trestné činy hanobení rasy a podněcování k nenávisti vůči skupině osob jedny z nejčastějších deliktů mládeže[117], přičemž vzhledem k častému využívání internetu mládeží se lze domnívat, že se poměrně velká část těchto jednání odehrává právě na internetu.

4.1.1.1. Typologie pachatelů nenávistných trestných činů na internetu

Smieško uvádí, že obecné typologie pachatelů nenávistné trestné činnosti jsou poměrně univerzální a lze je tedy využít jak v případě, kdy se pachatel dopouští trestné činnosti na internetu, tak mimo něj (uvádí např. Herczegovu typologii dle motivace pachatele nebo Burdovu typologie dle sociálního postavení pachatele). Zároveň však *Smieško* vytváří vlastní velmi zajímavou typologií pachatelů, která bere v úvahu specifika páchání této trestné činnosti na internetu. Dle činnosti a motivace rozlišuje tři kategorie pachatelů, přičemž role prvních dvou skupin se mohou prolínat:

a) ryba: zahrnuje každého uživatele internetu, který reaguje na různé podněty (pozitivně nebo negativně, nejčastěji komentováním nebo tzv. lajkováním příspěvků jiných osob);
b) rybář: každý, kdo na internetu něco uveřejňuje (články, obrázky, videa), zejména na sociálních sítích, může se jednat o administrátory facebookových stránek

[116] Smieško, I., 2017, op. cit., s. 160.
[117] Ministerstvo vnitra ČR. *Zpráva o projevech extremismu a předsudečné nenávisti na území České republiky v roce 2018.* Praha, 2019, s. 14.

a skupin, cílem je získat co nejvíce reakcí od „ryb“, čím více takových reakcí, tím větší dosah a vliv jeho činnost má;

c) troll: uživatel praktikující tzv. trolling – provokativní, urážlivé či jinak kontroverzní zapojování se v diskuzích, cílem je vyprovokovat ostatní k emotivní reakci nebo až k tzv. „flame war“, v praxi se můžeme setkat např. se situací, kdy se pachatel snaží rozpoutat nenávistnou diskuzi mezi příslušníky menšiny a většiny.

Skupinu, které by při boji proti nenávistným projevům měla být pravděpodobně věnována největší pozornost, představují rybáři, jelikož vytváří anebo alespoň rozšiřují nenávistné projevy. Jejich cílem je zajistit si získáním dostatečného počtu „fanoušků“ určitý vliv či rozšířit dosah své činnosti, přičemž se lze domnívat, že přitom mohou být motivováni jak finančně (například zavedenou stránku na Facebooku je možné využít jako platformu pro sdílení reklam, za které dostane správce stránky zaplaceno), ale také šířením myšlenek a přesvědčení založených na nenávisti, netoleranci nebo zakázané ideologii.

Pokud se jedná o pachatele označované jako ryby, předmětem odborných diskuzí stále zůstává otázka, zda pouhé „olajkování“ příspěvku s nenávistným obsahem nebo jeho sdílení lze chápat jako naplnění subjektivní stránky některého z nenávistných trestných činů a zda tedy u této osoby může dojít ke vzniku trestní odpovědnost za některý z těchto trestných činů[118].

4.1.2. Oběti hate crimes na internetu

Nenávistnými trestnými činy jsou potenciálně ohroženy osoby, které jsou příslušníky skupiny vyznačující se jakoukoli odlišností, kterou nemohou ovlivnit nebo změnit. Právě z tohoto důvodu jsou možnosti prevence těchto trestných činů velmi omezené[119]. Oběťmi se nejčastěji stávají příslušníci národnostních, etnických či náboženských skupin. *Vegrichtová* zmiňuje jako potenciální oběti v budoucnu také staré osoby a připouští, že se oběťmi hate crimes možná stávají již dnes, avšak v rámci latentní viktimizace[120]. Je pravděpodobné, že vzhledem k citlivosti tématu menšinové problematiky je míra latence u nenávistných trestných činů velmi vysoká, přičemž důvodem tohoto jevu může být také tolerance a bagatelizace ze strany většinové společnosti. V České republice a na Slovensku se v současné době setkáme s nenávistnými projevy na internetu orientovanými zejména na příslušníky romské menšiny,

[118] Smieško, I., 2017, op. cit., s. 99.
[119] Čírtková, L., 2014, op. cit., s. 130.
[120] Vegrichtová, B. *Extremismus a společnost*. 2. aktualizované a doplněné vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017, s. 25.

což dokládá také soudní praxe např. v trestní věci poškozeného Radka Bangy[121]. Další skupinou ohroženou nenávistnými projevy jsou migranti, mezi lety 2017 a 2018 byl zaznamenán nárůst počtu nenávistných projevů právě v souvislosti s migrační krizí[122]. Terčem nenávistných útoků však v době migrační krize nemusí být pouze samotní migranti, ale také vlády za či mezinárodní organizace, které rozhodují o řešení migrační krize nebo osoby, které migranty či uprchlíky podporují a nabízí jim pomoc[123].

Nenávistné trestné činy jsou z hlediska psychologických dopadů na oběť řazeny mezi jedny z nejzávažnějších. Jelikož příčiny této kriminality tkví ve skutečnostech, které nelze jednoduše nebo vůbec ovlivnit (např. barva pleti), je osoba, která se stane terčem nenávistných útoků vůči pachateli zcela bezbranná. U obětí mohou nenávistné útoky na jejich osobu spustit úzkostné poruchy, deprese, v krajních případech u nich dochází k sebeodmítání a ztrátě identity[124]. Lze navíc předpokládat, že osoby, které jsou nositeli některých viktimogennních faktorů čelí nenávistným útokům i v tzv. off-line světě, a proto pro ně útoky páchané na internetu mohou představovat velmi zraňující zkušenost spojenou také s rizikem terciární viktimizace.

V závěru lze poznamenat, že viktimizace nenávistnými trestnými činy je navíc charakteristická tím, že se nemusí projevit pouze u osoby, která je adresátem projevu, ale také u dalších příslušníků skupiny, k níž tato osoba náleží a vykazují stejné odlišnosti. Neopominutelné jsou také následky těchto projevů na společnost, kdy tyto trestné činy společnost rozdělují a vytváří atmosféru napětí mezi menšinami a většinou.

4.2. Kyberstalking

Podstata jednání pachatelů kyberstalkingu byla nastíněna výše v části věnující se vztahu pachatele a oběti kybernetických trestných činů (bod 3.3.2.1.). Je vhodné připomenout, že kyberstalking se od obecné formy stalkingu liší tím, že pachatel obtěžuje oběť pouze prostřednictvím internetu a jiných elektronických prostředků komunikace, přičemž mezi nimi nedochází k fyzickému kontaktu. Kyberstalking tedy představuje konkrétní druh

[121] Ústavní soud. *Zvláštní povaha a proměnnost tzv. trestných činů z nenávisti ukládá soudům povinnost posoudit povahu každého z takových útoků z perspektivy jeho potenciálních konkrétních obětí a prostředí (sociální sítě), ve kterém jsou páchány*. Brno, 2016. [online]. [cit. 2020-03-01] Dostupné z: https://www.usoud.cz/aktualne/zvlastni-povaha-a-promennost-tzv-trestnych-cinu-z-nenavisti-uklada-soudum-povinnost-poso/

[122] Ministerstvo vnitra ČR. *Zpráva o projevech extremismu*, 2019, op. cit., s. 47.

[123] Hanzelka J., Schmidt I. *Dynamics of Cyber Hate in Social Media: A comparative Analysis of Anti-Muslim Movements in the Czech republic and Germany*. International Journal of Cyber Criminology, January - June 2017, s. 152. [online]. [cit. 2020-03-01] Dostupné z: http://www.cybercrimejournal.com/Hanzelka&Schmidtvol11issue1IJCC2017.pdf

[124] Čírtková, L., 2014, op. cit., s. 130.

či podkategorii stalkingu. Lze mínit, že podmínky pro páchání této trestné činnosti jsou pro pachatele v dnešní době velmi příznivé, jelikož díky rozšíření internetu, sociálních sítí a jiných prostředků moderní komunikace může oběť obtěžovat téměř neustále. Charakteristickým znakem stalkingu je právě soustavnost obtěžování pachatele, kdy jeho útoky přetrvávají rámcově alespoň po několik týdnů a také neměnnost rolí pachatele a oběti[125].

Jelikož kyberstalking představuje poměrně novou problematiku, v České republice nebyl dosud proveden rozsáhlejší výzkum či sestavena statistika zaměřená výlučně na tento jev. Pro vytvoření alespoň základní představy o četnosti tohoto jevu je však možné vycházet z výsledků viktimologického výzkumu zabývajícího se stalkingem v jeho obecné podobě, který v přehledu výsledků rozlišuje mezi tím, zda pachatel kontaktoval oběť za použití počítače nebo telefonu anebo ji naopak obtěžoval pouze jednáním v tzv. off-line světě[126].

4.2.1. Pachatel kyberstalkingu

Pachatel bývá častěji mužského pohlaví, přičemž jeho hlavním motivem je získání pocitu moci a kontroly nad obětí, navázání vztahu s obětí, případně pomsta oběti[127]. V odborné literatuře se setkáme s různými typologiemi pachatelů kyberstalkingu. Typologií, kterou lze považovat za nejvíce zohledňující charakteristické znaky „kybernetického“ prvku stalkingu, je typologie vytvořená americkým forenzním psychologem McFarlenem[128]:

- kyberstalker z pomsty (*„vindictive cyber stalker“*): je nejnebezpečnějším typem pachatele, jeho jednání zahrnuje nadměrné kontaktování oběti prostřednictvím internetové komunikace, ale také krádež identity nebo zavirování počítače oběti, má pokročilé znalosti informačních technologií;
- klidný, vyrovnaný kyberstalker (*„composed cyber stalker“*): jeho útoky vůči oběti nejsou tak intenzivní jako u kyberstalkera z pomsty, jeho cílem je u oběti vyvolat pocit přetrvávajícího neklidu;
- důvěrný kyberstalker (*„intimate cyber stalker“*): jeho cílem je prostřednictvím stalkingu navázat s obětí vztah, je obětí posedlý, v některých případech se jedná o pachatele, kteří již v minulosti s obětí navázali vztah běžnými prostředky;

[125] Národní centrum bezpečnějšího internetu. *Kybergrooming a kyberstalking.* 2012, s. 15 [online]. [cit. 2020-03-01] Ke stažení z: https://www.ncbi.cz/
[126] Roubalová M. a kol., 2019, op. cit., s. 88 a násl.
[127] Národní centrum bezpečnějšího internetu, 2012, op. cit.
[128] McFarlen L. in Pittaro M. L. Cyber stalking: An Anylysis of Online Harassment and Intimidation. International Journal of Cyber Criminology, 2007, Vol. 1, Issue 2, [online]. [cit. 2020-03-01]. Dostupné z: http://www.cybercrimejournal.com/pittaroijccvol1is2.htm

- kolektivní kyberstalker (*„collective cyber stalker“*): kyberstalking je úmyslně prováděn dvěma či více pachateli současně vůči téže oběti, lze se domnívat, že tato forma kyberstalkingu je jednou z nejzávažnějších vzhledem k intenzitě pronásledování, které lze dosáhnout při zapojení více pachatelů.

S typologiemi pachatelů kyberstalkingu se setkáme také v tuzemské odborné literatuře, nezohledňují však v takové míře konkrétní prostředky a způsoby, které pachatel k pronásledování používá, ale více se věnují hledisku vztahu mezi pachatelem a obětí:

- bývalý partner: případy, kdy se stalker není schopen vyrovnat s ukončením vztahu, zvláště problematické mohou být případy nejasně ukončených vztahů, viz dále;
- uctívač: s obětí se obvykle osobně nezná, ale zpovzdálí ji obdivuje, obětí se mohou stát v tomto případě známé osobnosti;
- neobratný nápadník: vyznačuje se nezkušeností v oblasti intimních vztahů, stalking je u něj projevem této nezkušenosti, lze se domnívat, že si často ani neuvědomuje závadnost svého jednání;
- ublížený pronásledovatel: jeho motivem je odplata za újmu, kterou mu oběť způsobila (může jít o újmu reálně či pouze domněle způsobenou);
- poblouzněný milovník: pachatel je do oběti zamilovaný a domnívá se, že jeho city opětuje, což jej ještě více podněcuje v jeho aktivitách[129].

Na základě podobných kritérií rozlišuje pachatele stalkingu také *Čírtková*, která uvádí, že až v 50 % jde o případy stalkerů – ex-partnerů. Rovněž upozorňuje na to, že zejména u pachatelů typu „poblouzněný milovník“ neboli „umanutý obdivovatel“ mohou být diagnostikovány psychické poruchy, přičemž tito pachatelé nemají náhled na své jednání, a tudíž mohou být velmi nebezpeční[130]. Ze všech typologií je patrné, že z hlediska otázky vztahu mezi pachatelem a obětí se setkáme u kyberstalkingu jak s případy, kdy je jednání pachatele založeno na jeho předchozím vztahu s obětí, tak s případy obětí pachatelům zcela neznámým. Více k této problematice bylo uvedeno v části 3.3.2.1.

4.2.2. Oběti kyberstalkingu

Z výsledků výzkumu *Institutu pro kriminologii a sociální prevenci* vyplynulo, že se stalkingem má zkušenost 5 % respondentů (158 osob z celkového počtu 3393 dotázaných).

[129] Národní centrum bezpečnějšího internetu, 2012, op. cit., s. 15.; Přednášky doc. PhDr. Ludmily Čírtkové, CSc. v rámci předmětu Soudní psychologie v zimním semestru akademického roku 2019/2020.
[130] Přednášky doc. PhDr. Ludmily Čírtkové, CSc. v rámci předmětu Soudní psychologie v zimním semestru akademického roku 2019/2020.

Oběti byly pachatelem nejčastěji obtěžovány prostřednictvím e-mailové komunikace, SMS zpráv a sociálních sítí, případně telefonicky, jednalo se v souhrnu o 102 případů[131]. Terčem útoku stalkera byly ve 2/3 případů ženy, ale autoři výzkumu stejně jako např. *Čírtková* upozorňují na to, že pokud se jedná o trestné činy mezi partnery, u trestných činů s mužskými oběťmi je nezbytné brát v úvahu předpokládanou vysokou míru latence, jelikož se často z různých důvodů uchylují k nenahlašování trestné činnosti[132].

Kyberstalking není omezen na konkrétní věkovou kategorii obětí, faktorem zvyšujícím riziko viktimizace je zde pouhé používání moderních komunikačních technologií, prostřednictvím kterých může pachatel oběť kontaktovat. Teoreticky tak mohou být obětí jak děti, tak senioři, postačí, aby používali například telefon.

Na rozdíl od obecné formy stalkingu, kdy je možné setkat se s následky trestné činnosti i v majetkové sféře oběti (stalkeři se uchylují k ničení věcí ve vlastnictví oběti, např. aut nebo dokonce zabíjení domácích mazlíčků oběti), byly u obětí kyberstalkingu popsány především následky ve sféře psychické. Jak bylo ale uvedeno výše, některé typy pachatelů se mohou uchylovat také k útokům v podobě zavirování počítače či jiného elektronického zařízení oběti, a tedy následky v podobě škody na majetku oběti nelze vyloučit.

Lze se domnívat, že závažnost psychických následků trestného činu na oběť se bude odvíjet od intenzity a doby trvání jednání pronásledovatele a také od její osobnosti a schopností se se situací vypořádat. Pokud je jednání pachatele intenzivní, oběť neustále pociťuje jeho přítomnost a je ve stavu napětí. U obětí dochází často k narušení či absolutní ztrátě pocitu bezpečí v důsledku kterého se u nich objevují poruchy spánku a sebevražedné myšlenky[133]. V krajním případě může pachatel kyberstalkingu dohnat svým jednáním oběť k sebepoškozování nebo právě k sebevraždě[134] (a to přímým nabádáním k sebevraždě nebo nepřímým vyvíjením tlaku na oběť, který oběť neunese a spáchá sebevraždu).

Jednou z otázek, jež si viktimologie klade, je otázka podílu oběti na trestném činu, tedy zda oběť nějakým způsobem ke spáchání trestného činu přispěla. Pokud se jedná o stalking v jeho obecné podobě mezi bývalými partnery, bylo prokázáno, že nebyl-li vztah mezi osobami ukončen dostatečně jasně a definitivně a potenciální oběť v ex-partnerovi živí naději na další pokračování vztahu, existuje vyšší pravděpodobnost, že k jednání naplňujícímu znaky stalkingu

[131] Roubalová, M. a kol., 2019, op. cit., s. 88.
[132] Čírtková, L., 2013, op. cit., s. 254., Roubalová, M. a kol., 2019, op. cit., s. 88.
[133] Čírtková, L., 2013, op. cit., s. 254; Papakitsou, V. Cyberstalking, a new crime: The nature of cyberstalking victimization. *Dialogues in Clinical Neuroscience* [online]. 2020, 3(3), 197-202 [cit. 2020-05-23]. DOI: 10.26386/obrela.v3i3.162. ISSN 25852795, Dostupné z: https://www.obrela-journal.gr/index.php/obrela/article/view/162/169
[134] Smejkal, V., 2018, op. cit., s. 404.

ze strany odmítnutého partnera dojde[135]. Lze se domnívat, že také oběti kyberstalkingu přispívají určitou měrou k jednání kyberstalkera, a to svou otevřeností ohledně sdílení informací o své osobě, která může v potenciálním pachateli vzbudit zájem o takto snadno dosažitelný cíl. Z veřejných profilů na sociálních sítích může pachatel jednoduše zjistit, kde se oběť nachází, některé osoby zde také uvádí své e-mailové adresy i telefonní čísla, přičemž právě získání těchto kontaktů je základem trestné činnosti kyberstalkera.

Kyberstalking představuje vzhledem k psychickým následkům na jeho oběti velmi závažný jev. Moderní komunikační prostředky jsou dnes již běžnou součástí života a jejich používání se není možné vzdát. Přesto se lze domnívat, že ve srovnání se stalkingem v jeho tzv. off-line formě, tj. např. při fyzickém pronásledování oběti pachatelem, mají oběti větší příležitost zmírnit riziko viktimizace, a to především zvolením vhodného zabezpečení při používání těchto elektronických komunikačních prostředků.

4.3. Podvodná jednání na internetu

Pravděpodobně nejčetnějšími kybernetickými trestnými činy jsou trestné činy majetkové, které lze obvykle kvalifikovat jako trestné činy podvodu, případně úvěrového podvodu[136]. Souhrnně bývají označovány jako tzv. scamy a zahrnují například phishing, malware, hoax, podvodné loterie a nabídky, dárcovský scam apod[137]. Vzhledem k omezenému rozsahu práce bude v této kapitole bližší pozornost věnována pouze dvěma formám jednání z této kategorie, a to podvodům, k nimž dochází při nakupování na internetu a podvodným e-mailům.

Podvody při nakupování na internetu spočívají v jednání pachatele, který prostřednictvím internetu nabízí různé zboží nebo služby a poté, co si u něj oběť zboží objedná a zaplatí zálohu nebo celkovou cenu, pachatel zboží nebo služby nedodá a oběti se jej obvykle nepodaří kontaktovat. Pachatelé zboží či služby obvykle inzerují na věrohodně vypadajících webových stránkách, případně za účelem zvýšení důvěryhodnosti využívají k inzerci známé internetové portály a bazary, ve spojení s jejichž jmény nakupující ani nenapadne, že se by se mohlo jednat o podvodnou nabídku[138]. Jak se zdá, pachatelé podvodů na internetu se dopouštějí trestné činnosti bez jakýchkoli morálních zábran – z nabídky konkrétních produktů, kterými jsou často léky či neúčinné zdravotní pomůcky je patrné, že si jako oběti svých trestných činů

[135] Čírtková, L., 2014, op. cit., s. 56.
[136] Gřivna, T., Scheinost M., Zoubková I.: op. cit. sub 2, s. 421.
[137] Kolouch, J., 2016, op. cit., s. 235.
[138] Kolouch, J., 2016, op. cit., s. 240-243.

často vybírají osoby nemocné, které se nachází v bezvýchodné životní situaci a v nabízených produktech vidí naději na uzdravení[139]. Pachatelé jsou také schopni velmi pružně reagovat na poptávku vyvolanou konkrétními společenskými okolnostmi, například v době koronavirové pandemie bylo identifikováno množství podvodných e-mailů, jejichž předmětem byly nabídky „zázračných" antibakteriálních masek, cílem pachatele bylo však pouze vylákat z obětí peníze[140]. Podvodné e-maily představují jednu z technik tzv. sociálního inženýrství (viz bod 3.4.) a mohou mít podobu spamů, poplašných zpráv, podvodných nabídek apod [141]. Prostřednictvím e-mailů se může pachatel vydávající se za pracovníka banky například snažit z adresáta vylákat přihlašovací údaje do internetového bankovnictví či pro internetovou platbu kartou. E-mailová komunikace je dnes velmi rozšířeným prostředkem komunikace, lidé ji využívají jak pro pracovní, tak osobní komunikaci, a tak lze předpokládat velkou množinu potenciálních obětí těchto trestných činů.

Údaje o podvodných jednáních na internetu můžeme čerpat např. z výše představeného výzkumu *Institutu pro kriminologii a sociální prevenci* z roku 2019. Hlavní metodou výzkumu byl osobní rozhovor a celkem bylo provedeno 3393 rozhovorů. Cílovou skupinou byli obyvatelé České republiky starší 15 let. Ve výzkumném vzorku byli rovnoměrně zastoupeni muži i ženy různé úrovně vzdělání a věkových kategorií, přičemž věk nejmladších respondentů byl 15 let a nejstarších respondentů nad 60 let. Dotazník týkající se těchto trestných činů byl vzhledem ke specifičnosti kybernetické kriminality formulován odlišně od dotazníků týkajících se jiných trestných činů. Lze se domnívat, že vzhledem k velikosti výzkumného vzorku, zastoupení respondentů příslušících k různým skupinám z hlediska věku, pohlaví, vzdělání aj., ale také zohlednění specifik kybernetické kriminality při formulaci dotazníku, mohou být závěry výzkumu velmi relevantní.

Tabulka zachycuje podíl viktimizovaných obětí v uvedených obdobích:

Delikt	Obětí v posledních 12 měsících (%)	N
Podvod při internetovém nakupování	16, 0	1911
Podvodné e-maily	53,0	2403

[139] Česká obchodní inspekce. Rizikové e-shopy. [online]. [cit. 2020-03-01] Dostupné z: https://www.coi.cz/pro-spotrebitele/rizikove-e-shopy/
[140] ESET. Experti varují před podvodnými e-maily zneužívající obavy z koronaviru. [online]. [cit. 2020-03-01] Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/experti-varuji-pred-podvodnymi-e-maily-zneuzivajici-obavy-z-koronaviru/
[141] Kolouch, J., 2016, op. cit., s. 188.

Z výzkumu vyplývá, že se s podvodnými e-maily setkala více než polovina respondentů a s podvody při internetovém nakupování více než šestina respondentů, přičemž ve srovnání s ostatními delikty, které výzkum monitoroval byly tyto delikty celkově nejčastější. Další trestné činy bylo navíc za kybernetickými trestnými činy zaznamenány až s poměrně velkým odstupem (8,8 % respondentů se setkalo s vloupáním do chaty a 7,5 % s krádeží osobních věcí)[142]. Výsledky výzkumu rovněž podporují výše uvedená tvrzení o neustálém nárůstu kybernetické kriminality, jelikož na otázku, zda se setkali respondenti s podvody při internetovém nakupování nebo podvodnými e-maily v období před třemi lety, odpověděla většina z nich negativně.

4.3.1. Pachatelé podvodných jednání na internetu

S typologií pachatele podvodných jednání na internetu se v odborné literatuře nesetkáme a pravděpodobně ji pro rozmanitost podvodných jednání není možné ani vytvořit. Vzhledem ke skutečnosti, že spáchání tohoto trestného činu nevyžaduje zvláštní vzdělání pachatele v oblasti informačních technologií, lze se domnívat, že z hlediska věku a vzdělání představují pachatelé podvodů heterogenní skupinu. Jelikož se jedná o trestné činy majetkové, motivem pachatele bude nejčastěji vidina snadného zisku. Přestože je motiv podvodů poměrně jasný, nezůstávají jejich pachatelé zcela stranou výzkumů. Tyto především sociologické výzkumy se zaměřují zejména na příčiny vedoucí pachatele k rozhodnutí pro trestnou činnost jako způsob získání finančních prostředků, ačkoli by mohli stejně jako příslušníci nekriminální populace tyto prostředky získat například prací[143]. Z psychologického hlediska jsou motivy a cíle pachatelů totiž ve většině případů totožné jako motivy a cíle nekriminální populace, pachatelé pouze volí jiné (kriminální) prostředky k dosažení těchto cílů[144].

4.3.2. Oběti podvodů na internetu

Ohledně obecných poznatků o obětech kybernetických trestných činů *Roubalová* konstatuje, že je sice v praxi realizován výzkum a aplikovány preventivní nástroje, které cílí na nejohroženější skupiny, jako jsou děti a senioři, ale zbylá část populace stojí v tomto ohledu na

[142] Pozn.: Celkově bylo zkoumaných deliktů 14, Roubalová a kol., 2019, op. cit., s. 69.
[143] Tambe Ebot, A. C., Siponen, M. Towards a Rational Choice Process Theory of Internet Scamming: The Offender's Perspective. *International Conference on Information Systems*. 2014. [online]. [cit. 2020-03-01] Dostupné z: https://www.researchgate.net/publication/271527329_Towards_a_Rational_Choice_Process_Theory_of_Internet_Scamming_The_Offender's_Perspective
[144] Čírtková, L., 2013, op. cit., s. 81.

okraji zájmu[145]. V následující části textu se zaměříme na otázku, zda existuje typická oběť podvodů, které jsou páchány při nakupování na internetu a podvodných e-mailů a jaké jsou viktimogenní faktory u těchto jednání. Lze předpokládat, že i u těchto trestných činů pachatelé využívají zejména důvěřivosti a neopatrnosti obětí[146]. Faktorů, které však u osob vedou k tomu, že pachateli podlehnou a stanou se obětí jeho podvodného jednání však může být více v závislosti na tom, o jaké konkrétní jednání se jedná.

4.3.2.1.Oběti podvodů při nakupování na internetu

Základní podmínkou pro spáchání jakéhokoliv podvodu na internetu je samotné používání internetu potenciální obětí, frekvence používání a uskutečňování nákupů přes internet. Dle výsledků výzkumu internet používá 80 % respondentů, přičemž většina z nich jej používá denně. Bylo zaznamenáno, že určujícím faktorem pro používání a frekvenci používání internetu je především věk a sociální postavení respondenta, kdy internet častěji využívají osoby s vyšším vzděláním, dobře zajištění, studenti a podnikatelé. Nejvíce internet používají osoby v domácnosti, zejména jsou-li na mateřské dovolené[147].

Výhodami, které spotřebitelé spatřují v nakupování po internetu ve srovnání s nakupováním v kamenných obchodech, je zejména přehlednost nabízeného zboží, které lze na webových stránkách jednoduše vyhledat; různorodost nabízených produktů, jež není omezena „teritoriem“, na kterém se spotřebitelé pohybují, nýbrž je jim díky internetu umožněno nakupovat zboží také od zahraničních prodejců; soukromí při nakupování, cenová výhodnost, doručení až do domu a mnohé další[148]. Lze se domnívat, že potenciální obětí podvodu na internetu tak bude jakákoliv osoba, která vnímá tato kritéria jako činitel motivující ji k upřednostnění online nákupu před tzv. off-line nákupem.

V praxi se často setkáme se stereotypním názorem, podle kterého jsou nejčastější obětí internetových podvodů senioři, a to z důvodu nedostatečné orientace a nezkušenosti v oblasti informačních technologií. Tato premisa byla vyvrácena výše popsaným výzkumem, který naopak potvrdil vyšší riziko viktimizace u osob mladšího věku, které používají internet mnohem častěji než senioři. Další vysvětlení těchto výsledků uvádí *Ross*, dle kterého *„vyšší věk může působit jako ochranný faktor ve smyslu, že starší osoby budou méně často používat*

[145] Roubalová a kol., 2019, op. cit., str. 93.
[146] Kolouch, J., 2016, op. cit., s. 266.
[147] Roubalová a kol., 2019, op. cit., str. 94.
[148] Patro, C. S. Predicting Consumers' Acceptance of Online Shopping on the Internet: An Empirical Study. International Journal of Cyber Behavior, Psychology and Learning (IJCBPL), 8(1), 33-60. 2018. doi:10.4018/IJCBPL.2018010103, [online]. [cit. 2020-05-22]. Dostupné z: https://www-igi-global-com.ezproxy.is.cuni.cz/gateway/article/full-text-html/216982

internet k provedení finančních transakcí"[149]. Pokud je jedná o podvody při nakupování na internetu, lze očekávat, že se osoby vyššího věku rozhodnou obchod v případě, kdy jedinou možností platby je platba kartou, která musí být navíc provedena předem, vůbec nerealizovat. Lze se však domnívat, že vzhledem ke stále se zvyšující digitální gramotnosti populace se v průběhu následujících let stane věk jako rizikový faktor u trestných činů internetových podvodů irelevantním, a proto je třeba se zaměřit na jiné, více konstantní faktory[150].

Jak je možné dovodit z definice podvodného jednání, oběti internetových podvodů mohou v rámci primární viktimizace utrpět zejména majetkovou škodu. Výrazné psychické následky viktimizační výzkumy nepředpokládají, ale lze se domnívat, že oběť může trpět zvýšeným pocitem nedůvěry v souvislosti s uskutečňováním internetových transakcí. Pokud se jedná o majetkovou škodu, výzkum zaznamenal vznik této škody u 15 % respondentů, kteří alespoň jeden internetový nákup uskutečnili. Výsledky výzkumu ohledně otázky zkušenosti s podvodem při nakupování korespondují se statistikami IKSP, podle kterých podvod při nákupu na internetu v posledním roce (2017) zažilo 16 % lidí z těch, kteří na internetu v posledních třech letech nakoupili, přičemž oklamanými byli zejména studenti (patrně kvůli častějšímu nakupování na internetu)[151]. Průměrně škoda způsobená respondentům činila 2 300 Kč, nejvyšší uvedená škoda dosáhla 17 000 Kč. Můžeme doplnit, že popularita nakupování přes internet dle údajů Českého statistického úřadu neustále narůstá a tím se zvyšuje množství potenciálních obětí a příležitostí pro pachatele[152].

V návaznosti na kapitolu věnující se latenci kybernetické kriminality (bod 3.1.) je vhodné pojednat také o reakcích oklamaných obětí. Respondenti na zjištění podvodu nejčastěji reagovali přímým kontaktováním prodejce (75 %), policii informovalo pouze 8,4 % respondentů. Autoři výzkumu se shodují na tom, že důvodem pro neoznámení policii byla u většiny respondentů nízká výše škody, upozorňují však, že policii ani prodejce nekontaktovaly často ani osoby, kterým vznikla škoda v hodnotě desítek tisíc. Příčiny tohoto pasivního přístupu lze pravděpodobně spatřovat ve skutečnostech, o kterých bylo pojednáno výše, přičemž jedním z hlavních argumentů většiny osob patrně může být skepse k dopadení anonymně vystupujícího pachatele. Ohledně viktimogenních faktorů obětí podvodů při nakupování na internetu lze

[149] Norris, G., Brookes, A., Dowell, D. The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology*, 34, 231–245 (2019). https://doi.org/10.1007/s11896-019-09334-5 [online]. [cit. 2020-05-22]. Dostupné z: https://link.springer.com/article/10.1007/s11896-019-09334-5

[150] Český statistický úřad. Jak vysoká je digitální gramotnost obyvatel ČR? [online]. [cit. 2020-05-22]. Dostupné z: https://www.czso.cz/csu/stoletistatistiky/jak-vysoka-je-digitalni-gramotnost-obyvatel-cr/

[151] Ministerstvo vnitra, *Zpráva o situaci v oblasti vnitřní bezpečnosti,* 2019, op. cit., s. 16.

[152] Parlamentní listy. Český statistický úřad: Obliba nákupů přes internet nepřetržitě roste. [online]. [cit. 2020-05-22]. Dostupné z: https://www.parlamentnilisty.cz/zpravy/tiskovezpravy/Cesky-statisticky-urad-Obliba-nakupu-pres-internet-nepretrzite-roste-598809

shrnout, že nejvíce jsou patrně ohroženy osoby, které mají ve srovnání s ostatními relativně větší množství času, tj. studenti nebo např. osoby na mateřské dovolené a tento čas tráví právě na internetu.

4.3.2.2.Oběti podvodných e-mailů

Vzhledem k záměru zmapovat mimo dalších aspektů podvodných e-mailů rovněž výši způsobené škody se autoři výše popsaného výzkumu IKSP zaměřili pouze na e-maily požadující finanční plnění, tj. např. e-maily v podobě výzvy k úhradě neexistujícího dluhu, faktury za neobjednané zboží apod. Na základě výzkumu bylo zjištěno, že e-mailovou komunikaci používá 90 % respondentů, přičemž nejčastějšími uživateli byla skupina osob v rozmezí 31–35 let a z hlediska vzdělání osoby vysokoškolsky vzdělané, naopak senioři a osoby s nižším vzděláním využívají e-mail méně.

Polovina uživatelů e-mailové komunikace (1271 osob) uvedla, že v posledních 12 měsících obdržela podvodný e-mail, přičemž 86 % osob tyto e-maily obdrželo opakovaně. Adresáty podvodných e-mailů byli častěji muži s vysokoškolským vzděláním nebo podnikatelé. Celkem 90 % z těchto respondentů uvedlo, že na e-maily nereagovali. Zřejmě právě díky této skutečnosti pouze 8 respondentů utrpělo v souvislosti s podvodným e-mailem škodu, a to nejčastěji do výše 5 000 Kč. Stejně jako tomu bylo u podvodů spojených s nakupováním na internetu, i v tomto případě většina (6) respondentů kontaktovala za účelem odškodnění přímo odesílatele e-mailu. Pouze 2 osoby nahlásily případ policii a stejný počet osob se obrátil na zprostředkovatele internetové platby.

Lze dodat, že zvláštní typ obětí podvodných e-mailů představují oběti tzv. „romance scams“ – jejich pachatelé většinou prostřednictvím e-mailů, ale také různých seznamkových portálů nebo aplikací navážou s obětí romantický vztah, který již od počátku směřuje k získání finančních prostředků oběti. Z výzkumů zabývajících se tímto typem podvodů vyplývá, že obětí se ve více než 60 % stávají ženy středního věku, což může být dle autorů výzkumu způsobeno také tím, že představují v porovnání s mladými lidmi nebo seniory skupinu s relativně nejstálejšími příjmy, a proto pro ně finanční podpora jiné osoby nepředstavuje větší problém[153].

Z výsledků poměrně rozsáhlého výzkumu je patrné, že podvodnými jednáními na internetu je ohrožena velká část populace, přičemž potenciální obětí je prakticky každý, kdo používá internet. Rizikovým viktimním faktorem je zejména důvěřivost, proto lze obětem

[153] Whitty M. T. Do You Love Me? Psychological Characteristics of Romance Scam Victims. *Cyberpsychology, behavior and social networking*, 2018, *21*(2), 105–109. https://doi.org/10.1089/cyber.2016.0729 [online]. [cit. 2020-05-23]. Dostupné z: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5806049/

především doporučit důsledné ověřování původu nabídky například prostřednictvím monitoringu webových stránek České obchodní inspekce, která průběžně doplňuje seznam podvodných portálů[154].

Závěrem

V návaznosti na bližší zkoumání tří forem kybernetické trestné činnosti lze konstatovat, že v rámci jednotlivých forem je možné poměrně úspěšně vysledovat charakteristické znaky či alespoň kategorizaci pachatelů i obětí trestné činnosti. Pokud se jedná o oběti, lze shrnout, že zatímco například u podvodných jednání a kyberstalkingu je jediným viktimním znakem samotné používání počítačového či jiného zařízení obětí, u nenávistných trestných činů je nezbytné, aby oběť disponovala určitými charakteristickými znaky (nebo aby se pachatel alespoň domníval, že jimi disponuje). Z hlediska dopadu trestného činu na oběť byly identifikovány jak následky ve sféře finanční (u podvodných jednání na internetu, ale také kyberstalkignu), tak psychické (u všech typů jednání), což potvrzuje zjištění předchozích kapitol. Nejzávažnější psychické dopady na oběť lze předpokládat u kyberstalkingu, ale také nenávistných trestných činů. Lze také uzavřít, že existence předchozího vztahu pachatele nebyla prokázána jako podmínka pro spáchání ani jedné ze zkoumaných forem kybernetické trestné činnosti, jako nejpravděpodobnější se případně jeví u kyberstalkingu.

[154] Česká obchodní inspekce, op. cit.

5. Závěr

Cílem této diplomové práce bylo zejména analyzovat a shrnout kriminologické poznatky o pachatelích a obětech kybernetické trestné činnosti a odhalit a poukázat na specifika oproti pachatelům a obětem trestné činnosti, ke které nedochází v kyberprostoru.

Z hlediska historického vývoje kriminologického pohledu na pachatele kybernetické kriminality bylo zjištěno, že původní představy o pachateli jako IT profesionálovi již nereflektují dnešní realitu. Lze se sice stále setkat s kybernetickými trestnými činy, u nichž je nezbytnou vlastností pachatele pro spáchání trestného činu vyšší úroveň vzdělání v oblasti informačních technologií (jde-li např. o DDoS útoky nebo napadení počítače virem), velká část kybernetických trestných činů však může být spáchána pachatelem disponujícím pouze běžnou uživatelskou znalostí počítače a jeho základních funkcí. Tyto závěry lze odůvodnit především zvýšeným nápadem kybernetické trestné činnosti, kterou lze spáchat pouze s uživatelskou znalostí e-mailu nebo sociálních sítí – např. podvody, kyberstalking, nenávistné trestné činy, přičemž tyto znalosti jsou již v dnešní době vlastní většině světové populace.

Pokud jde o charakteristiku typického pachatele kybernetické kriminality, bylo zjištěno, že sice je možné identifikovat určité převažující znaky pachatelů kybernetické kriminality – pachatelem je nejčastěji muž do 35 let s vyšším vzděláním – tato zjištění však nemusí být nutně vypovídající pro konkrétní druh kybernetické trestné činnosti, jelikož kybernetická kriminalita zahrnuje velké množství rozmanitých forem této trestné činnosti. Ohledně zkoumání pachatelů kybernetické trestné činnosti lze uzavřít, že se jako vhodnější jeví sledovat podobnosti pachatelů již konkrétní formy kybernetické trestné činnosti, což bylo provedeno v části práce 4. Vhodným pomocným nástrojem pro vyšetřování kybernetické trestné činnosti se jeví být také popsané teoretické kategorizace pachatelů, jelikož umožňují zařadit pachatele do skupiny osob s podobnými znaky a lépe pochopit a případně také předvídat jeho jednání. Jako jeden z problematických aspektů páchání kybernetické kriminality byla identifikována organizovanost jejích pachatelů v organizovaných zločineckých skupinách, která umožňuje realizaci této trestné činnosti ve velkém rozsahu. Byly identifikovány specifické znaky těchto skupin oproti organizovaným zločineckým skupinám páchajícím jiné druhy kriminality, kterými je zejména geografická neomezenost těchto skupin a také v některých případech ospravedlňování jejich činnosti společenským zájmem či cílem. Také tyto poznatky je nezbytné zohlednit jak při odhalování trestné činnosti, tak její prevenci či predikci.

Ve vztahu k obětem trestné činnosti bylo nejprve poukázáno na jejich podíl na latenci kybernetické kriminality, která představuje jeden z nejproblematičtějších aspektů kybernetické

kriminality a byly podrobněji diskutovány důvody motivující oběti k nenahlašování této trestné činnosti. Dále bylo zjištěno, že oběti kybernetické kriminality jsou ohroženy primární, sekundární i terciární viktimizací, a to v podobě majetkové škody i nemajetkové újmy v závislosti na konkrétním kybernetickém trestném činu, přičemž bylo konstatováno, že závažnost následků je srovnatelná s následky trestné činnosti, ke které nedochází v kyberprostoru.

Z hlediska typologie obětí se dá říci, že konkrétní charakteristiku obětí je možné stejně jako u pachatelů vytvořit vždy až ve vztahu ke konkrétnímu kybernetickému trestnému činu, společným znakem všech obětí je obvykle důvěřivost a neopatrnost. Zajímavé poznatky z této části se týkají vztahu pachatele a oběti, kdy mezi kybernetickými trestnými činy nalezneme jak tzv. vztahové, tak nevztahové delikty, přičemž bylo poukázáno na to, že oběti mohou svým nerozvážným jednáním na internetu v mnohých případech pachatelům páchání trestné činnosti značně usnadnit. Za varující lze označit zjištění, že velmi velké míře jsou oběťmi kybernetické kriminality tzv. zvláště zranitelné oběti. V závěru této části byla pozornost věnována tzv. sociálnímu inženýrství, kterým pachatelé na oběti působí a možnostem jeho prevence.

Poslední část práce byla podrobněji věnována třem vybraným jednáním z oblasti kybernetické kriminality – nenávistným trestným činům, kyberstalkingu a podvodným jednáním na internetu a jejich obětem a pachatelům. Prostřednictvím analýzy těchto různorodých jednání bylo poukázáno na to, jak pestrou škálu trestných činů kybernetická kriminalita pokrývá a jak různorodé mohou být motivy jejích pachatelů, ale také skupina jejich obětí. Bylo zjištěno, že se kriminologické výzkumy začínají postupně více věnovat jednotlivým oblastem kybernetické kriminality, jejich pachatelům i obětem, což lze považovat za velmi pozitivní z hlediska prevence i represe. Také však byla identifikována skutečnost, že většinou kybernetických trestných činů je ohrožena skutečně téměř neomezená část populace, kdy často jediný viktimní faktor představuje pouhé používání internetu a zkušenost s kybernetickou kriminalitou má velké množství lidí. Pokud se jedná o viktimizaci, byla potvrzena zjištění z třetí části práce, tedy vznik škody v majetkové, tak nemajetkové sféře obětí. U nenávistných trestných činů byly jako sekundární následek identifikovány také dopady na společnost, která je těmito trestnými činy rozdělována, případně jsou touto činností viktimizovány i osoby, na které útok pachatele přímo necílil, ale z důvodu příslušnosti k napadené skupině jsou trestným činem zasaženy nepřímo.

Za důležitý poznatek práce lze označit také výrazné tendence k bagatelizaci kybernetické kriminality ze strany společnosti, ale také orgánů činných v trestním řízení a samotných obětí – společnost často vnímá oběť jako subjekt nesoucí alespoň částečnou vinu za

své jednání (např. u kyberstalkingu, ale i podvodů), orgány činné v trestním řízení někdy velmi negativně reagují na podněty o trestné činnosti (např. u kybergroomingu), oběti z různých výše analyzovaných důvodů trestnou činnost neoznamují. Všechny tyto faktory přispívají, k již tak problematické latenci kybernetické kriminality, ale také prohlubují primární viktimizaci oběti či způsobují její viktimizaci sekundární.

V diplomové práci bylo poukázáno také na nedostatky viktimologických výzkumů, které jsou často orientovány na velmi malý vzorek respondentů a jejich výsledky tak nemusí vždy dosahovat potřebné relevance. Lze předpokládat, že vhodným nástrojem pro získání co nejkvalitnějších poznatků z oblasti kybernetické kriminality se jeví být mezinárodní spolupráce či alespoň spolupráce mezi státy na evropské úrovni, která by mohla být zprostředkována některou mezinárodní organizací či institucí specializovanou na kybernetickou kriminalitu. Na úrovni Evropské unie se této problematice včetně výzkumu věnuje Evropské centrum pro boj proti kybernetické kriminalitě, spolupráce v této oblasti probíhá také z iniciativy Rady Evropy.

Závěrem lze shrnout, že kybernetická kriminalita představuje stále se rozšiřující kategorii trestné činnosti, přičemž její pachatelé a oběti reprezentují velmi heterogenní skupinu. Nejvhodnějším přístupem kriminologických výzkumů se tak jeví být zaměření na jednotlivé kybernetické trestné činy a jejich oběti tak, aby byly získány co nejrelevantnější poznatky pro oblast prevence této trestné činnosti. Lze se totiž domnívat, že právě prevence, zejména v podobě dostatečné osvěty společnosti, by mohla umožnit výraznou eliminaci alespoň některých kriminálních jednání, ke kterým na internetu dochází, přičemž tato prevence bude nejúčinnější, pokud bude cílena vhodnými nástroji na nejohroženější skupiny obětí.

Seznam použitých zdrojů

1. Seznam použité literatury

Čírtková, L. *Forenzní psychologie*. 3., upr. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013, 446 s. ISBN 978-80-7380-461-9.

Čírtková, L. *Viktimologie pro forenzní praxi*. Praha: Portál, 2014, 160 s. ISBN 978-80-262-0582-1.

Gřivna, T., Scheinost, M., Zoubková I. a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019, 588 s. ISBN 978-80-7598-554-5.

Jelínek, J. *Terorismus - základní otázky trestního práva a kriminologie*. Praha: Leges, 2017, 244 s. ISBN 978-80-7502-256-1.

Jirovský, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, 288 s. ISBN 978-80-247-1561-2.

Musil, S. *Počítačová kriminalita: nástin problematiky: kompendium názorů specialistů*. Praha: Institut pro kriminologii a sociální prevenci, 2000, 299 s. Studie (Institut pro kriminologii a sociální prevenci). ISBN 80-86008-80-0.

Smejkal, V. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, 934 s. ISBN 978-80-7380-720-7.

Smieško, I. *Internet a trestné činy extrémismu*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2017, 246 s. ISBN 978-80-7380-691-0.

Válková, H., Kuchta, J., Hulmáková, J. a kol. *Základy kriminologie a trestní politiky*. 3. vydání. Praha: C.H. Beck, 2019, 616 s. ISBN 978-80-7400-732-3.

Vegrichtová, B. *Extremismus a společnost*. 2. aktualizované a doplněné vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017, 320 s. ISBN 978-80-7380-665-1.

Završnik, A. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017, 148 s. ISBN 978-80-7552-758-5.

2. Seznam použitých internetových zdrojů

Aricak et al. in Armstrong, S. B., Dubow, E. F., Domoff S.E. *Adolescent coping: In-person and Cyber-victimization.* Journal of psychosocial research on cyberspace. Vol 13, No 4, 2019. [online]. [cit. 2020-04-07]. Dostupné z: https://cyberpsychology.eu/article/view/12559/10906

Centrum prevence rizikové virtuální komunikace. Kyberšina. Úvod do problematiky. E-bezpečí, 2016 [online]. [cit. 2020-03-15] Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/bud-v-bezpeci/78-bud-v-bezpeci-kybersikana/file

Centrum prevence rizikové virtuální komunikace. *Statistika kybernetické kriminality za rok 2019*. [online]. [cit. 2020-03-10]. Dostupné z: https://www.e-bezpeci.cz/index.php/z-jinych-webu/1749-statistika-kyberneticke-kriminality-za-rok-2019

Česká obchodní inspekce. Rizikové e-shopy. [online]. [cit. 2020-03-01] Dostupné z: https://www.coi.cz/pro-spotrebitele/rizikove-e-shopy/

Český statistický úřad. Jak vysoká je digitální gramotnost obyvatel ČR? [online]. [cit. 2020-05-22]. Dostupné z: https://www.czso.cz/csu/stoletistatistiky/jak-vysoka-je-digitalni-gramotnost-obyvatel-cr/

Dvořák, M. *Phishing, pharming a jejich trestněprávní postih.* Trestněprávní revue 4/2018, s. 84. [online]. [cit. 2020-03-01]. Dostupné prostřednictvím https://www.beck-online.cz/

European Crime Prevention Network. *Cybercrime: A theoretical overview of the growing digital threat.* 2016. [online]. [cit. 2020-03-07]. Dostupné z: https://eucpn.org/sites/default/files/document/files/theoretical_paper_cybercrime_.pdf,

Europol. *Internet organised crime threat assessment 2019* [online]. [cit. 2020-03-10]. Dostupné z: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

ESET. Experti varují před podvodnými e-maily zneužívající obavy z koronaviru. [online]. [cit. 2020-03-01] Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/experti-varuji-pred-podvodnymi-e-maily-zneuzivajici-obavy-z-koronaviru/

Hadzhidimova, L. I., Payne, B. K. The profile of the international cyber offender in the U.S. *International Journal of Cybersecurity Intelligence & Cybercrime*: *2(1),* 40-55, 2019 [online].

[cit. 2020-05-22]. Dostupné z: https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1012&context=ijcic

Hamuddin, B., Syahdan, S., Rahman, F., Rianita, D., Derin, T. (2019). Do They Truly Intend to Harm Their Friends?: The Motives Beyond Cyberbullying among University Students. *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL)*, 9(4), 32-44. doi:10.4018/IJCBPL.2019100103. [online]. [cit. 2020-05-22]. Dostupné z: https://www-igi-global-com.ezproxy.is.cuni.cz/gateway/article/full-text-html/241849.

Hanzelka J., Schmidt I. *Dynamics of Cyber Hate in Social Media: A comparative Analysis of Anti-Muslim Movements in the Czech republic and Germany*. International Journal of Cyber Criminology, January - June 2017, s. 152. [online]. [cit. 2020-03-01] Dostupné z: http://www.cybercrimejournal.com/Hanzelka&Schmidtvol11issue1IJCC2017.pdf

Henson, B., Reyns, B. W., Fisher, B. S. *Cybercrime Victimization.* The Wiley Handbook on the Psychology of Violence, 2016, s. 567 [online]. [cit. 2020-03-07]. Dostupné z: https://www.researchgate.net/publication/314826891_Cybercrime_Victimization

Keum, B. T. (2017). Qualitative Examination on the Influences of the Internet on Racism and its Online Manifestation. International Journal of Cyber Behavior, Psychology and Learning (IJCBPL), 7(3), 13-22. doi:10.4018/IJCBPL.2017070102 [online]. [cit. 2020-03-01] Dostupné z: https://www-igi-global-com.ezproxy.is.cuni.cz/gateway/article/full-text-html/190804

Koehler, C., Weber, M. (2018). "Do I really need to help?!" Perceived severity of cyberbullying, victim blaming, and bystanders' willingness to help the victim. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 12*(4), Article 4. https://doi.org/10.5817/CP2018-4-4. [online]. [cit. 2020-05-22] Dostupné z: https://cyberpsychology.eu/article/view/11451/10233

Kolouch, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7 [online]. [cit. 2020-03-14]. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf.

Kopecký, K. *Krátký úvod do sekundární viktimizace dětských obětí online vydírání*. E-bezpečí, 2012. [online]. [cit. 2020-03-15]. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/dalsi-temata/533-sekundarniviktimizace

Kopecký, K. *Kybergrooming. Nebezpečí kyberprostoru (studie).* E-bezpečí [online]. [cit. 2020-03-10]. Dostupné z: http://e-nebezpeci.cz/.

Kopecký, K. *Strategie manipulace dětí v online prostředích se zaměřením na tzv. kybergrooming.* Pediatr. praxi 2015; 16 (5), s. 209. [online]. [cit. 2020-03-01] Dostupné z: https://www.researchgate.net/profile/Kamil_Kopecky3/publication/280023825_Strategie_manipulace_deti_v_online_prostredich_se_zamerenim_na_tzv_kybergrooming/links/55c494c108aea2d9bdc32508.pdf

Kopecký, K., Szotkowsi R. Centrum prevence rizikové virtuální komunikace. Národní výzkum kyberšikany učitelů. Olomouc, 2016. [online]. [cit. 2020-03-01] Dostupné z: http://www.prevence-info.cz/sites/default/files/users/10/vyzkumnazprava.pdf

Kuchta, J. *Aktuální problémy počítačové kriminality včetně její prevence*. Časopis pro právní vědu a praxi 1/2016, s. 5. [online]. [cit. 2020-03-01]. Dostupné prostřednictvím https://www.beck-online.cz/

Macalíková, J. Policie ČR. *Kybernetické hrozby jsou stále aktuálnější*, 2014 [online]. [cit. 2020-03-07]. Dostupné z: https://www.policie.cz/clanek/kyberneticke-hrozby-jsou-stale-aktualnejsi.aspx

Marešová, A. Martinková M. O významu poznávání obětí trestné činnosti. Ministerstvo vnitra ČR. [online]. [cit. 2020-05-22]. Ke stažení: https://www.mvcr.cz/clanek/o-vyznamu-poznavani-obeti-trestne-cinnosti.aspx

McFarlen L. in Pittaro M. L. Cyber stalking: An Anylysis of Online Harassment and Intimidation. International Journal of Cyber Criminology, 2007, Vol. 1, Issue 2, [online]. [cit. 2020-03-01]. Dostupné z: http://www.cybercrimejournal.com/pittaroijccvol1is2.htm

Ministerstvo vnitra ČR. *Zpráva o projevech extremismu a předsudečné nenávisti na území České republiky v roce 2018,* Praha, 2019 [online]. [cit. 2020-03-01] Dostupné z: https://www.mvcr.cz/clanek/extremismus-vyrocni-zpravy-o-extremismu-a-strategie-boje-proti-extremismu.aspx

Ministerstvo vnitra ČR. *Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2018,* Praha, 2019, s. 47 [online]. [cit. 2020-03-14]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx

Národní centrum bezpečnějšího internetu. *Kybergrooming a kyberstalking.* 2012, s. 15 [online]. [cit. 2020-03-01] Ke stažení z: https://www.ncbi.cz/

Národní centrum kybernetické bezpečnosti. *Sociální inženýrství.* [online]. [cit. 2020-03-01] Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/

Norris, G., Brookes, A., Dowell, D. The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology*, 34, 231–245 (2019). https://doi.org/10.1007/s11896-019-09334-5 [online]. [cit. 2020-05-22]. Dostupné z: https://link.springer.com/article/10.1007/s11896-019-09334-5

Nurse, J. R. C., Bada, M. *The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations.* [online]. [cit. 2020-03-02]. Dostupné z: https://arxiv.org/pdf/1901.01914.pdf.

Nurse, J. R. C., Bada, M. *The social and psychological impact of cyber-attacks.* Benson & McAlaney (2019/20) Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press, 21 s. [online]. [cit. 2020-03-07]. Dostupné z: https://arxiv.org/ftp/arxiv/papers/1909/1909.13256.pdf

Papakitsou, V. Cyberstalking, a new crime: The nature of cyberstalking victimization. *Dialogues in Clinical Neuroscience* [online]. 2020, 3(3), 197-202 [cit. 2020-05-23]. DOI: 10.26386/obrela.v3i3.162. ISSN 25852795, Dostupné z: https://www.obrela-journal.gr/index.php/obrela/article/view/162/169

Parlamentní listy. Český statistický úřad: Obliba nákupů přes internet nepřetržitě roste. [online]. [cit. 2020-05-22]. Dostupné z: https://www.parlamentnilisty.cz/zpravy/tiskovezpravy/Cesky-statisticky-urad-Obliba-nakupu-pres-internet-nepretrzite-roste-598809

Patro, C. S. Predicting Consumers' Acceptance of Online Shopping on the Internet: An Empirical Study. International Journal of Cyber Behavior, Psychology and Learning (IJCBPL), 8(1), 33-60. 2018. doi:10.4018/IJCBPL.2018010103, [online]. [cit. 2020-05-22]. Dostupné z: https://www-igi-global-com.ezproxy.is.cuni.cz/gateway/article/full-text-html/216982

Policie ČR. Statistika kyberkriminality. Zveřejněné informace 2019. [online]. [cit. 2020-03-12]. Dostupné z: https://www.policie.cz/clanek/statistika-kyberkriminality.aspx

Požár, J. Vybrané trendy kybernetické kriminality. *Acta Informatica Pragensia* [online]. 2015, 4 (3): 366-348. [cit. 2020-03-10]. Dostupné z: https://aip.vse.cz/pdfs/aip/2015/03/11.pdf

Roubalová a kol. Institut pro kriminologii a sociální prevenci. *Oběti kriminality. Poznatky z viktimizační studie*, 2019, Praha, s. 93, [online]. [cit. 2020-03-14]. Dostupné z: http://www.ok.cz/iksp/docs/449.pdf

Smejkal, V. Kybernetická kriminalita – fenomén dneška. *Právní prostor.* [online]. 2015 [cit. 2020-03-10]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska

Šepec, M. Revenge pornography or non-consentual dissemination of sexually explicit material as a sexual offence or as a privacy violation offence. *International Journal of Cyber Criminology*, Volume: 13 I 2019, s. 420. [online]. [cit. 2020-04-06] Dostupné z: http://www.cybercrimejournal.com/MihaSepecVol13Issue2IJCC2019.pdf

Tambe Ebot, A. C., Siponen, M. Towards a Rational Choice Process Theory of Internet Scamming: The Offender's Perspective. *International Conference on Information Systems*. 2014. [online]. [cit. 2020-03-01] Dostupné z: https://www.researchgate.net/publication/271527329_Towards_a_Rational_Choice_Process_Theory_of_Internet_Scamming_The_Offender's_Perspective

United Nations Office On Drugs and Crime. *E4J University Module Series, Module 13: Cyber organized crime activities*. [online]. [cit. 2020-03-01]. Dostupné z: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html

Ústavní soud. *Zvláštní povaha a proměnnost tzv. trestných činů z nenávisti ukládá soudům povinnost posoudit povahu každého z takových útoků z perspektivy jeho potenciálních konkrétních obětí a prostředí (sociální sítě), ve kterém jsou páchány*. Brno, 2016. [online]. [cit. 2020-03-01] Dostupné z: https://www.usoud.cz/aktualne/zvlastni-povaha-a-promennost-tzv-trestnych-cinu-z-nenavisti-uklada-soudum-povinnost-poso/

Vakhitova, Z. a kol. *Offender – victim relationship and offender motivation in the context of indirect cyber abuse: A mixed-method explanatory analysis. International review of Victimology,* 2018, Vol. 24(3) 347-366. [online]. [cit. 2020-03-02]. Dostupné z: https://www.researchgate.net/publication/321000126_Offender-

Victim_Relationship_and_Offender_Motivation_in_the_Context_of_Indirect_Cyber_Abuse_A_Mixed-Method_Exploratory_Analysis

Walker, J. A., Jeske, D. Understanding Bystanders' Willingness to Intervene in Traditional and Cyberbullying Scenarios. *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL),* 2016, 6(2), 22-38. doi:10.4018/IJCBPL.2016040102. [online]. [cit. 2020-05-22] Dostupné z: https://www-igi-global-com.ezproxy.is.cuni.cz/gateway/article/full-text-html/158156

Whitty M. T. Do You Love Me? Psychological Characteristics of Romance Scam Victims. *Cyberpsychology, behavior and social networking*, 2018, *21*(2), 105–109. https://doi.org/10.1089/cyber.2016.0729 [online]. [cit. 2020-05-23]. Dostupné z: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5806049/

3. Seznam použitých právních předpisů

Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12.srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV, [online]. [cit. 2020-03-10]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32013L0040

Zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů

Zákon č. 40/2009 Sb., trestní zákoník

4. Seznam ostatních zdrojů

Clough, Jonathan. *Principles of Cybercrime.* Cambridge: Cambridge University Press, 2015. Chapter 1. DOI: 10.1017/CBO9780511845123. ISBN 9780511845123 (Pozn.: přístup byl poskytnut prostřednictvím KU Leuven v rámci studia předmětu Cybercrime z University Publishing Online)

Csonka, Peter. *The council of Europe's convention on cyber-crime and other European initiatives*. Revue internationale de droit pénal, 2006, s. 476. ISSN 0223-5404 (Pozn.: přístup k publikaci byl poskytnut prostřednictvím KU Leuven v rámci studia předmětu Cybercrime)

De Hert, P., González-Fuster, G., Koops, B. *Fighting cybercrime in the two Europes. The added value of the EU framework decision and The Council of Europe Convention*. International Review of penal law (Vol. 77), 2006. (Pozn.: přístup k publikaci byl poskytnut prostřednictvím KU Leuven v rámci studia předmětu Cybercrime)

Přednáška Mgr. Tomáše Brunera v rámci povinně volitelného předmětu Kybernetické kriminality a kybernetické bezpečnosti v zimním semestru 2019/2020.

Přednášky a konzultace v rámci předmětu *Cybercrime* na Katholiek Universiteit Leuven vedeného profesorem Michelem Panzavoltou v letním semestru akademického roku 2018/2019.

Přednášky doc. PhDr. Ludmily Čírtkové, CSc. v rámci předmětu Soudní psychologie v zimním semestru 2019/2020

Přednášky v rámci povinně volitelného předmětu Kybernetické kriminality a kybernetické bezpečnosti v zimním semestru 2019/2020

Kriminologické aspekty kybernetické kriminality

Abstrakt

Diplomová práce se zabývá pachateli a oběťmi kybernetické kriminality jako vybranými kriminologickými aspekty kybernetické kriminality. Cílem práce bylo zejména analyzovat a shrnout kriminologické poznatky o pachatelích a obětech kybernetické trestné činnosti a odhalit a poukázat na specifika oproti pachatelům a obětem trestné činnosti, ke které nedochází v kyberprostoru. Při zpracování diplomové práce byly použity jak tuzemské, tak zahraniční zdroje.

V první části jsou objasněny základní pojmy, se kterými tato diplomová práce pracuje, tedy pojem kybernetické kriminality, pachatele a oběti včetně zvláště zranitelné oběti.

Druhá část je věnována vývoji představ o pachateli kybernetické kriminality, jeho charakteristice ve srovnání s pachateli kriminality, k níž nedochází v kyberprostoru a jeho kategorizaci. Zvláštní pozornost je věnována organizovaným zločineckým skupinám v oblasti kybernetické kriminality a motivaci pachatele jako jednomu z kriminogenních faktorů této trestné činnosti.

Ve třetí části jsou diskutovány různé aspekty viktimologie zaměřené na oběti kybernetické kriminality včetně otázky dopadů této trestné činnosti na zvláště zranitelné oběti. V souvislosti s latencí kybernetické kriminality jsou vedle dalších příčin latence zkoumány důvody nenahlašování této trestné činnosti jejími oběťmi. Dále jsou analyzovány dopady kybernetické trestné činnosti na její oběti, vztah oběti a pachatele a metody sociálního inženýrství, které pachatel využívá ke spáchání trestného činu.

Čtvrtá část práce navazuje na závěry z předchozích částí zkoumáním tří konkrétních forem kybernetické trestné činnosti, a to nenávistných trestných činů, kyberstalkingu a podvodných jednání na internetu, přičemž pozornost je věnována opět charakteristice pachatelů a obětí těchto forem kybernetické trestné činnosti a formám viktimizace.

Klíčová slova: kybernetická kriminalita, pachatelé, oběti

Criminological aspects of cybercrime

Abstract

The thesis concerns the offenders and victims of cybercrime as the selected criminological aspects of cybercrime. The objective of the thesis was to particularly analyse and compare the criminological findings of the offenders and victims of cybercrime and discover and point out the specifics in comparison to the offenders and victims of the offline criminality. Both Czech and foreign literary sources were used for the purposes of this thesis.

In the first part the basic terms which are used in this thesis are clarified – cybercrime, the offender and victim including the particularly vulnerable victims.

The second part concerns the development of the image of the offender of cybercrime, his characteristics in comparison to the offenders of crimes committed out of cyberspace and his categorization. Particularly the attention was brought to the organized groups of criminals in the area of cybercrime and the motivation of the offender as one of the criminogenic factors.

In the third part different victimological aspects of cybercrime including the impact of this kind of criminality on the particularly vulnerable victims are discussed. In relation to the latency of cybercrime the causes of this latency including the reasons for not reporting this kind of criminality are examined. Furthermore, the impact of cybercrime on its victims, the relationship between the victim and offender and the methods of social engineering used by the offender to commit the crime are analysed.

The fourth part of this thesis develops the conclusions from the previous parts by examining three particular forms of cybercrime – online hate crimes, cyberstalking and online frauds while the attention is brought to the characteristics of the offenders and victims of this criminality and the forms of victimization.

Key words: cybercrime, offenders, victims