UNIVERZITA KARLOVA

Právnická fakulta

Alexandra Eliášová

Kriminalizace útoků na informační systémy

Diplomová práce

Vedoucí diplomové práce: JUDr. Dalibor Šelleng, Ph.D.

Katedra trestního práva

Datum vypracování práce (uzavření rukopisu): 15. 9. 2020

ČESTNÉ PROHLÁŠENÍ

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 diplomové práce včetně poznámek pod čarou má 238 534 znaků včetně mezer.

V Praze dne ……. ……

Alexandra Eliášová

PODĚKOVÁNÍ AUTORA

Zde chci poděkovat JUDr. Daliboru Šellengovi, Ph.D., za jeho vstřícný přístup a za jeho cenné připomínky a rady při zpracovávání této práce. Ráda bych také poděkovala své rodině a příteli za podporu.

OBSAH

Seznam grafů 1

Seznam tabulek 1

Úvod 2

1. Kybernetická kriminalita 4

1.1 Základní pojmy 4

1.2 Specifické aspekty kyberprostoru 6

2. Mezinárodní instrumenty v boji proti kyberkriminalitě 8

2.1 Evropská unie 8

2.1.1 Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) 11

2.1.2 Europol a Evropské centrum pro boj proti kyberkriminalitě (EC3) 11

2.2 Rada Evropy 13

2.2.1 Úmluva Rady Evropy o počítačové kriminalitě 13

2.2.2 Konference Octopus 14

2.2.3 Cybercrime Convention Committee (T-CY) a Cybercrime Programme Office of the Council of Europe (C-PROC) 16

2.3 Organizace spojených národů 17

2.4 Severoatlantická aliance 18

3. Kyberútoky 22

3.1 Útoky proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů 22

3.1.1 Hacking 22

3.1.2 Phishing 24

3.1.3 Sniffing a spoofing 25

3.1.4 Phreaking 25

3.1.5 Man-in-the-middle attack 26

3.1.6 Malware 26

3.1.7 DoS a DDoS útok 27
3.1.8 Zneužívání zařízení 27
3.2 Útoky související s počítačem 28
3.2.1 Počítačové padělání 28
3.2.2 Počítačový podvod 28
3.2.3 Kyberterorismus 29
3.3 Útoky související s obsahem 29
3.3.1 Dětská pornografie 29
3.3.2 Kybergrooming 30
3.3.3 Kyberšikana 30
3.3.4 Hoax 31
3.3.5 Dark web 31
3.3.6 Kyberextremismus 32
3.4 Útoky týkající se porušení autorského práva a práv souvisejících s právem autorským 32
3.4.1 Peer-to-peer 32
3.4.2 File hosting 33
3.4.3 Warez 34
3.4.4 Embedded link 34
3.4.5 Cybersquatting a typosquatting 34
4. Vyšetřování kyberkriminality 35
4.1 Pachatel 35
4.2 Motiv 39
4.3 Digitální důkazy 42
4.4 Vyšetřování 48
5. Současná česká právní úprava 62
5.1 Trestné činy proti majetku 65
5.1.1 Podvod (§ 209 TZ) 65

5.1.2 Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ).....66

5.1.3 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ) 69

5.1.4 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZ) 70

5.2 Trestné činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství 71

5.3 Trestné činy proti České republice, cizímu státu a mezinárodní organizaci..... 73

5.4 Trestné činy proti lidské důstojnosti v sexuální oblasti 74

5.5 Trestné činy hospodářské 78

5.6 Trestné činy proti pořádku ve věcech veřejných..... 83

6. Současné technologické trendy 85

6.1 Umělá inteligence..... 85

6.2 Cloudová úložiště..... 91

6.3 Virtuální měny 94

6.4 Internet věcí..... 98

Závěr 103

Seznam používaných zkratek..... 106

Seznam použitých zdrojů..... 112

Seznam použité literatury..... 112

Seznam použitých internetových zdrojů 118

Seznam použitých právních předpisů..... 125

Seznam použité judikatury 126

Seznam ostatních zdrojů 128

Přílohy..... 129

Název diplomové práce v českém jazyce 130

Abstrakt..... 130

Klíčová slova 130

Název diplomové práce v anglickém jazyce..... 131

Abstract..... 131

Keywords 131

SEZNAM GRAFŮ

Graf 1 Nápad trestné činnosti kybernetické kriminality a kriminality páchané na internetu 2011–2019 62

SEZNAM TABULEK

Tabulka 1 Dimenze kybernetické bezpečnosti 8

Tabulka 2 Motivace pachatelů 40

Tabulka 3 Počet zjištěných trestných činů zahrnutých pod pojem počítačová kriminalita v letech 1993-1997 63

Tabulka 4 Dělení skutkových podstat do pěti skupin 64

ÚVOD

Kyberkriminalita je v současné době velice aktuální téma. Každý rok se informační technologie čím dál více rozvíjí. Veškerá technická zařízení se stávají rychlejšími, výkonnějšími a používanějšími v každodenním životě. Kybernetický prostor se neustále zvětšuje a tak, jak se celý svět pomocí informačních technologií propojuje, zvyšuje se jeho komplexnost. Útoky jsou již v dnešní době velmi sofistikované a vzhledem k anonymitě internetu je velmi těžké odhalit skutečného pachatele.

Celá společnost je závislá na správném fungování informačních technologií a jakýkoliv útok na ně ji může zcela ochromit. Technologická závislost se projevuje mimo jiné i v oblastech na úrovni řízení státu, jako jsou komunikační infrastruktura, energetická oblast, zdravotnictví, doprava a další. Stát je ohrožován také kyberšpionáží, kdy útočníci získají citlivá data za účelem nabytí převahy v důležitých oblastech, jako jsou politika, diplomacie, ekonomika a další.

Kybernetický prostor je velmi dynamický a je poměrně náročné flexibilně reagovat na změny v něm probíhající. Z toho důvodu je důležitá hlavně prevence. Prostřednictvím bezpečnostních opatření jednotlivých institucí je snaha zabránit jakýmkoliv útokům na informační systémy, a zajistit tak kybernetickou bezpečnost. Součástí prevence jsou také včasná varování, díky kterým se příslušné subjekty dozví o kybernetickém útoku a jsou schopné na něj rychle a účinně reagovat.

Vzhledem k propojenosti celého světa prostřednictvím kyberprostoru a vzhledem k tomu, že kybernetické útoky neznají hranice, je kladen velký důraz na mezinárodní spolupráci. Kybernetická bezpečnost je řešena jak na úrovni samotného státu, tak i na úrovni Evropské unie, Rady Evropy, OECD, OSN či NATO. V rámci těchto institucí byly zřízeny specializované orgány – Agentura Evropské unie pro bezpečnost sítí a informací (ENISA), Cybercrime Convention Comittee (T-CY) a NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE). K posílení spolupráce mezi státy v této oblasti se pravidelně konají odborné konference, jako je například NIAS – největší NATO konference v oblasti kybernetické bezpečnosti, nebo konference Octopus, kterou každoročně pořádá Rada Evropy.

Hlavním cílem této práce je zjistit, jaké útoky na informační systémy představují hrozbu pro stát, jak se s nimi lze vypořádat z hlediska vyšetřování, zda představují nové

technologické trendy v oblasti útoků na informační systémy výzvu pro současnou českou právní úpravu v oblasti trestního práva, a nakonec prezentovat návrhy řešení *de lege ferenda*. Práce si klade za cíl zjistit, jaké jsou výkladové problémy právní úpravy a jaká jsou úskalí v souvislosti s umělou inteligencí, cloudovými úložišti, virtuální měnou a internetem věcí. Metodologie se napříč touto prací různí. K naplnění cíle práce je použita především analytická metoda spolu se syntézou. V některých částech je pak užíván přístup empirický.

V teoretické části vychází práce zejména z odborné literatury. Z české literatury je nejčastějším zdrojem publikace Kybernetická kriminalita[1], Kyberkriminalita a právo[2] a CyberCrime[3], ze zahraniční literatury je stěžejní dílo Principles of Cybercrime[4]. Dále práce čerpá z velkého množství odborných článků, především zahraničních, jelikož v novinách je velmi často o jednotlivých útocích pojednáváno. Práce čerpá také z primárních zdrojů, což je zejména zákon č. 40/2009 Sb., trestní zákoník, zákon č. 141/1961 Sb., o trestním řízení soudním, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a zákon č. 127/2005 Sb., o elektronických komunikacích, a dále vychází z dokumentů EU, Rady Evropy, OSN a NATO. V praktické části využívá tato práce komentářové literatury, soudních rozhodnutí, příspěvků z odborných konferencí pořádaných mezinárodními organizacemi, odborných článků a statistických údajů.

Diplomová práce vychází z právního stavu platného ke dni 10. září 2020.

---

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

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

[3] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8.

[4] CLOUGH, Jonathan. *Principles of cybercrime*. Cambridge, UK ; New York: Cambridge University Press, 2010. ISBN 978-0-521-89925-3.

1. KYBERNETICKÁ KRIMINALITA

1.1 Základní pojmy

Již v roce 1948 definoval Norbert Wiener, zakladatel kybernetiky, pojem kybernetika jako „*vědu o řízení a komunikaci v živých organismech a strojích*“[5]. Následně tak pojmenoval i svou knihu.[6] V této definici autor kombinuje komunikaci a řízení, kdy běžný rozhovor mezi dvěma lidmi vlastně není nic jiného než řízené předávání informací. „*Pokud chci, aby mé řízení bylo efektivní, musím vzít na vědomí jakoukoliv zprávu od druhé osoby, která ukazuje, zda příkaz je chápan a uposlechnut*.“[7] Zde narážíme na to, co vlastně znamená informace. Podle Wienera je „*informace pouhý název pro obsah, který je vyměňován s vnějším světem, tak jak se mu přizpůsobujeme a působíme na něj svým přizpůsobováním*.“[8]

Kybernetické útoky jsou zaměřeny na informační systémy, ve kterých dochází pomocí informačních technologií ke zpracovávání informací.[9] Kyberútoky mohou informace narušit buď z kvalitativní stránky, kdy se jedná o zásah do individuálních práv jednotlivce, nebo narušují informace z kvantitativní stránky, kdy ovlivňují množství informací v datové základně nebo jejich propustnost.[10]

Kybernetická kriminalita (angl. *cybercrime*), tzv. kyberkriminalita, je v současné době velmi užívaný pojem, není ale jednoduché říci, co vše tento pojem zahrnuje. Podle Jirovského se jedná o kriminalitu „*namířenou proti počítačům, jejich hardwaru, softwaru, datům, sítím apod., nebo v ní vystupuje počítač pouze jako nástroj pro páchání*

---

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

[6] WIENER, Norbert. *The Human Use of Human Beings: Cybernetics and Society*. London: Free Association Books, 1989. ISBN 978-1-85343-075-6.

[7] Ibid., s. 16.

[8] Ibid., s. 17.

[9] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 38. ISBN 978-80-7380-720-7.

[10] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 24–25. ISBN 978-80-903786-7-4.

trestného činu, případně počítačová síť a k ní připojená zařízení jsou prostředím, v němž se taková činnost odehrává.“[11] Jiní autoři označují kybernetickou kriminalitu jako „*trestný čin související s technologiemi, počítači a internetem, který má za následek poškození majetku a/nebo osob*“.[12] Až v roce 2013, kdy Česká republika ratifikovala Úmluvu o počítačové kriminalitě, se tento pojem objevil v našem právním řádu.

Počítač, jako předmět útoku, je jakékoliv programovatelné zařízení. Každý počítač je tvořen dvěma nezbytnými složkami, a to hardwarem a softwarem. Hardware jsou všechny komponenty (např. disk, procesor, operační paměť, grafická karta), které se nacházejí uvnitř skříně počítače, a dále ty komponenty, které jsou k němu připojeny (např. myš, klávesnice či monitor). Software je programové vybavení a umožňuje počítač ovládat a plně využívat.[13] Počítačový systém je mnohdy používán jako synonymum k pojmu počítač. Jediným rozdílem, který je v literatuře zdůrazňován, je, že počítačový systém zahrnuje i síťově připojená zařízení.[14]

Veškeré útoky na informační systémy probíhají v kybernetickém prostoru (či kyberprostoru, angl. *cyberspace*), a proto je nutné pochopit, co vše tento prostor zahrnuje. Vůbec s prvním vysvětlením pojmu přišel v roce 1982 William Gibson, který jej chápal jako halucinaci, kterou lidé pociťují každý den.[15] V zákoně o kybernetické bezpečnosti je kybernetický prostor definován jako digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.[16] Zjednodušeně lze říci, že je to sdílený prostor bez jakékoliv hmotné podstaty, kde dochází k výměně informací mezi jednotlivými subjekty a systémy

---

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

[12] SCHELL, Bernadette H a Clemens MARTIN. *Cybercrime: a reference handbook*. Santa Barbara, Calif.: ABC-CLIO, 2004, s. 225. ISBN 978-1-85109-683-1.

[13] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 26–30. ISBN 978-80-7380-720-7.

[14] GŘIVNA, Tomáš. § 230 [Neoprávněný přístup k počítačovému systému a nosiči informací]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2306. ISBN 978-80-7400-428-5.

[15] GIBSON, William. *Neuromancer*. 20th anniversary ed. New York: Ace Books, 2004, s. 69. ISBN 978-0-441-01203-9.

[16] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), § 2 písm. a).

navzájem.[17] Autoři Schell a Martin označují kyberprostor jako „*nervový systém globální ekonomiky*“.[18]

Data[19] představují jakoukoliv informaci, která je v takové podobě, aby byla vhodná pro komunikaci, uchování nebo zpracování.[20] Počítačová data můžeme chápat jako jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.[21]

1.2 Specifické aspekty kyberprostoru

Pojetí kyberprostoru s sebou přináší celou řadu problémů. Především je to absence centrální autority, která by nad kyberprostorem dohlížela. To je ale zároveň i primárním důvodem vzniku kyberprostoru, což dokládá i Deklarace nezávislosti Kyberprostoru[22], kterou v roce 1996 zveřejnil John Perry Barlow, zakladatel organizace Electronic Frontier Foundation. Kyberprostor by podle něj měl zůstat nezávislý a svobodný, a to hned ze tří důvodů. Není zde žádná vůle „*virtuálních realit*“ k uzavření společenské smlouvy, která by založila fungování autority, dále taková autorita ani není potřebná, vzhledem k tomu, že si uživatelé nastalé problémy mohou vyřešit sami, a Barlow také argumentuje neefektivností států v oblasti kyberprostoru.[23]

Dalším problematickým aspektem je jeho dostupnost a nízké náklady. Dnes si prakticky každý člověk může dovolit do kyberprostoru vstoupit. Postačí mu k tomu jakékoliv

---

[17] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 130–131. ISBN 978-80-7380-720-7.

[18] SCHELL, Bernadette H a Clemens MARTIN. *Cybercrime: a reference handbook*. Santa Barbara, Calif.: ABC-CLIO, 2004, s. 225. ISBN 978-1-85109-683-1.

[19] K rozdílu „nosič informací“ vs. „nosič dat“ blíže kapitola 5.1.2 (§ 230 odst. 2).

[20] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 35–36. ISBN 978-80-7380-720-7.

[21] Sdělení Ministerstva zahraničních věcí č. 104/2013 Sb.m.s., o sjednání Úmluvy o počítačové kriminalitě, článek 1 písm. b).

[22] BARLOW, John Perry. A Declaration of the Independence of Cyberspace. *Electronic Frontier Foundation* [online]. 20. leden 2016 [vid. 2019-03-31]. Dostupné z: https://www.eff.org/cyberspace-independence

[23] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 18–21. ISBN 978-80-903786-7-4.

zařízení, které lze k připojit k síti. Pokrytí Wi-Fi sítí je dnes velice široké a umožňuje každému připojit své zařízení, stejně tak mohou uživatelé využívat i dnes již většinou neomezená datová připojení. Kyberútoky proto mohou být prováděny kýmkoliv jak z pohodlí domova, tak z jakéhokoliv jiného místa na světě, a to proti komukoliv.

Kyberprostor je všudypřítomný, místně neomezený a velká část útoků má přeshraniční charakter. Útočník může sídlit v Německu, útoky provádět přes servery umístěné v Rusku a cíl útoku se může nacházet v USA, ale server dané společnosti, vůči které útok směřuje, se může nacházet v Číně. Je velmi těžké vysledovat, odkud útoky směřují, a pod jakou jurisdikci konkrétní případ spadá. Poslední dobou se navíc rozšířilo užívání VPN[24], a tak se situace ještě více komplikuje. Jakýkoliv uživatel v kyberprostoru musí počítat s tím, že může být kdykoliv postaven před soud kdekoliv na světě.[25]

S tím souvisí i anonymita uživatelů v kyberprostoru. Každému uživateli je přiřazena IP adresa, a tak je zakrytá jeho pravá identita. Spíše ti zkušenější uživatelé mohou IP adresu zjistit a lokalizovat. Kdo se za IP adresou skrývá, je možné zjistit pomocí ISP – poskytovatele internetového připojení – ale to samozřejmě není umožněno každému a takové prostředky využívají až policejní orgány v rámci trestního řízení.

Odhalování trestné činnosti v kyberprostoru ztěžuje vysoká latence. Mnoho obětí (např. banky, školy, větší společnosti) kyberzločinů totiž není ochotno podat trestní oznámení vzhledem k tomu, jaký by to mělo dopad pro veřejné mínění. Útoky na jejich servery a například ohrožení osobních údajů klientů by mohlo poškodit jejich dobrou pověst. Oběti se také mohou dozvědět, že jsou napadeny až se značným zpožděním.

---

[24] VPN (Virtual Private Network) umožňuje šifrované připojení k jiné síti, většinou zahraniční. Jakákoliv aktivita uživatele se poté jeví, jako by pocházela právě z příslušeného serveru. Uživatel je poté úplně anonymní. Dnes existuje mnoho služeb, které toto připojení umožňují, ať už zdarma či formou měsíčního předplatného. Jedná se například o NordVPN, Windscribe, CyberGhost či ExpressVPN. Služba umožňuje i obcházet polohové služby, kdy se uživatel může připojit k serverům v USA, UK či jinde ve světě a využívat tak služby, které jsou v jeho poloze nepřístupné.

[25] GROOTERS, Howard J. Territorial Jurisdiction in Cyberspace. *Oregon Review of International Law* [online]. 2002. Dostupné z: https://heinonline.org/HOL/P?h=hein.journals/porril4&i=5

2. MEZINÁRODNÍ INSTRUMENTY V BOJI PROTI KYBERKRIMINALITĚ

Vzhledem k tomu, že kyberprostor nezná hranice a kyberútoky probíhají napříč státy, je třeba, aby existovaly mezinárodní instrumenty umožňující boj s kyberkriminalitou. V poslední době se zvyšují zejména obavy z teroristických či politicky motivovaných útoků, které by mohly ohrozit klíčovou státní infrastrukturu a životy velkého množství lidí. Je tedy zásadní posílit mezinárodní spolupráci a koordinaci. Právní úprava existuje na úrovni EU, Rady Evropy, OSN i NATO. Působení jednotlivých mezinárodních organizací přibližuje tabulka[26].

Tabulka 1 Dimenze kybernetické bezpečnosti

	EU	**Rada Evropy**	**OSN**	**NATO**
Internet Governance	✓	✓	✓	
Cyber Crime	✓	✓	✓	
Cyber Terrorism			✓	✓
Cyber Warfare			✓	✓

2.1 Evropská unie

Boj proti kyberkriminalitě představuje nejvyšší politickou prioritu EU v oblasti organizované a vážné mezinárodní trestné činnosti.[27] Na úrovni EU jsou nejčastěji přijímána rámcová rozhodnutí, směrnice, sdělení či nařízení. Mezi nejvýznamnější předpisy patří směrnice č. 2011/93/EU, směrnice č. 2013/40/EU a směrnice č. 2019/713.

---

[26] TIKK, Eneken. Global Cybersecurity–Thinking About the Niche for NATO. *SAIS Review* [online]. 2010, **30**, 105–119. Dostupné z: doi:10.1353/sais.2010.0012

[27] CHRISTOU, George. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. 2016, s. 89. ISBN 978-1-137-40052-9.

V roce 2018 byla Evropskou komisí předložena legislativa týkající se elektronických důkazů – nařízení o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech a směrnice, kterou se stanoví harmonizovaná pravidla pro jmenování právních zástupců za účelem shromažďování důkazů v trestním řízení.

V roce 2017 bylo přijato Společné sdělení Evropskému parlamentu a Radě s názvem „Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU“. V tomto dokumentu jsou stanoveny priority EU v oblasti zajištění větší odolnosti EU před kybernetickými útoky, kdy mezi nejdůležitější patří komplexní přístup a zavedení struktur, které umožní rychlou a účinnou reakci všech subjektů. Cílem je zavedení jednotného režimu certifikace kybernetické bezpečnosti, zabezpečení kritické aplikace obsluhující automobily, letadla či elektrárny, dále zajištění rychlé výměny informací mezi subjekty, posílení šifrování klíčových systémů, zvýšení povědomí lidí o kybernetické bezpečnosti a zvýšení informovanosti o online dezinformačních kampaních.[28]

Pro koordinaci orgánů, institucí a agentur EU bylo vytvořeno speciální centrum CERT-EU s cílem reagovat na počítačové hrozby. Významný podíl na spolupráci v oblasti zajišťování kyberbezpečnosti EU má také INTCEN (European Union Intelligence and Situation Centre). Dále by mělo být vytvořeno Evropské výzkumné a odborné středisko pro kybernetickou bezpečnost. Právě v něm by se odborníci soustředili na rozvoj technologií a na výzvy, které přináší umělá inteligence, kvantová výpočetní technika, blockchain či elektronická identita.

Směrnice č. 2011/93/EU o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii ze dne 13. prosince 2011 upravuje trestné činy pohlavního zneužívání, pohlavního vykořisťování, dětské pornografie a trestný čin navazování kontaktu s dětmi k sexuálním účelům. Tyto závažné trestné činy vyžadují komplexní přístup při jejich vyšetřování a stíhání. Směrnice si dává za cíl zejména dosažení souladu právních předpisů členských států, dále klade důraz na účinné využívání dostupných nástrojů pro konfiskaci výnosu z trestné činnosti, zabránění sekundární viktimizace obětí, usnadnění oznamování těchto trestných činů, vybízení osob k oznamování podezření ze spáchání trestného činu, a velký důraz je kladen na ochranu dětských obětí

[28] Společné sdělení Evropskému parlamentu a Radě ze dne 13. 9. 2017 „Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU“.

a zohledňování jejich potřeb. Problematickým aspektem je tzv. sexuální turistika[29], takže je třeba změnit pravidla soudní příslušnosti pro zajištění trestního stíhání pachatelů.[30]

Směrnice č. 2013/40/EU o útocích na informační systémy byla přijata 12. srpna 2013 a upravuje trestný čin neoprávněného přístupu k informačním systémům, neoprávněného zasahování do informačních systémů, neoprávněného zasahování do údajů a sledování údajů. Vzhledem k tomu, že kyberútoky mohou způsobit rozsáhlé hospodářské škody, je třeba zavést přísnější sankce za trestné činy spáchané v rámci zločinného spolčení, dále sankcionovat vytváření botnetů, které umožňují dálkové ovládání velkého množství počítačů a dále zabránit krádežím totožnosti. Pro účinné potírání kyberútoků je třeba úzká spolupráce veřejnoprávního a soukromoprávního sektoru a zejména zvýšení odolnosti informačních systémů a ochrana kritické infrastruktury států.[31]

Směrnice č. 2019/713 ze dne 17. dubna 2019 o potírání podvodů v oblasti bezhotovostních platebních prostředků a jejich padělání upravuje trestný čin podvodného použití bezhotovostních platebních prostředků, trestné činy související s podvodným použitím hmotných a nehmotných bezhotovostních platebních prostředků. Platební podvody představují zdroj příjmů pro organizovanou trestnou činnost a ztěžují vytvoření jednotného digitálního trhu, a proto je důležité tyto trestné činy stíhat. Vzhledem k přeshraničnímu charakteru útoků je třeba zejména úzká spolupráce států, vytvoření společných definic a zaujetí jednotného přístupu vůči znakům skutkových podstat trestných činů. Je důležité reflektovat technologický vývoj a zahrnout do definic i virtuální měny, jako bezhotovostní platební prostředky, a zohlednit užívání mobilních aplikací a autorizačních prvků při provádění plateb.[32]

---

[29] Sexuální turistika je trestná činnost, kdy pachatel vycestuje do zahraničí a tam pohlavně vykořisťuje děti.

[30] Směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV [ÚV L 335/1].

[31] 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 [ÚV L 218/8].

[32] Směrnice Evropského parlamentu a Rady 2019/713 ze dne 17. dubna 2019 o potírání podvodů v oblasti bezhotovostních platebních prostředků a jejich padělání a o nahrazení rámcového rozhodnutí Rady 2001/413/SVV [ÚV L 123/18].

2.1.1 Agentura Evropské unie pro kybernetickou bezpečnost (ENISA)

Agentura Evropské unie pro kybernetickou bezpečnost vznikla v roce 2004 a sídlí v řeckém Heraklionu. Právním základem je nařízení Evropského parlamentu a Rady č. 2019/881 ze dne 17. dubna 2019, ve kterém je mimo jiné upravena i organizační struktura této agentury, skládající se ze správní rady, výkonné rady, výkonného ředitele, poradní skupiny agentury ENISA a sítě národních styčných úředníků.[33]

Cílem této agentury je dosažení vysoké kybernetické bezpečnosti v celé Evropě. Činí tak prostřednictvím posilování důvěryhodnosti produktů, služeb a procesů týkajících se kybernetické bezpečnosti, kooperace s členskými státy EU, sdílení znalostí, budování kapacit a zvyšováním povědomí o bezpečnosti v kyberprostoru. Kvůli výskytu onemocnění COVID-19 se převážná většina lidí přesunula do kyberprostoru, ať už z důvodu práce či online výuky. Koronavirová pandemie tak zdůraznila potřebu zajištění vyšší bezpečnosti v online prostředí, zejména v oblasti elektronického obchodování a online plateb, ale také v oblasti zdravotnictví.[34]

ENISA vypracovala studii týkající se bezpečnosti cloud computingu a big dat[35], ochrany osobních údajů, technologie zvyšující ochranu soukromí, elektronické identifikace a odhalování kybernetických hrozeb.

2.1.2 Europol a Evropské centrum pro boj proti kyberkriminalitě (EC3)

Evropské centrum pro boj proti kyberkriminalitě (EC3) bylo zřízeno v roce 2013 v rámci Europolu s cílem posílit infrastrukturu před kyberútoky. EC3 za roky své činnosti významně přispělo k účinnému boji s kyberkriminalitou, a to zejména díky velkému množství operací a rozsáhlým analýzám souborů, z nichž se převážná většina z nich ukázala být škodlivá. EC3 se skládá ze dvou hlavních forenzních týmů - digitálního

---

[33] Nařízení Evropského parlamentu a Rady č. 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení č. 526/2013 („akt o kybernetické bezpečnosti“) [ÚV L 151/15].

[34] ENISA. About ENISA – The European Union Agency for Cybersecurity. *ENISA* [online]. [vid. 2020-08-05]. Dostupné z: https://www.enisa.europa.eu/about-enisa/about-enisa

[35] Big data jsou tak velká data, která je velmi obtížné zachytit, zpracovat a analyzovat běžně dostupnými softwarovými nástroji v reálném čase.

a dokumentového. Svou činnost soustřeďuje zejména do oblasti kyber-závislého zločinu (angl. *cyber-dependent crime*), dále se soustředí na sexuální vykořisťování dětí online a platební podvody.

Veškeré aktivity EC3 jsou podporovány ještě specializovanými útvary, mezi něž patří CIT (Cyber Intelligence Team), který pomocí analýzy dostupných informací od různých subjektů dokáže identifikovat vzorce a hrozby. Dále je to J-CAT (Joint Cybercrime Action Taskforce), který se soustředí na spolupráci na mezinárodním poli.[36] EC3 každý rok vydává hodnocení hrozby týkající se kyberkriminality s názvem IOCTA (Internet Organised Crime Threat Assessment).

Dle IOCTA z roku 2019 je pro vyšetřování kyberkriminality velkou výzvou rychlý rozvoj technologií, jako je umělá inteligence. Mezi klíčový prvek z hlediska kriminální i vyšetřovací činnosti patří data, ta jsou totiž primárním cílem kyberzločinů. Mezi velmi časté útoky patří platební podvod, kdy není přítomna platební karta (CNP fraud)[37], dále ransomware[38] a DDoS[39]. Práci vyšetřovacích týmů ztěžuje zejména čím dál tím sofistikovanější šifrování a také kryptoměny, které umožňují ukrytí peněz získaných z nelegálních činností. Stejně tak vyšetřovatelé v praxi naráží na legislativní bariéry a na zvyšující se potřebu přeshraniční spolupráce států v oblasti elektronických důkazů. Velmi tíživý problém představuje dark web jako zdroj citlivých dat a pole pro získání nelegálních prostředků umožňujících následné páchání trestné činnosti.[40]

---

[36] European Cybercrime Centre – EC3. *Europol* [online]. [vid. 2020-08-07]. Dostupné z: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[37] Při CNP (card not present) podvodu nemusí mít útočník vůbec fyzicky k dispozici platební kartu. Platební údaje zpravidla získá pomocí phishingového útoku, či jiným způsobem, a následně provede nějakou transakci online z cizího účtu. In: KAGAN, Julia. Card-Not-Present Fraud Definition. *Investopedia* [online]. [vid. 2020-08-08]. Dostupné z: https://www.investopedia.com/terms/c/cardnotpresent-fraud.asp

[38] Ransomware je vyděračský software, který zablokuje počítačový systém a pro jeho odblokování je třeba zaplacení výkupného, zpravidla v bitcoinech. Blíže viz kapitola 6.3.

[39] Blíže viz kapitola 3.1.7.

[40] EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION. *Iocta, Internet Organised Crime Threat Assessment: 2019.* [online]. 2019. Dostupné z: https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

2.2 Rada Evropy

2.2.1 Úmluva Rady Evropy o počítačové kriminalitě

Úmluva Rady Evropy o počítačové kriminalitě byla připravována více než 16 let a byla prvním multilaterálně závazným nástrojem v boji proti kyberkriminalitě.[41] V listopadu roku 2001 bylo přijato znění této Úmluvy a dne 23. listopadu 2001 byla Úmluva v Budapešti otevřena k podpisu. Proto se jí také přezdívá Budapešťská úmluva. Je klíčovým dokumentem v oblasti kyberkriminality a klade si za cíl zejména sjednocení právní úpravy jednotlivých států. Ty implementují právní úpravu do svých vnitrostátních právních řádů. Tato harmonizace je důležitá ze dvou důvodů. Prvním z nich je eliminace tzv. bezpečných rájů, tedy států, ve kterých by bylo možné beztrestně provádět kyberzločiny a zasahovat i do jurisdikcí jiných států. Druhým důvodem je zajištění mezinárodní spolupráce mezi státy.[42]

Úmluva vstoupila v platnost 1. července 2004, v České republice až 1. prosince 2013. Ke dni 10. září 2020 byla ratifikována již 65 státy. Kromě členských států Rady Evropy k ní přistoupilo několik dalších států, jako Austrálie, Brazílie, Kanada, Izrael, Japonsko, Mexiko, Peru, Jihoafrická republika, USA a další.

Úmluva rozděluje kybernetické trestné činy do čtyř skupin:

1) Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů;
2) Trestné činy související s počítači;
3) Trestné činy související s obsahem;
4) Trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským.

V Úmluvě jsou upraveny procesní postupy pro odhalení, vyšetřování a následné stíhání kybernetických trestných činů, zabývá se elektronickými důkazy a nakládání s nimi a také upravuje účinný systém mezinárodní spolupráce. Celkem obsahuje 48 článků a skládá se

---

[41] CLOUGH, Jonathan. A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation. *Monash University Law Review*. 2014, **40**(3), 698–736.

[42] Ibid.

ze 4 kapitol: i) užití pojmů; ii) opatření, která mají být přijata na vnitrostátní úrovni; iii) mezinárodní spolupráce a iv) závěrečná ustanovení.

Velmi zásadní je Dodatkový protokol Rady Evropy č. 189 k Úmluvě o počítačové kriminalitě, který byl přijat 7. listopadu roku 2002 a rozšířil okruh o následující trestné činy:

1) šíření rasistického a xenofobního materiálu skrze počítačový systém;
2) rasisticky a xenofobně motivovaná výhružka;
3) rasisticky a xenofobně motivovaná urážka;
4) popírání, hrubé zlehčování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti.

Tyto skutkové podstaty zahrnující činy s rasistickým a xenofobním obsahem byly považovány za kontroverzní z toho důvodu, že jsou v rozporu s právem na svobodu projevu. Aby co nejvíce států ratifikovalo samotnou Úmluvu, byly tyto kontroverzní skutkové podstaty zařazeny samostatně do Dodatkového protokolu.[43]

2.2.2 Konference Octopus

Konference Octopus je Radou Evropy pořádána každých 12 až 18 měsíců a je jednou z největších a nejlepších platforem pro odborníky z oblasti kyberkriminality. Každá konference se zaměřuje na nějaké specifické téma. Jejím cílem je provádět ustanovení Úmluvy o počítačové kriminalitě, posílit ochranu dat a záruky právního státu a zlepšit kooperaci států v boji proti kyberkriminalitě.

Poslední odborná konference Rady Evropy Octopus, která se konala v listopadu roku 2019 pod názvem „Kooperace proti kyberzločinu“, přinesla několik závěrů.[44] Od roku 2016 se zvyšuje počet útoků narušujících průběh voleb. Jednotlivé státy musí přijmout zákony, které zajistí, že systémy zabezpečující volby a volební kampaně budou bezpečnější a zároveň budou zásahy do svobodného a spravedlivého volebního práva občanů bezpodmínečně stíhány.

---

[43] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 146. ISBN 978-80-903786-7-4.

[44] Octopus 2019 „Cooperation against Cybercrime“, 20.–22. November 2019, Palais de l’Europe, Council of Europe, Strasbourg, France.

Je třeba posílit mezinárodní i vnitrostátní spolupráci v případě ochrany dětí před sexuálním vykořisťováním a zneužíváním online. Je také nezbytné zvýšit povědomí a informovanost dětí a ostatních účastníků, aby bylo možné s touto kriminalitou účinně bojovat. V návaznosti na živé vysílání teroristického útoku v městě Christchurch na Novém Zélandu byla vytvořena výzva s názvem The Christchurch Call[45], která si klade za cíl odstranit teroristický a násilný extremistický obsah z online prostředí.

V budoucnu by k Úmluvě o počítačové kriminalitě měl být přidán další dodatkový protokol, který by měl podporovat posílení mezinárodní spolupráce a přístup k elektronickým důkazům v cloudu. Při vyšetřování kyberkriminality je nutné brát v potaz práva na ochranu soukromí a na ochranu osobních údajů. V současné době je zejména problematické, že je nedostatečný přístup do systému WHOIS[46], k soudním rozhodnutím ohledně uchování dat (angl. *data retention*) anebo ohledně zacházení s dynamickými adresami internetového protokolu.

Je nutné zvýšit kooperaci a sdílení informací na všech úrovních tak, aby bylo možné posilovat kybernetickou bezpečnost. Hlavně by měla být přijata jasná taxonomie kybernetických incidentů, jasný právní rámec a jasný rozsah akcí pro aktéry kybernetické bezpečnosti a také společné záruky. Je to hlavně budování kapacit, které umožní účinné stíhání a trestání kybernetické trestné činnosti. Příkladem takovéto kapacity je Cybercrime Programme Office of the Council of Europe (C-PROC).

V roce 2018 bylo na konferenci Octopus vyzdviženo i téma umělá inteligence, která se spolu se strojovým učením velmi rychle rozvíjí. Tyto prostředky mohou využívat zločinci právě při kybernetické kriminalitě, kdy se útoky mohou automatizovat. Na jednu stranu může umělá inteligence sloužit jako užitečný nástroj, na druhou stranu může být zneužívána. Je proto třeba pozorně sledovat vývoj v této oblasti a řešit otázky trestní odpovědnosti a etických limitů při používání umělé inteligence.

---

[45] Christchurch Call | to eliminate terrorist and violent extremist content online [online]. [vid. 2020-02-05]. Dostupné z: https://www.christchurchcall.com/

[46] WHOIS je databáze, která obsahuje údaje o majitelích internetových domén, IP adres, DNS serverů a dalších objektů na síti. Whois Lookup & IP. *Whois.net* [online]. [vid. 2020-02-05]. Dostupné z: https://www.whois.net/

2.2.3 Cybercrime Convention Committee (T-CY) a Cybercrime Programme Office of the Council of Europe (C-PROC)

Cybercrime Convention Committee (T-CY) neboli Výbor k Úmluvě o počítačové kriminalitě zajišťuje efektivní implementaci ustanovení Úmluvy o počítačové kriminalitě, a to zejména prostřednictvím pravidelně se konajících plenárních zasedání. Mezi hlavní aktivity tohoto výboru patří přijímat stanoviska a doporučení k výkladu a provádění Úmluvy, příprava návrhů legislativních dokumentů, přijímání stanovisek, přezkum fungování kontaktních míst, podpora přistoupení dalších států k Úmluvě, podpora společných postojů stran na mezinárodních konferencích a zapojení se do dialogu s příslušnými mezinárodními organizacemi, a to s cílem posílit mezinárodní spolupráci v oblasti kyberkriminality.[47]

V rámci Rady Evropy byla vytvořena i kancelář zabývající se kyberkriminalitou a posilováním kapacit jednotlivých států v oblasti trestního soudnictví nazývající se Cybercrime Programme Office of the Council of Europe (C-PROC). Jejím cílem je zajistit příslušná odborná školení, zřízení specializovaných jednotek pro kyberkriminalitu, podpora spolupráce veřejného a soukromého sektoru, ochrana dětí před sexuálním násilím online a zvyšování účinnosti mezinárodní spolupráce. Kancelář vznikla v roce 2014, sídlí v Bukurešti a zajišťuje několik projektů. Jedním z nich je právě konference Octopus. Dále má ve své gesci projekt GLACY+[48], CyberSouth[49], iPROCEEDS-2[50], EndOCSEA[51] a CyberEast[52]. C-PROC velmi úzce spolupracuje s T-CY a zajišťuje tak co nejefektivnější implementaci ustanovení Úmluvy o počítačové kriminalitě.

---

[47] COUNCIL OF EUROPE. *T-CY Rules of Procedure* [online]. 8. červenec 2019. Dostupné z: https://rm.coe.int/t-cy-2013-25-rules-of-procedure/1680965e5f

[48] Více informací o projektu GLACY+ zde: https://www.coe.int/en/web/cybercrime/glacyplus

[49] Více informací o projektu CyberSouth zde: https://www.coe.int/en/web/cybercrime/cybersouth

[50] Více informací o projektu iPROCEEDS-2 zde: https://www.coe.int/en/web/cybercrime/iproceeds-2

[51] Více informací o projektu EndOCSEA zde: https://www.coe.int/en/web/cybercrime/endocsea-europe

[52] Více informací o projektu CyberEast zde: https://www.coe.int/en/web/cybercrime/cybereast

2.3 Organizace spojených národů

V roce 1990 na osmém kongresu OSN[53] byl v Havaně přijat Manuál OSN o prevenci a kontrole trestných činů spojených s počítači, ve kterém je popisován fenomén počítačové kriminality. Manuál obsahuje první hmotněprávní i procesněprávní normy týkající se kyberkriminality.[54] V současné době neexistuje žádná úmluva na úrovni OSN, která by komplexně upravovala boj s kyberkriminalitou, podobně jako je tomu na úrovni Rady Evropy. Ruská federace přišla s návrhem rezoluce týkající se kyberkriminality a s návrhem úmluvy, která by nahradila Budapešťskou úmluvu. Dne 27. prosince 2019 byla rezoluce schválena, a měla by tak být vytvořena expertní skupina zabývající se možným vytvořením úmluvy OSN o kyberkriminalitě. Takový krok ale vzbuzuje obavy, zejména kvůli neurčitosti definice o trestnosti informačních a komunikačních technologií a dalších nejasných ustanovení, která by pak umožňovala Rusku, Číně a jiným autoritářským zemím pronásledovat jejich politické odpůrce.[55]

V rámci OSN bylo přijato několik rezolucí týkajících se boje proti kyberkriminalitě. Rezoluce č. 22/7 o posilování mezinárodní spolupráce v boji proti kyberkriminalitě ze dne 1. ledna 2013 poukazuje na nutnost posílení spolupráce států v boji proti kyberkriminalitě a zdůrazňuje roli OSN a úlohu CCPCJ v oblasti výměny informací, poskytování technické podpory a zajišťování prevence. Rezoluce připomíná významnou rezoluci č. 65/230 ze dne 21. prosince 2010, která jako první požadovala zřízení specializovaného orgánu pro provedení rozsáhlé studie ohledně kyberkriminality. Rezoluce č. 22/8 pak zajišťuje technickou podporu a budování kapacit s cílem posílit vnitrostátní opatření a mezinárodní spolupráci v boji proti kyberkriminalitě.

---

[53] UNITED NATIONS, ed. *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August-7 September 1990: report*. New York: United Nations, 1991. ISBN 978-92-1-130143-4.

[54] ZAVRŠNÍK, Aleš. Cybercrime – Definitional Challenges and Criminological Particularities. *Masaryk University Journal of Law and Technology*. 2009, **2**(2), 1–29. ISSN 1802-5951.

[55] HAKMEH, Joyce a Allison PETERS. A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet. *Council on Foreign Relations* [online]. [vid. 2020-08-19]. Dostupné z: https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet

United Nations Office on Drugs and Crime (UNODC)

Na boj s kyberkriminalitou se soustředí United Nations Office on Drugs and Crime (UNODC) v rámci Globálního programu na kyberkriminalitu, a to zejména podporou aktivit a struktur jednotlivých států, kdy soustřeďuje odborníky z oblasti trestního soudnictví, zvyšuje prevenci a povědomí subjektů, podporuje mezinárodní spolupráci a provádí technickou podporu, výzkum a analýzu kybernetické kriminality. V souladu s článkem 42 Salvadorské deklarace[56] byla vytvořena expertní skupina EGM (Expert Group Meeting) za účelem vytvoření komplexní studie ohledně kybernetické kriminality a vhodné reakce členských států na útoky. V roce 2019 byl také vytvořen ad hoc Výbor pro vypracování souhrnné mezinárodní úmluvy o boji proti užívání informačních a komunikačních technologií pro trestní účely. Tento výbor by se měl pravidelně setkávat v období od srpna roku 2021 až do června roku 2024, kde by na sedmdesátém devátém setkání Generálního shromáždění OSN představil návrh rezoluce.[57] Pod záštitou UNODC bylo vytvořeno tzv. Cybercrime Repository[58] – úložiště, které shromažďuje veškeré rozhodnuté případy týkající se kyberkriminality a obsahuje databázi legislativy, která danou problematiku upravuje.

2.4 Severoatlantická aliance

NATO se soustředí na kybernetickou obranu. V roce 2014 se kybernetická obrana stala součástí kolektivního obranného systému a provedení kyberútoku může být aktivováno článkem 5 Severoatlantické smlouvy. Na Varšavském summitu v roce 2016 byl kyberprostor uznán jako oblast operací, ve kterých se musí NATO bránit stejně účinně jako ve vzduchu, na zemi i na moři. Kyberútoky jsou totiž čím dál tím častější,

---

[56] Salvadorská deklarace o komplexních strategiích pro globální výzvy: Prevence kriminality a systémy trestní justice a jejich vývoj v měnícím se světě.

[57] UN GENERAL ASSEMBLY. *Proposed outline and modalities for the further activities of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Background paper prepared by the Secretariat.* [online]. 15. červen 2020. Dostupné z: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Background_paper/A_AC.291_2_E.pdf

[58] Cybercrime Repository dostupné zde: https://sherloc.unodc.org/cld/v3/cybrepo/

sofistikovanější a škodlivější.[59] Hlavním cílem NATO je ochrana jeho vlastních sítí, včetně operací a misí a tím zvyšování odolnosti struktury aliance. Tuto ochranu zajišťuje NCIRC (NATO Computer Incident Response Capability).

V roce 2018 bylo v Belgii schváleno zřízení Kybernetického operačního centra CyOC s cílem poskytovat situační povědomí a koordinaci operační činnosti NATO v kyberprostoru, poskytnout zázemí pro provádění misí v kyberprostoru a zajistit centralizované plánování aspektů kyberprostoru a misí aliance. Centrum by mělo být plně funkční do roku 2023.[60]

NATO každý rok pořádá NIAS (NATO Information Assurance Symposium), což je největší konference NATO na téma kybernetické bezpečnosti. V roce 2019 patřila mezi hlavní témata umělá inteligence, strojové učení a big data.[61]

Speciální centrum NATO pro kybernetickou obranu CCD CoE

Speciální centrum NATO pro kybernetickou obranu CCD CoE sídlí v Tallinu a vzniklo v roce 2008 jako reakce na politicky motivované kyberútoky na Estonsko.[62] Hlavním posláním centra je posilovat spolupráci mezi členskými státy a poskytnout interdisciplinární přístup k nejdůležitějším problémům v oblasti kybernetické obrany. CCD CoE provádí výzkum, školení a různá cvičení v oblasti technologií, strategií, operací a práva. Mezi tři hlavní projekty patří Tallinský manuál 2.0, cvičení Locked Shields, Crossed Swords a Cyber Coalition, a mezinárodní konference Cyber Conflict (CyCon).[63]

---

[59] BRENT, Laura. NATO's role in cyberspace. *NATO Review* [online]. 12. únor 2019 [vid. 2020-08-20]. Dostupné z: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

[60] VAVRA, Shannon. NATO cyber-operations center will be leaning on its members for offensive hacks. *Cyberscoop* [online]. 30. srpen 2019 [vid. 2020-08-20]. Dostupné z: https://www.cyberscoop.com/nato-cyber-operations-offensive-hacking-neal-dewar/

[61] NCI AGENCY. NIAS19-Digital Transformation. In: NIAS'19 [online]. 2018 [cit. 10.09.2020]. Dostupné z: https://nias19.com

[62] TAMKIN, Emily. 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats? *Foreign Policy* [online]. [vid. 2020-08-20]. Dostupné z: https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

[63] PLANTERA, Federico. NATO CCDCOE – Expertise and cooperation make our cyber space safer. *e-Estonia* [online]. 16. říjen 2018 [vid. 2020-08-20]. Dostupné z: https://e-estonia.com/nato-ccdcoe-expertise-cyber-space-safer/

CCD CoE vede databázi publikací expertů v oblasti kybernetické obrany s názvem Cyber Defence Library, dále vede INCYDER – interaktivní databázi dokumentů týkajících se kybernetické bezpečnosti, a spravuje International Cyber Law Interactive Toolkit – zdroj relevantních ustanovení mezinárodního práva v oblasti operací v kyberprostoru. Každoročně je pořádaná konference CyCon, kde se schází odborníci z celého světa, aby se věnovali aktuálním problémům v oblasti kybernetické bezpečnosti. Výstupem této konference je kniha obsahující příspěvky odborníků týkající se různých témat.

Tallinský manuál 2.0 o aplikovatelnosti mezinárodního práva na kybernetické válčení

Tallinský manuál 2.0 je vylepšenou verzí prvního manuálu z roku 2013 a obsahuje 154 pravidel pro kybernetické operace s rozsáhlým komentářem. Manuál je rozdělen do čtyř částí. První část upravuje obecně mezinárodní právo a kyberprostor – suverenita, náležitá péče, jurisdikce, mezinárodní odpovědnost a kybernetické operace, na které se nevztahuje mezinárodní právo. V části druhé jsou upraveny specializované režimy mezinárodního práva a kyberprostoru – mezinárodní lidské právo, diplomatické a konzulární právo, právo moře, právo vzduchu, právo vesmíru a mezinárodní telekomunikační právo. Třetí část se soustřeďuje na mezinárodní mír a bezpečnost a kybernetické aktivity – mírové řešení sporů, zákaz zasahování, použití síly a kolektivní bezpečnost. V poslední a nejrozsáhlejší části se nachází pravidla upravující právo kyber-ozbrojeného konfliktu – obecně právo ozbrojeného konfliktu, vedení nepřátelských akcí, některé osoby, předměty a činnosti (zdravotnický personál, zadržené osoby, děti, novináři, kulturní památky apod.), okupace a neutralita.

Manuál reflektuje mnoho paradoxů a snaží se odstranit některé nejasné aspekty. Dle některých autorů ale tyto nejistoty týkající se kybernetické války spíše odráží a utvrzuje, než že by je odstraňoval.[64] Dle Jensena bude manuál výchozím bodem pro diskuzi v následujících letech. Jedná se o velmi komplexní analýzu vypracovanou odborníky. Přestože existuje mnoho oblastí neshod, je třeba reflektovat, že oblast kybernetických útoků a kyberprostoru je stále rostoucí oblastí práva, a proto je třeba mít dostatečné

[64] KESSLER, Oliver a Wouter WERNER. Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare International Legal Theory: Symposium: Expertise, Uncertainty, and International Law. *Leiden Journal of International Law*. 2013, **26**(4), 793–810.

porozumění a postupně vytvářet nové přístupy.[65] Skepticismus k regulování kyberprostoru prostřednictvím tradičních konceptů státnosti, suverenity, územní celistvosti a mezinárodní odpovědnosti není až tak překvapivý. Některé státy mohou regulaci využít ve svůj prospěch, státy mají také nerovnoměrně rozložené kapacity a není zde žádná mezinárodní organizace, která by mohla shledávat subjekty odpovědnými a která by aplikovala dané normy. Státy zatím nedůvěřují plně pravidlům stanoveným v Tallinnském manuálu a mnohdy na kyberútoky reagují taktéž prováděním kyberútoků či jiných operací, a to neoficiální cestou.[66]

---

[65] JENSEN, Eric Talbot. The Tallinn Manual 2.0: Highlights and Insights International Justice: Where We Stand, Where We Fall, and Where We Need to Be. *Georgetown Journal of International Law*. 2016, **48**(3), 735–778.

[66] EFRONY, Dan a Yuval SHANY. A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. *American Journal of International Law* [online]. 2018/10/17 vyd. 2018, **112**(4), 583–657. ISSN 0002-9300. Dostupné z: doi:10.1017/ajil.2018.86

3. KYBERÚTOKY

Úmluva o počítačové kriminalitě rozděluje kybernetické trestné činy do těchto kategorií:

1) trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů;
2) trestné činy související s počítačem;
3) trestné činy související s obsahem;
4) trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským.

Schéma kyberútoků se nachází v Příloze 1.

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

3.1.1 Hacking

V článku 2 Úmluvy o počítačové kriminalitě je jako první uveden trestný čin „Nezákonný přístup“. Pod tuto kategorii trestných činů spadají všechny útoky nazývající se „hacking“ či „cracking“. Osoba, která se snaží získat neoprávněný přístup k počítačovému systému se správně označuje cracker (z angl. *to crack* – prolomit). V dnešní době se ale hlavně díky medializaci ustálil spíše výraz hacker, jehož původní význam je trochu odlišný, dokonce pozitivní. Hacker je totiž někdo nadšený do počítačů, kdo umí programovat a snaží se počítače a jejich systémy vylepšit.[67]

Takový hacker by patřil do skupiny tzv. „white hats“, kteří se řídí pravidly[68], která jejich komunita vytvořila a standardně neporušují žádné zákony. Crackeři se ale řadí do skupiny „black hats“, kde už dochází k napadání systému a neoprávněnému přístupu k němu.

---

[67] GUNKEL, David J. *Hacking cyberspace*. Boulder, Colo: Westview Press, 2001, s. 3–4. Polemics. ISBN 978-0-8133-3669-5.

[68] Pravidla komunity hackerů, jejich žargon, popis typického hackera a také popis, jak se stát hackerem, dostupné na: http://www.catb.org/jargon/html/index.html.

Pokud není zcela jasné, do jaké skupiny je možné hackera (resp. crackera) zařadit, dále existuje ještě skupina „grey hats“, která je na pomezí dvou předchozích.[69]

Typickým hackerským nástrojem je prolamování hesel (angl. *password crackers*). K tomu slouží nespočet programů vyskytujících se volně na internetu. Nejjednodušším typem útoku je tzv. brute-force attack. Buď daný program obsahuje tisíce hesel (známých slov) a postupně zkouší, které je to správné, anebo program generuje náhodné kombinace znaků. V závislosti na složitosti hesla prolomení trvá různě dlouhou dobu.[70]

Sofistikovanějším nástrojem je tzv. kryptografická analýza, kdy nejenže program generuje různé kombinace, ale zároveň využívá i další dostupné informace, jako je správné načasování dat či různé dostupné dvojice textu. Další rozměr a potenciál této metodě přidává využití umělé inteligence. Program takto vytvářený dokáže pomocí umělé inteligence vymýšlet sám další kombinace na základě informací získaných v průběhu prolamování hesla. Takovýto algoritmus má až 57% úspěšnost oproti klasické brute-force attack metodě, která má za stejných podmínek úspěšnost 24 %.[71]

Další metodou útoku je tzv. keylogger, což je program, který zaznamenává stisky kláves na klávesnici, a útočník tak může získat cenné osobní údaje. Ze zaznamenaných písmen a číslic lze získat nejen přihlašovací údaje, ale také obsahy různých dokumentů či historii webového prohlížeče. Primárně se využívají softwarové nástroje, které je jednodušší do počítače infiltrovat, ale existují i nástroje hardwarové.[72] Někdy je tento útok řazen mezi malware, ale nachází se spíše na pomezí mezi malwarem (zasahování do dat) a hackerským nástrojem (nezákonný přístup). Tento nástroj ale nemusí vždy sloužit

---

[69] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 284. ISBN 978-80-247-1561-2.

[70] Uvádí se, že 4místné heslo složené pouze z malých písmen je možné prolomit za méně než 1 sekundu, 6místné heslo složené z kombinace malých a velkých písmen, číslic a speciálních znaků za 11 hodin a stejně složené 10místné heslo lze prolomit za 91 800 let. Blíže viz: http://toplinestrategies.com/blogs/ net/how-much-time-needed-crack-password-brute-force.

[71] TRIEU, Khoa a Yi YANG. Artificial Intelligence-Based Password Brute Force Attacks. *MWAIS 2018 Proceedings*. 2018, (39), 8.

[72] TULI, Preeti a Priyanka SAHU. System Monitoring and Security Using Keylogger. *International Journal of Computer Science and Mobile Computing*. 2013, **2**(3), 6. ISSN 2320-088X.

pouze k nelegálním účelům, může být využíván například zaměstnavatelem, který monitoruje aktivitu zaměstnanců v pracovní době.[73]

3.1.2 Phishing

Mezi nejčastěji využívané útoky v dnešní době patří tzv. phishing. Phishing funguje na bázi podvodných e-mailů, pomocí kterých útočníci obelstí uživatele a získají tak citlivá data, jako jsou například přihlašovací údaje do internetového bankovnictví. Slovo phishing vzniklo ze slova „fishing“, tedy „rybařit“, což znamená, že útočník hodí návnadu, na kterou se může potenciálně cílený uživatel chytit. Sám se dostane do pasti tím, že zpravidla klikne na odkaz uvedený v e-mailu, který jej přesměruje na podvodnou stránku, kde uživatel vyplní své přihlašovací údaje a ty jsou následně doručeny útočníkovi. Tyto e-maily vypadají velice důvěryhodně a běžný nepozorný uživatel se často nechá nachytat, i přes překlepy a další nedokonalosti, které se v e-mailové zprávě vyskytují.[74]

Specifickým druhem phishingu je tzv. spear-phishing, který je poslední dobou velmi populární a je velmi obtížné se proti němu bránit. „*Spear-phishing je personalizovaná forma podvodných e-mailů, která cílí na konkrétní osobu nebo skupinu osob. Základem útoku je tzv. sociální inženýrství, tedy techniky manipulace oběti k tomu, aby se chovala způsobem, který není v jejím zájmu*.“[75] Cílem je vylákat přístupové údaje či jiné informace, které může následně zneužít. Útoky jsou směřovány na konkrétní osoby, často na řadové zaměstnance i na vedoucí organizace. Spear-phishing je prováděn e-mailem, SMS zprávami (smishing), pomocí telefonátu (vishing) a také prostřednictvím sociálních

---

[73] Keyloggers: How they work and how to detect them (Part 1) | Securelist [online]. [vid. 2019-09-02]. Dostupné z: https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/

[74] DE KIMPE, Lies, Michel WALRAVE, Wim HARDYNS, Lieven PAUWELS a Koen PONNET. You’ve got mail! Explaining individual differences in becoming a phishing target. *Telematics and Informatics* [online]. 2018, **35**(5), 1277–1287. ISSN 0736-5853. Dostupné z: doi: 10.1016/j.tele.2018.02.009

[75] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Podvodné e-maily nebo zprávy na sociálních sítích na míru: spear-phishing a jak se před ním chránit* [online]. 3. duben 2020 [vid. 2020-04-26]. Dostupné z: https://nukib.cz/download/publikace/doporuceni/Doporuceni_spear_phishing_2.0.pdf s. 1.

sítí. „*Fyzickou formou spear-phishingu (metoda, které se také říká „baiting“) může být i pohozený USB disk v blízkosti vytipovaného cíle*.“[76]

Sofistikovanější verzí phishingového útoku je pharming, který spočívá v přesměrování uživatele na podvodnou stránku tak, že útočník napadne DNS server a změní IP adresu. Uživatel do příkazového řádku napíše adresu webové stránky, kterou běžné využívá, ale je přesměrován na jinou webovou stránku, která na první pohled vypadá totožně, ale je ve skutečnosti podvodná a útočník z ní může získat jakákoliv data.[77]

3.1.3 Sniffing a spoofing

Pomocí útoku s názvem sniffing útočník odposlouchává komunikaci v dané síti. Zpravidla k tomu využívá nějaký softwarový či hardwarový nástroj, kterému se říká sniffer. Útočník se dozví veškeré údaje o daném zařízení a dokáže sledovat datové toky, které v dané síti probíhají. Získá tak citlivá data, jako jsou přihlašovací údaje a hesla a následně je může zneužít.[78]

Existují tři druhy útoku s názvem spoofing. Prvním z nich je IP spoofing, kdy útočník zasílá zprávy ze změněné IP adresy tak, aby vypadala jako z důvěryhodného zdroje. Druhým způsobem je e-mail spoofing, který spočívá v zasílání e-mailu s falešnou odesílací adresou, která má opět vzbuzovat důvěru a obelstít uživatele. Posledním způsobem je DNS spoofing, který podobně jako při pharmingu modifikuje DNS server a přesměruje uživatele na jinou IP adresu.[79]

3.1.4 Phreaking

Phreaking spočívající v napojení se na telekomunikační linku byl velmi populární v šedesátých a sedmdesátých letech minulého století. Pomocí vygenerovaných zvukových signálů dokázali útočníci obelstít cílovou destinaci hovoru, a tak použít

---

[76] Ibid., s. 2.

[77] DVOŘÁK, Marek. Phishing, pharming a jejich trestněprávní postih. *Trestněprávní revue*. 2018, (4), 84-89.

[78] SHEMA, Mike. *Hacking web apps: detecting and preventing web application security problems*. Amsterdam; Boston: Syngress, 2012, s. 146–148. ISBN 978-1-59749-951-4.

[79] Spoofing – what it is and how to defend against it. *Avast* [online]. [vid. 2019-09-15]. Dostupné z: https://www.avast.com/c-spoofing

nestandardní prostředky k jeho uskutečnění. Takovými prostředky jsou Voice over IP (VoIP) a Cellular (neboli mobilní data). Útočník tak zadarmo využívá telefonní linku, může cizí linku odposlouchávat, a dokonce se i připojit k internetu. Pokud se útočník napojí na telekomunikační linku, tak má možnost využít i tzv. VoIP phishing útok, kdy se vydává za nějakou finanční instituci a požaduje po klientovi číslo účtu a PIN kód. Pokud útočník využívá k útoku LTE sítě mobilních dat, dokáže získat sériové číslo mobilního telefonu (IMSI, IMEI) a následně se za něj vydávat a využívat jeho připojení.[80]

3.1.5 Man-in-the-middle attack

Článek 3 Úmluvy o počítačové kriminalitě upravuje trestný čin „Nezákonný odposlech". Tyto útoky se nazývají tzv. man-in-the-middle attack (MITM), kdy je mezi dva programy umístěn jeden škodlivý program, který zaznamenává přenos dat mezi nimi. Mnoho předchozích útoků může naplňovat skutkovou podstatu tohoto trestného činu. Jedná se například o keylogger, sniffing, IP spoofing či phreaking. Mezi MITM se řadí i krádež cookies dat, která jsou dnes hojně využívaná na všech webových stránkách.[81]

3.1.6 Malware

V článku 4 Úmluvy o počítačové kriminalitě je definován trestný čin „Zasahování do dat". Útoky naplňující tuto skutkovou podstatu se souhrnně označují jako malware a jedná se o všechny červy, viry, trojské koně, spyware, adware, botnety a rootkity. Všechny tyto druhy útoků jsou nechtěné, neznámé a nepřátelské a ve většině případů jsou nainstalovány do počítače neúmyslnou akcí nic netušícího uživatele. Jejich cílem je primárně proniknout do systému, a ohrozit tak data či dokonce celou infrastrukturu.[82]

Botnet je síť infikovaných počítačů, které spolu komunikují za účelem koordinace útoků. Právě botnety jsou využívány při níže popsaném útoku DDoS. Zakladatel botnetu se nazývá „bot herder" a počítače infikované botem se nazývají „zombies" („bot" je zkratka

---

[80] GOLD, Steve. The rebirth of phreaking. *Network Security* [online]. 2011, **2011**(6), 15–17. ISSN 1353-4858. Dostupné z: doi:10.1016/S1353-4858(11)70064-2

[81] What is a man-in-the-middle attack? *NortonLifeLock* [online]. [vid. 2019-09-22]. Dostupné z: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

[82] MCQUADE, Samuel C., ed. *Encyclopedia of cybercrime*. Westport, Conn: Greenwood Press, 2009, s. 122. ISBN 978-0-313-33974-5.

slova „robot“ a znamená program, který provádí automatické operace). Bot herder ovládá celou síť počítačů a může jim zadávat příkazy k jakýmkoliv operacím.[83]

3.1.7 DoS a DDoS útok

Článek 5 Úmluvy o počítačové kriminalitě definuje „Zasahování do systému“. Útoky této kategorie se nazývají Denial of Service (DoS) či jeho podtyp Distributed Denial of Service (DDoS). Jak již název napovídá, tak DoS útok spočívá v odepření přístupu k informačnímu systému počítače či jiného elektronického zařízení. Útočník zaplaví systém obrovským množstvím dat ve velmi krátkém čase a servery si s tím neumí poradit, což poté znemožňuje síťový provoz. DoS útoky mohou směřovat proti procesorům, jejich paměti či diskové kapacitě. Takový útok může být proveden zasláním tisíců e-mailů s přílohami, což přetíží možnosti připojení nebo dostupné místo na disku.

DDoS útoky využívají botnet, kdy je již velké množství počítačů v různých částech světa infikováno a je možné je na dálku ovládat. Útok je tak prováděn tisíci počítači najednou a společnou silou mohou vyřadit z provozu i ty největší sítě. DDoS útoky se řadí mezi nejzávažnější formu kyberútoků, protože dokážou využít masivní množství provozu z obrovského množství zdrojů.[84]

3.1.8 Zneužívání zařízení

Poslední článek prvního oddílu Úmluvy o počítačové kriminalitě upravuje trestný čin „Zneužívání zařízení“. Útočník zneužívá zařízení právě za účelem uskutečnění všech výše zmíněných útoků. Může se jednat například o počítač či telefon, který může být ve vlastnictví útočníka, ale nemusí. Často se různé hackerské nástroje objevují na černém trhu a je zde snaha zabránit prodeji těchto zařízení. V roce 2001 byla přijata Evropská úmluva o právní ochraně služeb s podmíněným přístupem a služeb tvořených

---

[83] What is a Botnet? | Preventing Botnet Attacks. *Kaspersky* [online]. [vid. 2019-09-28]. Dostupné z: https://www.kaspersky.com/resource-center/threats/botnet-attacks

[84] MCQUADE, Samuel C., ed. *Encyclopedia of cybercrime*. Westport, Conn: Greenwood Press, 2009, s. 63–64. ISBN 978-0-313-33974-5.

podmíněným přístupem, která bojuje proti protiprávnímu přístupu ke službám jako je televizní a rozhlasové vysílání či jiné služby informační společnosti.[85]

3.2 Útoky související s počítačem

3.2.1 Počítačové padělání

Článek 7 upravuje trestný čin „Počítačové padělání“. Tuto skutkovou podstatu naplňují útoky spočívající ve vytváření falešných dokumentů, dále jejich změny, úpravy, mazání či potlačení dat. Příkladem může být vytváření falešných webových stránek, vytváření falešných identit a jejich následné užívání na internetu či v e-mailových zprávách nebo prodej či distribuce falešných identifikačních dokumentů.[86] Do této kategorie může být zařazen i tzv. skimming, neboli padělání platebních karet, ke kterému dochází zkopírováním dat z magnetického proužku karty, což je možné například prostřednictvím speciálně upraveného bankomatu.[87]

3.2.2 Počítačový podvod

Článek 8 definuje „Počítačový podvod“. Mezi nejčastější útoky tohoto typu patří tzv. nigerijské dopisy neboli podvod se „zálohovým poplatkem“ známý jako Scam 419. Prostřednictvím e-mailových zpráv oslovují útočníci velké množství lidí a ve zprávách uvádí, že daný člověk získá velké dědictví nebo odměnu za to, že útočníkovi pomůže převést peníze ze země. Vše je ale podmíněno zasláním peněžité zálohy. Slibovaného obnosu peněz se ale člověk pochopitelně nikdy nedočká. Velmi často se útočník vydává za někoho z Nigérie, z čehož plyne i název tohoto útoku. Existuje mnoho dalších druhů podvodů, jako jsou podvodné online prodeje, intriky s předběžnými poplatky, podvody

---

[85] Evropská úmluva o právní ochraně služeb s podmíněným přístupem a služeb tvořených podmíněným přístupem [ÚV L 336/2]

[86] JÎRLĂIANU, Silviu. Computer Related Forgery, Between Concept And Reality. *International conference KNOWLEDGE-BASED ORGANIZATION* [online]. 2015, **21**. Dostupné z: doi:10.1515/kbo-2015-0075

[87] POLICIE ČR. Skimming. *Policie.cz* [online]. [vid. 2019-10-05]. Dostupné z: https://www.policie.cz/clanek/ncoz-skimming.aspx

s elektronickými převody peněžních prostředků, podvodné investice a podvody s identitou.[88]

3.2.3 Kyberterorismus

Kyberterorismus v současné době představuje globální hrozbu a dynamicky se rozšiřuje po celém světě. „*O kyberterorismu budeme hovořit v případě, že cílem nebo nástrojem útoku teroristů je informační nebo telekomunikační systém*.“[89] Velmi často je útok politicky nebo nábožensky motivován. Dané struktury mají obvykle za cíl ovlivnit veřejné mínění a zastrašit obyvatelstvo.[90] Dle Denningové je „*kyberterorismus konvergence kyberprostoru a terorismu. Jde o protiprávní útoky a hrozby útoků proti počítačům, sítím a informacím v nich uložených, s účelem zastrašit nebo donutit vládu nebo její lid při prosazování politických nebo sociálních cílů. Dále, aby byl útok kvalifikován jako kyberterorismus, měl by vyústit v násilí proti osobám nebo majetku, nebo alespoň generovat strach. Příkladem jsou pak útoky, které vedou ke smrti či ublížení na zdraví, výbuchům nebo těžkým ekonomickým ztrátám. Vážné útoky vedené proti kritické infrastruktuře by také mohly být kvalifikovány jako kyberterorismus s ohledem na jejich dopad. Útoky, které naruší postradatelné služby nebo které jsou převážně jen drahou nepříjemností bychom takto kvalifikovat nemohli*.“[91]

3.3 Útoky související s obsahem

3.3.1 Dětská pornografie

V tomto oddíle Úmluvy je upraven pouze jeden trestný čin, pod který ale spadá velké množství útoků. Jedná se o trestné činy související s dětskou pornografií. Za dětskou pornografii je považováno „*takové pornografické dílo, které zobrazuje nebo jinak využívá*

---

[88] CLOUGH, Jonathan. *Principles of cybercrime*. Cambridge, UK; New York: Cambridge University Press, 2010, s. 183–192. ISBN 978-0-521-89925-3.

[89] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 114. ISBN 978-80-7380-720-7.

[90] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z. s. p. o., 2016, s. 323. ISBN 978-80-88168-18-8.

[91] WEIMANN, Gabriel. *Cyberterrorism. How Real Is the Threat?* [online]. B.m.: United States Institute of Peace, Special Report 119. prosinec 2004. Dostupné z: https://www.usip.org/sites/default/files/sr119.pdf

dítě nebo osobu, jež se jeví být dítětem".[92] Podle příslušného článku 9 odst. 2 Úmluvy o počítačové kriminalitě zahrnuje pojem „dětská pornografie" materiál, ve kterém se vyskytuje nezletilá osoba, osoba jevící se jako nezletilá, ale i jejich realistické zobrazení. Počítače v dnešní době umožňují vytváření virtuálních pornografických děl, u kterých je těžké rozpoznat, zda jde o realitu či nikoliv. Také se pomocí technologií pornografie velice snadno a rychle šíří a je velmi dobře dostupná každému.

Mezi útoky v této oblasti patří zejména samotná produkce dětské pornografie a šíření nápadů a fantazií mezi pedofily na síti, dále nabízení dětské pornografie prostřednictvím počítačových systémů, kdy cílí zejména na šíření hypertextových odkazů umožňujících přístup k závadnému obsahu. Trestáno je i zasílání, přenos, stahování a ukládání obsahu na nosič dat.[93]

3.3.2 Kybergrooming

Kybergrooming označuje proces, kdy se potencionální násilník spřátelí s dítětem ve snaze získat jeho důvěru, což mu následně umožňuje přimět dítě k tomu, aby se podvolilo zneužití. Útočník s obětí komunikuje nejčastěji na sociálních sítích a nejdříve se snaží si vytvořit přátelský a poté vážný vztah. Následně se snaží zjistit rizikové faktory, které by mohly způsobit jeho odhalení. V další fázi je již mezi obětí a útočníkem velice intimní a důvěryhodný vztah, což umožní přejít k sexuálnímu kontaktu.[94]

3.3.3 Kyberšikana

Kyberšikana představuje úmyslné, opakované a škodlivé činnosti prováděné na počítači, mobilním telefonu či jiném elektronickém zařízení. Útočník obtěžuje oběť tak, že jí prostřednictvím e-mailu, SMS zprávy nebo jiným způsobem zasílá nepříjemné a zlé zprávy, oběti se vysmívá, šíří o ní pomluvy či jí nadává. Často se vše odehrává veřejně

---

[92] GŘIVNA, Tomáš. § 192 [Výroba a jiné nakládání s dětskou pornografií]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 1891. ISBN 978-80-7400-428-5.

[93] CLOUGH, Jonathan. *Principles of cybercrime*. Cambridge, UK; New York: Cambridge University Press, 2010, s. 281. ISBN 978-0-521-89925-3.

[94] Ibid., s. 332–335.

na sociální síti, ať už prostřednictvím komentáře k nějakému příspěvku či zveřejněním fotografie nebo videa, které oběť zesměšňuje či jinak poškozuje.[95]

Mezi metody kyberšikany patří tzv. flaming, což je zasílání naštvaných, či dokonce vulgárních zpráv, online obtěžování spočívající v opakovaném zasílání urážlivých zpráv, kyberstalking, kdy je oběť vystavena nebezpečí poškození či urážky na cti, a tzv. trolling, kdy útočník zasílá zprávy o nějaké osobě jiným lidem, či takové věci uveřejňuje, dále tzv. masquerading, kdy se útočník vydává za někoho jiného a poškozuje tak oběť, a tzv. outing, tedy zveřejnění materiálu obsahujícího citlivé, soukromé či trapné informace.[96]

3.3.4 Hoax

Hoax je poplašná zpráva, která „*se snaží svým obsahem vyvolat dojem důvěryhodnosti. Informuje např. o šíření virů nebo útočí na sociální cítění adresáta*."[97] Hoaxy jsou často rozesílány prostřednictvím e-mailových zpráv a tyto e-maily bývají přeposílány mezi uživateli, a šíří se tak řetězovou reakcí. Speciálním typem hoaxu je tzv. virus hoax, který upozorňuje uživatele, že má infikovaný počítač, ačkoliv to není pravda.

3.3.5 Dark web

Dark web je součástí deep webu (nebo také invisible web, Undernet či hidden web), což je schovaná část webu, která není přístupná prostřednictvím klasických vyhledávačů, které dokážou zobrazit pouhé 0,03 % informací.[98] Dark web je záměrně skrytá část deep webu, kde je zaručena anonymita uživatelů a zároveň jsou veškeré operace šifrovány a nemohou být monitorovány. Nejznámější sítí vyskytující se na dark webu je Tor a I2P. Samotný přístup do dark webu je legální a v některých zemích je to jediná platforma

---

[95] KOPECKÝ, Kamil a René SZOTKOWSKI. Cyberbullying, cyber aggression and their impact on the victim – The teacher. *Telematics and Informatics* [online]. 2017, **34**(2), 506–517. ISSN 0736-5853. Dostupné z: doi:10.1016/j.tele.2016.08.014

[96] Ibid.

[97] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Praha: Policejní akademie ČR v Praze: Česká pobočka AFCEA, 2013, s. 75. ISBN 978-80-7251-397-0.

[98] BERGMAN, Michael K. White Paper: The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing* [online]. 2001, **7**(1) [vid. 2019-11-01]. ISSN 1080-2711. Dostupné z: doi:10.3998/3336451.0007.104

umožňující vyhnout se cenzuře a svobodně brouzdat po internetu. Zároveň se zde ale vyskytuje veliké množství nelegálních aktivit, jako je obchod s drogami a kradeným zbožím, nájemné vraždy, terorismus, dětská pornografie, nelegální finanční transakce, obchod s lidmi a obchod se zbraněmi.[99]

3.3.6 Kyberextremismus

Kyberextremismus spočívá ve zveřejňování nenávistných či rasových postojů a ideologií v kyberprostoru. Pomocí sociálních sítí a dalších platforem mohou být lidé ovlivňováni, a dokonce rekrutováni do různých náboženských či teroristických skupin. Velmi často se na internetu objevuje propaganda ISIS obsahující násilné činy, jejímž cílem je zastrašit obyvatelstvo.[100]

3.4 Útoky týkající se porušení autorského práva a práv souvisejících s právem autorským

Poslední článek upravuje trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským. Útoky naplňující tuto skutkovou podstatu jsou velmi časté a spočívají v reprodukci a šíření autorských děl na internetu bez souhlasu jejich autora. Jedná se nejčastěji o literární, fotografická, hudební a audiovizuální díla.

3.4.1 Peer-to-peer

Peer-to-peer síť (P2P) doslova znamená „rovný s rovným“ a jedná se o síť dvou či více propojených počítačů, které si vzájemně přímo sdílejí data bez toho, aniž by bylo třeba nějakého serveru. Taková síť může být využívána jako trvalá infrastruktura například v kanceláři, či jako *ad hoc* výměna souborů.[101] Nejvíce využívaným protokolem v rámci P2P sítě je BitTorrent. Pomocí torrentu obsahujícího metadata o dílu získá uživatel cestu

---

[99] CHERTOFF, Michael a Tobby SIMON. The Impact of the Dark Web on Internet Governance and Cyber Security [online]. 2015 [vid. 2019-11-01]. Dostupné z: https://www.cigionline.org/publications/impact-dark-web-internet-governance-and-cyber-security

[100] AWAN, Imran. Cyber-Extremism: Isis and the Power of Social Media. *Society* [online]. 2017, **54**(2), 138–149. ISSN 1936-4725. Dostupné z: doi:10.1007/s12115-017-0114-0

[101] COPE, James. What's a Peer-to-Peer (P2P) Network? *Computerworld* [online]. 8. duben 2002 [vid. 2019-11-01]. Dostupné z: https://www.computerworld.com/article/2588287/networking-peer-to-peer-network.html

k samotnému obsahu. Ti uživatelé, kteří sdílí úplně celé dílo, se nazývají seeders (rozsévači) a ti, kteří si jednotlivé časti souboru stahují od seederů, se nazývají leeches (pijavice), společně tvoří swarm (roj). Soubory se skládají z menších bloků, kdy *„každý příjemce (leech) může požádat kteréhokoliv člena roje o chybějící blok a zároveň poskytuje ostatním svoje již kompletně stáhnuté bloky (nikoliv nutně celý soubor, ale jednotlivé bloky, které soubor tvoří)*.“[102] Každý, kdo si přes P2P sítě stahuje nějaký obsah, ho zároveň musí i sdílet, i když se mnohdy jedná pouze o jednotlivé bloky, nikoliv o celé dílo.

3.4.2 File hosting

File hosting je služba umožňující ukládání a stahování souborů. Nejčastěji je využívána k přenosu velkých souborů, které by jinak nebylo možné v dané síti zaslat. Dále ke sdílení velkých video souborů, či pro ukládání osobních souborů, jako jsou fotografie a hudba. File hosting je využíván i pro zálohování dat do cloudu. Některá uložiště poskytují služby zdarma, někdy je možné získat další nadstandardní služby díky předplatnému.[103] Mezi nejznámější file hosting službu v ČR patří Ulož.to, Letecká Pošta a Úschovna, dále je to např. One Drive, Google Drive, Dropbox, iCloud Drive a FileFactory. Několik hostingových webových stránek bylo zrušeno právě kvůli porušování autorského práva.[104]

---

[102] ČERMÁK, Jiří. Ochrana autorského práva v prostředí peer to peer sítí typu BitTorrent s přihlédnutím k rozsudku ve věci The Pirate Bay. *Právní rozhledy*. 2010, (8), 272–280.

[103] DELANEY, Darragh. File hosting services and their data leakage risks. *Computerworld* [online]. 14. červen 2011 [vid. 2019-11-01]. Dostupné z: https://www.computerworld.com/article/2470038/file-hosting-services-and-their-data-leakage-risks.html

[104] Megaupload sharing site shut down. *BBC News* [online]. 2012 [vid. 2019-11-01]. Dostupné z: https://www.bbc.com/news/technology-16642369

3.4.3 Warez

Warez je „*termín počítačového slangu označující autorská díla, se kterými je nakládáno v rozporu s autorským právem*.“[105] Stejné označení nesou i webové stránky, často prezentované jako fórum, na kterém se vyskytují odkazy ke stažení nelegálních souborů, jako je software, filmy, hudba, knihy a další.

3.4.4 Embedded link

Embedded link (nebo také inline link) umožňuje uživateli přehrát či stáhnout autorské dílo bez nutnosti opustit stránku, na které se samotný odkaz nachází. Uživatel tak vůbec nenavštíví webovou stránku, kde je obsah umístěn. Provozovatel webové stránky, na které jsou embedded linky umístěny, je za svoje jednání odpovědný i přesto, že sám přímo nezákonný obsah nikam nenahrál.[106]

3.4.5 Cybersquatting a typosquatting

Cybersquatting spočívá v tom, že útočníci nakupují internetové domény nebo je blokují s cílem vydělat na jejich následném prodeji společnosti, která je reálně používá. Typosquatting, jako jedna z forem cybersquattingu, je jednání spočívající ve zneužívání známé internetové domény tak, že je zaregistrována internetová doména velmi podobného názvu a spoléhá se na to, že se na ni uživatel dostane omylem, například pomocí překlepu. Tato stránka může obsahovat malware, a ohrozit tak uživatele.[107]

---

[105] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Praha: Policejní akademie ČR v Praze: Česká pobočka AFCEA, 2013, s. 110. ISBN 978-80-7251-397-0.

[106] Tuto problematiku řeší rozsáhlá judikatura. Blíže viz. kapitola 5.5.

[107] Typosquatting. *UpCounsel* [online]. 2019 [vid. 2019-11-04]. Dostupné z: https://www.upcounsel.com/typosquatting

4. VYŠETŘOVÁNÍ KYBERKRIMINALITY

Vyšetřování kyberkriminality má svá specifika, a to vzhledem k aspektům kyberprostoru, rychlému vývoji technologií a digitálním stopám. Tomu je třeba přizpůsobit metodiku vyšetřování, která umožní účinnější a snadnější dopadení pachatele. K vyšetřování kyberzločinů byly vytvořeny specializované týmy, protože jen úzkou spoluprací odborníků na toto téma je možné dosáhnout efektivního odhalení trestné činnosti.

4.1 Pachatel

Jak již bylo zmíněno výše, pachatelem kyberzločinu se dnes díky dostupnosti technologií a připojení k síti může stát úplně kdokoliv. Obecně známá představa je, že pachatelem je chytrý a osamělý dospívající jedinec, který umí velmi dobře s počítači a má nedostatek sociálních dovedností.[108] V jiné literatuře se objevuje archetyp hackera – pubertální chlapec, který prostřednictvím svého počítače uskutečňuje své sexuální fantazie a kovbojské sny a je „*narušený, nepořádný, žijící jen skrze počítač a pro počítač, posedlý, vzdálený od normální mládeže, a tím pádem společensky mimo, postrádající schopnost interakce se skutečným světem*.“[109] Takové vnímání hackerů je ale poněkud přehnané.

Marcus Rogers rozděluje hackery do 8 kategorií podle toho, jaké mají úrovně znalostí a jaká je jejich motivace:

1) nováčci (Novice – NV);
2) cyber-punkeři (Cyber-punks – CP);
3) vnitropodnikoví (Internals – IN);
4) drobní zlodějíčkové (Petty Thieves – PT);
5) autoři virů (Virus Writers – VW);
6) stará hackerská garda (Old guard hackers – OG);

---

[108] BEDNARZ, Ann. Profiling cybercriminals: A promising but immature science. *NETWORKWORLD* [online]. 29. listopad 2004 [vid. 2020-01-02]. Dostupné z: https://www.networkworld.com/article/2327820/profiling-cybercriminals--a-promising-but-immature-science.html

[109] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 41. ISBN 978-80-903786-7-4.

7) profesionální zločinci (Professional criminals – PC);
8) informační bojovníci (Information warriors – IW).[110]

Nováčci mají pouze omezené počítačové a programovací znalosti a spoléhají na již dříve napsané, a tudíž dostupné softwarové nástroje. Vzhledem k tomu, že plně nerozumí tomu, jak útok funguje, mohou způsobit rozsáhlé škody. Typickými hackery této kategorie jsou mladší jednotlivci a jejich primární motivací je hledání vzrušení, pohlazení jejich ega a zisk pozornosti médií.

Cyber-punkeři mají lepší počítačové a programovací schopnosti a mohou část kódu napsat sami. Jejich hlavní činností je zejména odesílání spamu, krádeže čísel kreditních karet a telekomunikační podvody. Taktéž mají touhu po mediální pozornosti, v některých případech chtějí dosáhnout peněžního zisku.[111] Nejznámějším cyber-punkerem je Kevin Mitnick, který jako black hat hacker napadal sítě známých společností jako IBM, Nokia či Motorola. Poté, co si odpykal svůj trest ve vězení, své dovednosti uplatňuje jako white hat hacker a je světoznámým bezpečnostním konzultantem.[112]

Vnitropodnikoví hackeři představují největší hrozbu, a přitom o nich není tak často pojednáváno. Jak již název napovídá, jedná se o současné či bývalé nespokojené zaměstnance, kteří zneužívají znalost daných vnitřních systémů a napadají je. Zpravidla se jedná o IT zaměstnance a profesionály, kteří se v problematice orientují. Jejich motivem je nejčastěji pomsta.[113]

Drobní zlodějíčci využívají hackerské útoky v rámci pokroku v jejich kriminálních aktivitách. Subjekty, vůči nimž trestné činy provádějí, se totiž nedávno přesunuly do kyberprostoru, a tak jim nic jiného nezbývá. Příkladem jsou banky, užívání kreditních karet online apod. Mezi typické jedince patří zaměstnanci, dodavatelé a konzultanti a využívají špatné zabezpečení daných subjektů. Jejich hlavním cílem je zisk peněz,

---

[110] ROGERS, Marcus K. The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach. In: *CERIAS Tech Report 2005-43*. 2005.

[111] Ibid.

[112] GREENBERG, Andy. Kevin Mitnick, Once the World's Most Wanted Hacker, Is Now Selling Zero-Day Exploits. *WIRED* [online]. 24. září 2014 [vid. 2020-01-02]. Dostupné z: https://www.wired.com/2014/09/kevin-mitnick-selling-zero-day-exploits/

[113] ROGERS, Marcus K. The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach. In: *CERIAS Tech Report 2005-43*. 2005.

v některých případech se jedná o pomstu. Je třeba podotknout, že hackerská aktivita v tomto případě není jejich parketa, představuje pouze hazardování a ohrožuje jejich dosavadní úspěšný kriminální život.

Autoři virů nebo také kodéři představují speciální skupinu hackerů, kteří jsou mentory pro nové členy hackerské komunity. Jsou motivovaní pocitem síly a prestiží. Jsou velmi nebezpeční, a jak název napovídá, vytvářejí počítačové viry, které jsou následně šířeny. Bylo zjištěno, že ve chvíli, kdy současní autoři „zestárnou“, nahradí je noví nezkušení, kterým opět trvá delší dobu zjistit, že jejich aktivita není tak nevinná, jak se může zdát, a proto se od těchto aktivit následně distancují. Vzniká tak jakási kontinuita.[114]

Stará hackerská garda sestává z takových hackerů, kteří mají velmi vysoké technické znalosti a píšou kódy a skripty, které následně využívají ti méně zkušení jedinci. Často své výtvory někde zveřejňují a podněcují ostatní členy hackerské komunity k jejich používání. Nemají žádné kriminální úmysly, jejich motivací je zejména zvědavost a potřeba nějaké intelektuální výzvy.

Profesionální zločinci jsou opravdoví, vysoce trénovaní profesionálové, s přístupem k nejmodernějším technologiím, kteří si na svých vysokých technických znalostech a dovednostech postavili podnikání. Hlavním cílem je pochopitelně zisk. Pachatelé jsou technicky prozíraví a velmi psychicky vyspělí. V určitých případech jejich služeb využívají nějaké organizované zločinecké skupiny. Někteří se specializují na obchodní špionáž.[115]

Poslední skupinou jsou informační bojovníci, kteří provádějí útoky, jejichž záměrem je destabilizovat, narušit nebo nějakým způsobem ovlivnit integritu dat nebo informačních systémů. Jsou velmi dobře financováni, často dokonce státem za účelem válčení, a jsou

---

[114] GORDON, Sarah. Virus writers: the end of the innocence? In: *10th Annual Virus Bulletin Conference (VB2000), Orlando, FL*. 2000.

[115] ROGERS, Marcus K. The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach. In: *CERIAS Tech Report 2005-43*. 2005.

vysoce kvalifikovaní a motivovaní patriotismem. Velmi často se věnují hacktivismu[116]. Někdy je tato skupina označována jako kyber-teroristi.[117]

Jirovský rozděluje pachatele do šesti kategorií. První z nich jsou kriminální hackeři (crackeři), jejichž cílem je zisk. Druhou kategorií jsou profesionální hackeři – dále rozděleni na black, white a grey hats. Do třetí kategorie spadají nespokojení zaměstnanci, jakožto nejnebezpečnější skupina. Čtvrtou kategorií jsou ideologičtí hackeři, kteří se snaží šířit své politické nebo ideologické cíle. Bývají označováni jako hacktivisté a jejich aktivity jsou často spojeny s nějakou politickou nebo ekonomickou událostí. Další kategorie hackerů se nazývá script-kiddies a zahrnuje nejmladší jedince, kteří nemají prakticky žádné technologické znalosti, a přesto využívají volně dostupné hackerské nástroje. Neuvědomují si ale možné dopady takovýchto zásahů. Poslední kategorií jsou tzv. nevyužití dospělí hackeři, kteří nenašli své uplatnění v dané hackerské komunitě.[118]

Obě dvě výše zmiňované kategorizace pachatelů se ve velké míře překrývají. Nikde ale není stanovena žádná společná kategorizace, která by pomohla vytvořit profil pachatele. Podle Kuchty by „*psychologickému profilu pachatele měla být v kriminologických výzkumech věnována pozornost, což se u nás dosud neděje*.“[119] Stejný názor zastává i Marcus Rogers, který by chtěl vidět tradiční profilování pachatelů v oblasti počítačové forenzní vědy, podle něj „*je na čase, abychom se na počítač a internet podívali jako na elektronické místo činu a podívali se po ukazatelích charakteristických znaků chování a modu operandi, což by nám umožnilo vidět odpovědného jedince v celé své kráse.*“[120]

---

[116] Hacktivismus vznikl spojením slova „hack“ a „aktivismus“ a znamená proces napadnutí počítačového systému za politickým či sociálně motivovaným účelem. In: FRANKENFIELD, Jake. Hacktivism. *Investopedia* [online]. [vid. 2020-01-02]. Dostupné z: https://www.investopedia.com/terms/h/hacktivism.asp

[117] ROGERS, Marcus K. The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach. In: *CERIAS Tech Report 2005-43*. 2005.

[118] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 56. ISBN 978-80-247-1561-2.

[119] KUCHTA, Josef. Aktuální problémy počítačové kriminality včetně její prevence. *Časopis pro právní vědu a praxi*. 2016, (1), 5–19.

[120] BEDNARZ, Ann. Profiling cybercriminals: A promising but immature science. *NETWORKWORLD* [online]. 29. listopad 2004 [vid. 2020-01-02]. Dostupné z: https://www.networkworld.com/article/2327820/profiling-cybercriminals--a-promising-but-immature-science.html

Kromě Kevina Mitnicka se proslavili i další jedinci. Mezi další známé hackery patří Kevin Poulsen, Robert Tappan Morris, John McAfee, Eugene Kaspersky, Jonathan James, Stephen Wozniak, ASTRA a mnoho dalších.[121] Existuje i velké množství hackerských skupin, z nichž nejznámější je Anonymous. Další je třeba Lizard Squad, The Level Seven Crew, Chaos Computer Club aj.[122]

4.2 Motiv

Motiv pachatele kyberzločinu je velmi podstatným aspektem kybernetického trestného činu. Pro následné zjištění pachatele je znalost motivu klíčová. Počítačová kriminalita je obvykle anonymní a může pocházet z prakticky nekonečného množství míst na internetu. Schopnost odlišit jedinečné chování pachatele je neocenitelnou pomocí při vyšetřování.[123] Mezi typické motivy, již výše zmiňované, patří především finanční zisk, pomsta, prosté hledání vzrušení, zvědavost, zábava, dobrodružství nebo šíření politického či ideologického přesvědčení. V mnohých případech má pachatel motivů hned několik.

Smejkal uvádí, že mezi motivy může patřit pocit převahy nad zaměstnavatelem (resp. státem, veřejností), snaha kompenzovat svou nespokojenost ať už s prací, či osobním životem. Dále to může být pocit ublížení, nenávist, závist nebo vykořisťování zaměstnance zaměstnavatelem. Motivem může být i touha po moci, zastírání jiné trestné činnosti, jako jsou například daňové úniky, nebo snaha uspořit nějaké peníze či získat jinou výhodu. V oblasti autorskoprávních deliktů je to zejména vidina zisku a snížení nákladů.[124]

Furnell uvádí motivy kyberzločinů podle skupin pachatelů a jejich charakteristik. Pachatele dělí na kyberteroristy (angl. *Cyberterrorists*), kyberbojovníky (angl. *Cyber warriors*), hacktivisty, autory malwaru (angl. *Malware writers*), „Old School“ hackery,

---

[121] 10 Most Notorious Hackers of All Time. *Hacked: Hacking Finance* [online]. 3. září 2015 [vid. 2020-01-03]. Dostupné z: https://hacked.com/hackers/

[122] RAZA, Ali. 10 Most Notorious Hacking Groups. *HackRead* [online]. 20. leden 2016 [vid. 2020-01-02]. Dostupné z: https://www.hackread.com/10-most-notorious-hacking-groups/

[123] WORI, Okechukwu. Computer Crimes: Factors of Cybercriminal Activities. *International Journal of Advanced Computer Science and Information Technology; Vol 3, No 1 (2014)* [online]. 2014. Dostupné z: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-136

[124] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 688–689. ISBN 978-80-7380-720-7.

phreakery, samuraje, Script Kiddies a Warez d00dz (*Wares Dudes*). K bližšímu porozumění prolínání motivů jednotlivých skupin pachatelů vypracoval následující tabulku.[125]

Tabulka 2 Motivace pachatelů

	Výzva	**Ego**	**Špionáž**	**Ideologie**	**Neplecha**	**Peníze**	**Pomsta**
Kyber teroristé				✓			✓
Kyber bojovníci			✓	✓		✓	
Hacktivisté				✓			✓
Autoři malware	✓	✓	✓		✓	✓	✓
Old School		✓		✓			
Phreakers	✓	✓			✓	✓	
Samuraj	✓					✓	
Script Kiddies		✓			✓		✓
Warez d00dz	✓	✓		✓		✓	

Je patrné, že motivy pachatelů jsou různorodé a odlišné pro každou kategorii pachatelů. Mezi každým typem hackera, a tudíž jeho motivy, existuje jen tenká hranice. Jeden hacker nemusí mít pouze jedinou motivaci, ale i více. V tomto směru je možné hackerské

[125] FURNELL, S. M. The Problem of Categorising Cybercrime and Cybercriminals. In: *Survival in the e-economy: proceedings: 2nd Australian Information Warfare & Security Conference*. Churchlands, W.A.: Edith Cowan University, School of Management Information Systems, We-B Centre, 2001, s. 34–35. ISBN 978-0-7298-0499-8.

dovednosti vnímat jako obecné – lze je vhodně použít v jakékoliv situaci a kdykoliv přímo na míru potřebám a motivaci hackera.[126]

V letech 2003–2004 započal projekt HPP – The Hacker‘s Profiling Project – kde bylo pomocí dotazníků vyplněných hackery v různých zemích světa analyzováno velké množství dat. Mezi zjištěné motivy patří všechny výše zmíněné, ale objevilo se i několik nových: láska k technologiím; nuda při normálním používání počítače; požitek z řešení problémů; zlepšení počítače; zabezpečení světa počítačů; útěk z konfliktního domácího prostředí; boj za svobodu; rutina, vztek a frustrace.

Důležité je zmínit, že motivace hackerů se mění v průběhu doby – v sedmdesátých letech byla hlavní hnací silou touha po poznání, v osmdesátých letech zejména zvědavost a módní trend, v devadesátých letech bylo cílem pouze hackovat a narušovat tak počítačové systémy, čtvrtá generace hackerů v novém tisíciletí byla poháněna vztekem a poprvé se začíná objevovat hacktivismus.[127] Pátá generace hackerů by spadala do let 2010–2020, kdy nastal veliký rozmach technologií a z hackerů se staly profesionální organizované skupiny provádějící masové kyberútoky na infrastruktury státu či velkých společností.

Lze konstatovat, že velká většina hackerů má přece jen nějaké společné znaky: obvykle mají vyšší než průměrné IQ a velmi dobré technické dovednosti a znalosti v oblasti řešení problémů. Jsou to brilantní adolescenti, kteří se potýkají s nedostatečně kvalitním vzdělávacím systémem, kde je vyučují špatně připravení nebo nevybavení učitelé. Obvykle pocházejí z problémových rodin a bouří se proti jakýmkoliv symbolům či projevům autority.[128] Vytvoření realistického vyobrazení hackera ovšem není snadné, protože musíme vzít v potaz velmi velké množství aspektů a přístupů, abychom zjistili, jaké jsou jeho motivy. Přitom dochází neustále k vývoji a svět hackerů se mění, roste a stává se více komplexním a hierarchickým.[129]

---

[126] Ibid.

[127] CHIESA, Raoul, Stefania DUCCI a Silvio CIAPPI. *Profiling hackers: the science of criminal profiling as applied to the world of hacking*. Boca Raton: Auerbach Publications, 2009, s. 145–147. ISBN 978-1-4200-8693-5.

[128] Ibid., s. XXII.

[129] Ibid., s. 189.

4.3 Digitální důkazy

Digitální (počítačová) stopa je dle SWGDE[130] (Scientific Working Group on Digital Evidence) definována jako „*jakákoliv informace s vypovídající hodnotou pro danou relevantní událost, uložená nebo přenášená v digitální podobě*.“[131] Digitální důkaz může být definován jako „*jakákoli data uložená nebo přenesená za použití počítače, která podporují nebo vyvracejí teorii o tom, jak se čin stál, či která pomáhají vysvětlit záměry pachatele, nebo jeho alibi*.“[132]

Jiné zdroje definují digitální stopu jako jakoukoliv důkazní informaci uloženou nebo přenesenou digitálně.[133] Digitální stopa by ale neměla být vždy spojována s důkazním prostředkem, protože ne vždy bude jako důkaz použita v řízení před soudem.[134] Proto je nejlepší digitální stopu chápat jako „*jakákoli data či informace přenesená, vytvořená, uložená či modifikovaná za použití počítačového systému*.“[135]

Stejně jako má kyberprostor své specifické aspekty, má je i digitální stopa (důkaz). Zpravidla je totiž digitální stopa velkého datového objemu a vyskytuje se v extrémně dynamickém, heterogenním a komplexním prostředí. Vyznačuje se latentností, velmi

---

[130] SWGDE je vědecká skupina zabývající se digitálními důkazy, která vznikla v roce 1998. Členové této skupiny mají mnohaleté zkušenosti v oboru forenzní analýzy digitálních důkazů a jsou to převážně členové významných organizací, jako je Americká akademie forenzních věd, IACIS (International Association of Computer Investigative Specialists), HTCIA (High Technology Crime Investigation Association) nebo IOCE (International Organization for Cooperation in Evaluation). In: POLLITT, M. Mark. *Who is SWGDE and what is the history?* [online]. 22. leden 2003 [vid. 2020-02-28]. Dostupné z: https://www.swgde.org/pdf/2003-01-22%20SWGDE%20History.pdf

[131] RAK, Roman a Viktor PORADA. Vlastnosti digitálních stop a jejich dopady na forenzní šetření. *Soudní inženýrství*. 2005, **16**(4), 183–192.

[132] CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the Internet*. 3rd ed. Waltham, MA: Academic Press, 2011, s. 7. ISBN 978-0-12-374268-1.

[133] Digital Evidence Law and Legal Definition. *USLegal, Inc.* [online]. [vid. 2019-11-22]. Dostupné z: https://definitions.uslegal.com/d/digital-evidence/

[134] Digitální stopy mohou být důkazní (slouží jako věcný důkaz), indikativní (nepřímé informace pomocí kterých zjistíme další souvislosti) či profilové (charakterizují pachatele a ukazují jeho profesní či osobní zájmy). In: RAK, Roman a Viktor PORADA. Vlastnosti digitálních stop a jejich dopady na forenzní šetření. *Soudní inženýrství*. 2005, 16(4), 183–192.

[135] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z.s.p.o., 2016, s.402–403. ISBN 978-80-88168-18-8.

nízkou životností a nestálostí, a typicky se bude jednat o nehmotný statek, který ale vždy zanechává hmotný otisk na nějakém hmotném statku.[136]

Digitální stopy patří do kategorie věcných a listinných důkazů dle § 112 odst. 1 a 2 TŘ. Elektronické dokumenty patří do listinných důkazů; počítače, počítačové systémy a nosiče dat patří do věcných důkazů.[137] „*Zajímavou formou důkazu může být záznam o elektronické komunikaci. Do doby, kdy je záznam v elektronické podobě, může být definován obecně jako důkaz věcný. V okamžiku, kdy je záznam vytištěn na tiskárně, mohl by být považován za důkaz listinný*."[138]

Podle Koloucha současná subsumpce digitálních důkazů pod věcné a listinné není dostačující a bylo by vhodné zavést samostatnou kategorii digitálních důkazů v TŘ. Nový odstavec 3 příslušného § 112 by podle něj mohl vypadat následovně:

> „*Digitálním důkazem jsou jakákoli data či informace, jež byly přeneseny, vytvořeny, uloženy či modifikovány za použití počítačového systému a které prokazují nebo vyvracejí dokazovanou skutečnost a mohou být prostředkem k odhalení a zjištění trestního činu a jeho pachatele, jakož i stopy trestného činu*."[139]

Při zajišťování digitálních stop je vždy nejprve nutné vytvořit identickou binární kopii původního nosiče dat, což má zachovat integritu a spolehlivost takových stop. Je pak možné zkoumat vytvořenou kopii, aniž by došlo k jakémukoliv pozměnění původního nosiče dat. Metoda, která toto umožňuje, se nazývá klasická digitální forenzní analýza statických datových nosičů, která je jedním z druhů digitální forenzní analýzy, „*exaktní forenzní vědy, která zkoumá procesy a zákonitosti vzniku, existence a zániku digitální informace v prostředí informačních systémů*."[140]

---

[136] RAK, Roman a Viktor PORADA. Vlastnosti digitálních stop a jejich dopady na forenzní šetření. *Soudní inženýrství*. 2005, **16**(4), 183–192.

[137] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 694. ISBN 978-80-7380-720-7.

[138] FENYK, Jaroslav, Tomáš GŘIVNA a Dagmar CÍSAŘOVÁ. *Trestní právo procesní*. 7. Praha: Wolters Kluwer, 2019, s. 418. ISBN 978-80-7598-306-0.

[139] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z. s. p. o., 2016, s. 419. ISBN 978-80-88168-18-8.

[140] HOLOŠKA, Jiří a Marián SVETLÍK ST. Sedm hříchů digitální forenzní analýzy. *Digital Forensic Journal*. 2014, (2). ISSN 2336-4769.

Dnes je ale mnohem potřebnější digitální forenzní analýza živých systémů (angl. *Live Forensics*), která umožňuje zajištění digitálních stop ze „živých“ systémů, které nelze pro účely analýzy vypnout nebo je k analýze třeba, aby stále běžely. Typicky se bude jednat o tablety a mobilní telefony.[141] V tomto případě nelze vytvořit binární kopii nosiče dat, ale je nutné zasáhnout do originálního nosiče dat, což v tu chvíli zasahuje do integrity digitální stopy. Hlavním problémem jsou neustále běžící procesy a datové toky, dále samotný analytický programový nástroj se stává součástí zkoumaného systému a sám provádí změny na nosiči dat, a pro použití analytického nástroje je třeba využití funkcí dotčeného operačního systému.[142]

V mnoha případech se data vůbec nenacházejí na daném nosiči dat, ale na nějakém cloudovém úložišti. To je velmi problematické, protože je velmi obtížné zjistit, kde se fyzicky nachází nosič dat, a navíc je zpravidla ve vlastnictví nějakého třetího subjektu, nacházejícího se v zahraničí, tedy mimo jurisdikci daného státu.[143]

Při vyšetřování trestného činu za využití digitálních stop je pro úspěšné objasnění klíčových skutečností a dopadení pachatele nezbytné pracovat rychle a zachovat co nejkratší čas mezi přijetím trestního oznámení a zahájením prověřování. Je nutné spolupracovat s vysoce kvalifikovanými odborníky a zachovat původ, integritu a obnovitelnost digitálních stop.[144]

Technická norma ISO/IEC 27037:2012[145] (Informační technologie – Bezpečnostní techniky – Směrnice pro identifikaci, sběr, akvizici a uchovávání digitálních důkazů)

---

[141] VEBER, Jaromír, Zdeněk SMUTNÝ a Ladislav VYSKOČIL. Practice of Digital Forensic Investigation in the Czech Republic and ISO/IEC 27037:2012 [in Czech]. *Acta Informatica Pragensia* [online]. 2015, **4**, 242–257. Dostupné z: doi:10.18267/j.aip.72

[142] PORADA, Viktor a Eduard BRUNA. Digitální svět a dokazování obsahu elektronických dokumentů. *Bezpečnostní technologie, systémy a management*. 2013, (3).

[143] HOLOŠKA, Jiří a Marián SVETLÍK ST. Sedm hříchů digitální forenzní analýzy. *Digital Forensic Journal*. 2014, (2). ISSN 2336-4769.

[144] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 700. ISBN 978-80-7380-720-7.

[145] Norma ISO/IEC 27037:2012 patří do rodiny norem ISO 27000, které se zabývají bezpečností informací. Konkrétně tato norma má za cíl upravit postup pro sběr digitálních stop „*a patří do skupiny standardů pro nejlepší postupy v praxi (best practices)*“. In: VEBER, Jaromír, Zdeněk SMUTNÝ a Ladislav VYSKOČIL. Practice of Digital Forensic Investigation in the Czech Republic and ISO/IEC 27037:2012 [in Czech]. *Acta Informatica Pragensia* [online]. 2015, **4**, 242–257. Dostupné z: doi:10.18267/j.aip.72

blíže upravuje rámec nakládání s digitálními stopami zejména s ohledem na manipulaci s nimi, první identifikaci, shromažďování a jejich následné uchovávání. Při zacházení s digitálními stopami je nutné dodržovat požadavky kontrolovatelnosti, ospravedlnitelnosti, opakovatelnosti a reprodukovatelnosti při zachování relevantnosti, spolehlivosti a dostatečnosti digitálních stop.

Fyzická osoba, která jako první přichází do styku s digitálním důkazem a je k nakládání s ním dostatečně odborně kvalifikována, je normou ISO/IEC 27037:2012 označována jako DEFR (Digital Evidence First Responder). Tato osoba (DEFR) by měla dodržovat následující základní principy:

- „*Minimalizovat manipulaci s digitálním zařízením či digitálními daty.*
- *Zdokumentovat veškeré akce a změny provedené s danou digitální stopu tak, aby si mohl nezávislý expert vytvořit názor na spolehlivost předložených důkazů.*
- *Postupovat v souladu se zákony dané země.*
- *DEFR by neměl postupovat nad rámec své působnosti*."[146]

Norma ISO/IEC 27037:2012 dále upravuje dílčí procesy manipulace s digitálními důkazy, mezi něž patří identifikace, zajištění zařízení, zajištění dat a jejich uchování. Při práci s důkazy musí být veškerý postup pečlivě zaznamenáván, místo incidentu musí být dobře ochráněno, DEFR by měl být k dané práci dostatečně technicky kvalifikovaný a právně vzdělaný, měl by se vyhnout takovým aktivitám, které mohou digitální stopy znehodnotit, vše důkladně dokumentovat a zabezpečit digitální stopy tak, aby nedošlo k jejich zničení. Norma dále podrobněji upravuje postupy zajištění digitálních zařízení, síťových zařízení a zajištění kamerových systémů, kdy každý z nich má svá specifika. Dle odborníků z praxe Vyskočila a Světlika však norma dostatečně obsáhla pouze obecná doporučení. Praktická doporučení jsou již obsoletní a nereflektují současnou praxi vyšetřovatelů. I přesto umožnila zvýšit povědomí o specifických aspektech práce s digitálními důkazy.[147]

---

[146] VEBER, Jaromír, Zdeněk SMUTNÝ a Ladislav VYSKOČIL. Practice of Digital Forensic Investigation in the Czech Republic and ISO/IEC 27037:2012 [in Czech]. *Acta Informatica Pragensia* [online]. 2015, **4**, 242–257. Dostupné z: doi:10.18267/j.aip.72

[147] Ibid.

Při užívání digitálních důkazů vyvstává otázka ochrany základních lidských práv a svobod. I při využívání digitálních důkazů a ICT prostředků během trestního řízení musí být zachováno právo na spravedlivý proces.[148] Velmi často se při uplatňování digitálních důkazních prostředků v trestním řízení zasahuje do práva na ochranu soukromí, zejména do práva na ochranu osobních údajů. Při vyšetřování trestných činů je možné vyhledávat velké množství dat v různých databázích (např. Google, zákaznické databáze, sociální sítě, věrnostní programy, záznamy z CCTV kamer), lze také používat polohová data, údaje o prohlížení webových stránek a RFID[149]. Díky digitalizaci, automatizovanému rozpoznávání a sdílení dat je dnes mnohem snazší data zpracovávat. Pomocí chytrých technologií, miniaturních kamer, skrytých mikrofonů, chytrého prachu, leteckých snímků a dalších vymožeností dnešní doby můžeme získat taková data jako nikdy předtím.[150]

Problém představuje zejména vyšetřovací fáze, kdy je pomocí veškerých dostupných informačních technologií (teplotní senzory, nahrávací zařízení, parabolické mikrofony, zařízení pro zachycení e-mailové komunikace, sledovací technika a další) umožněno provést rozsáhlé sledování, které vyšetřovatelům umožňuje překonat fyzické bariéry (zdi, tašky, šaty), které jsou standardně určeny k ochraně jednotlivce a jeho soukromí.[151]

Ochrana osobních údajů je jedním ze základních práv a musí být zachována i v digitálním světě. Právě soukromí musí být považováno za jednu z nejvyšších hodnot současné demokratické společnosti a musí být všem přístupné bez rozdílu. Podle autorů Warrena

---

[148] Článek 6 Evropské úmluvy o ochraně lidských práv ve znění Protokolů č. 11 a 14 s Protokoly č. 1, 4, 6, 7, 12, 13 a 16.

[149] Radio Frequency Identification, neboli Identifikace na rádiové frekvenci se dnes používá k identifikaci různých objektů. Příkladem jsou čipy při běžeckých závodech, čipy psů, čipy v cestovních pasech a další. Užití RFID vzbuzuje bezpečnostní otázky, protože kdokoliv mající správnou čtečku nacházející se v blízkosti daného čipu může citlivá data snadno získat a následně zneužít.

[150] TEEUW, Wouter B. a Anton VEDDER, ed. *Security Applications for Converging Technologies - Impact on the constitutional state and the legal order* [online]. B.m.: TELEMATICA INSTITUUT, ENSCHEDE. 2008 [vid. 2020-01-01]. Dostupné z: https://pure.uvt.nl/ws/portalfiles/portal/951064/Security_Applications_for_Converging_Technologies_WODC.pdf

[151] SIMONATO, Michele. Defence rights and the use of information technology in criminal procedure. *Revue internationale de droit pénal* [online]. 2014, **85**(1–2), 261–310. ISSN 9782749242224. Dostupné z: doi:10.3917/ridp.851.0261

a Brandeise je soukromí dynamickým konceptem a je třeba se vždy adaptovat aktuálním potřebám a hodnotám jednotlivců. [152]

Již v roce 1990 zveřejnila OSN instrukce pro nakládání s počítačovými osobními datovými soubory. Mezi hlavní zásady patří zásada zákonnosti a poctivosti, zásada přesnosti, zásada specifikace účelu, zásada přístupu zainteresované osoby, zásada nediskriminace a zásada bezpečnosti. Jedná se pouze o nezávazný dokument, který slouží jako podklad pro aktuální právní úpravu.[153]

Mezinárodní společnost pro trestní právo (AIDP)[154] se v roce 2014 na svém 19. setkání v Rio de Janeiru věnovala vztahu počítačové kriminality a trestního práva procesního a v závěru vydala řadu doporučení i ve vztahu k ochraně lidských práv. Jakýkoliv zásah do práva na soukromí musí být na základě zákona a musí být proporcionální, legitimní a nezbytný v demokratické společnosti. Při užívání informačních technologií v rámci trestního procesu je třeba veškeré zásahy činit s respektem k právu na ochranu osobních údajů a nesmí být porušeno právo na spravedlivý proces, mimo jiné právo na veřejné jednání, právo na přístup ke spisu a právo na přístup k obhajobě, která se specializuje v oblasti elektronických důkazů a zajistí tak rovnost stran.[155]

Podle AIDP by mělo být umožněno rychlé uchovávání a ukládání digitálních dat a měly by být k dispozici forenzní nástroje, které zabrání jakémukoliv pozměnění digitálních stop. Obhajoba by měla mít vždy zaručený přístup k digitálním důkazním prostředkům, aby bylo možné ověřit jejich pravost a případně ji i napadnout u soudu. Digitální důkazy

---

[152] WARREN, Samuel D. a Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review* [online]. 1890, **4**(5), 193–220. ISSN 0017811X. Dostupné z: doi:10.2307/1321160

[153] UN GENERAL ASSEMBLY. *Guidelines for the Regulation of Computerized Personal Data Files* [online]. 14. prosinec 1990 [vid. 2020-01-01]. Dostupné z: https://www.refworld.org/docid/3ddcafaac.html

[154] Association Internationale de Droit Pénal – Mezinárodní společnost pro trestní právo – je nejstarší organizací na světě, která sdružuje odborníky na trestní právo. Byla založena v roce 1924 a zabývá se trestní politikou a kodifikací trestního práva, srovnávacím trestním právem, mezinárodním trestním právem a také lidskými právy při výkonu trestního soudnictví. In: History of the International Association of Penal Law. *Association Internationale De Droit Pénal* [online]. [vid. 2020-01-02]. Dostupné z: http://www.penal.org/en/node/168

[155] Section III – Criminal Procedure. *Revue internationale de droit pénal*. 2014, **85**(3–4), 613–618. ISSN 9782749246499.

získané přímo či nepřímo takovými prostředky, které představují porušení základních práv a svobod, které mají zajistit rovnost stran a spravedlivý proces, jsou nepřípustné.[156]

4.4 Vyšetřování

Metodika

Kyberkriminalita má specifický charakter, a proto byla v průběhu času vytvořena zvláštní metodika, která umožňuje se s problematickými aspekty vypořádat. Vzhledem k variabilitě kybernetických trestných činů, dynamice a složitosti informačních systémů je nutné vytvořit specializovaný tým složený z odborníků, který bude vést samotné vyšetřování. Vyšetřováním kyberzločinů se zabývá zvláštní část kriminalistiky.[157]

Vyšetřování kyberkriminality se v současné době potýká s několika problémy. Prvním z nich je problém jurisdikce, který souvisí s výše zmiňovaným specifickým aspektem kyberprostoru – jeho neomezenost a všudypřítomnost. „*Fyzické servery se mohou nacházet kdekoli na světě. Virtuální servery se mohou nacházet na kterémkoliv z nich, například ve výpočetním centru nadnárodní společnosti, kam mají přístup uživatelé z celého světa na dálku, aniž by vnímali, že se – z hlediska právního řádu – ocitají v jiném teritoriu. V případě Internetu uživatel pak obvykle vůbec neví, kde se nachází zařízení, jehož IP adresu zadá či obdrží*.“[158]

Při vyšetřování kyberkriminality hraje důležitou roli evropský vyšetřovací příkaz. Směrnice Evropského parlamentu a Rady 2014/41/EU o evropském vyšetřovacím příkazu v trestních věcech byla přijata dne 3. dubna 2014. Česká republika měla povinnost daná ustanovení implementovat do vnitrostátního práva a bylo tak učiněno zákonem č. 178/2018 Sb., který novelizoval zákon o mezinárodní justiční spolupráci ve věcech trestních. Právní úprava evropského vyšetřovacího příkazu je pak obsažena v § 357-395 tohoto zákona. Dle § 358 se evropským vyšetřovacím příkazem rozumí příkaz: (a) vydaný justičním orgánem za účelem provedení úkonu právní pomoci s cílem

---

[156] Ibid.

[157] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 86–87. ISBN 978-80-903786-7-4.

[158] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 703. ISBN 978-80-7380-720-7.

opatřit důkaz na území jiného členského státu, nebo (b) vydaný justičním orgánem jiného členského státu nebo jiným než justičním orgánem jiného členského státu, který má v tomto členském státu pravomoc opatřovat důkazy, pokud jím vydaný příkaz potvrdil justiční orgán tohoto členského státu, za účelem provedení úkonu právní pomoci s cílem opatřit důkaz na území České republiky.

Evropský vyšetřovací příkaz je založen na zásadě vzájemného uznávání a dává si za cíl zavést komplexní systém pro získávání důkazů. „*Vykonávající orgán je povinen uznat žádost jiné země a zajistit její výkon. Příkaz je třeba vykonat stejným způsobem a za stejných podmínek, jako by daný vyšetřovací úkon byl nařízen orgánem vykonávajícího státu*.“[159] Může být využit i při získávání již existujících důkazů. Mezi dané vyšetřovací úkony patří například výslech svědků, telefonické odposlechy a další. V současné době je projednáván návrh nařízení Evropského parlamentu a Rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech 2018/0108/COD. V oblasti elektronických důkazů by tak mohlo být usnadněno jejich přeshraniční zajišťování.

V § 4 TZ je upravena jedna ze zásad místní působnosti, a to zásada teritoriality. Kyberzločiny se pak nejčastěji budou řadit do tzv. distančních deliktů a „*postačí, aby tu bylo provedeno jednání, i když následek (zpravidla půjde o účinek) nastal v cizině, nebo naopak (...). I když trestný čin byl započat i dokonán v cizině (...) je trestný, mělo-li k dokončení trestného činu podle záměru pachatele dojít v tuzemsku (...)*.“[160] Při vyšetřování je důležitá mezinárodní spolupráce, díky které mohou být důkazy včas zajištěny. V rámci Interpolu existuje Cyber Fusion Centre, které sdružuje experty na téma kyberkriminalita a analyzuje veškerou zločineckou aktivitu v kyberprostoru. Spolupráce probíhá i na úrovni Rady Evropy na základě Úmluvy o počítačové kriminalitě.

Druhý problém se týká odhalování trestné činnosti a je způsoben několika důvody. Prvním z nich je skutečnost, že mnoho obětí kyberzločinu tento skutek vůbec neoznámí

---

[159] EVROPSKÁ UNIE. Evropský vyšetřovací příkaz, vzájemná právní pomoc a společné vyšetřovací tým. *Portál evropské e-Justice* [online]. [vid. 2020-03-07]. Dostupné z: https://e-justice.europa.eu/content_european_investigation_order_mutual_legal_assistance_and_joint_investigation_teams-92--maximize-cs.do

[160] ŠÁMAL, Pavel. § 4 [Zásada teritoriality]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník I. § 1 až 139. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 69. ISBN 978-80-7400-428-5.

policii. Dále i když jsou trestné činy oznámeny, tak je policie kvůli nízké závažnosti ani nezačne prověřovat. Ve chvíli, kdy je nějaký trestný čin oznámen a začne být prověřován, je velmi obtížné pachatele vypátrat a usvědčit za pomoci dostatečného množství digitálních stop. Podle Smejkala by ke zvýšení efektivity trestního řízení pomohlo používání takových nástrojů, „*které jsou schopny zavčas odhalit, že došlo k mimořádné události (expertní systémy, vyhodnocování statistik apod.), zadokumentovat, co se v systému stalo (auditní stopy, logy, forenzní audit) a (…) co nejrychleji takové podezření oznámit kvalifikovaným orgánům činným v trestním řízení*.“ Podstatná je hlavně spolupráce oběti, která musí být dostatečně obezřetná. V případě, že obětí je nějaká společnost, musí mít implementovaný takový bezpečnostní systém, který umožní rychlé odhalení kriminální aktivity a její zaznamenání.

Třetím problémem vyšetřování kyberkriminality je dokazování, což je způsobeno specifickými vlastnostmi digitálních důkazů. Jak již bylo zmíněno výše, je problematické zjistit, kde se dané důkazy nachází, také kde se nacházel pachatel a jiné indicie potřebné k odhalení trestné činnosti. Problematický aspekt je čas – v počítači lze kdykoliv pozměnit časové údaje, samotný počítačový systém může být od začátku nastaven na jiné časové pásmo. S tím souvisí i dynamické prostředí počítače, které se neustále mění v čase, a stopy, které jsou potřeba k prokázání spáchání trestného činu, již nemusí být k nalezení. Problematickým aspektem je i čitelnost dat, která mohou být zaheslována, šifrována či jinak ukryta, nebo dokonce úmyslně zničena samotným pachatelem. Problematická je i identifikace a autentizace dat a prokázání, kdo je skutečným autorem dokumentu.[161]

V kybernetickém prostoru je obzvláště výzvou zjistit, zda je daná digitální stopa pravá. Dle Smejkala lze pochybovat ve dvou oblastech: „*(1) pravost dokumentů a datových zpráv, (2) pravost IP adres, e-mailových adres a jiných adres v kyberprostoru*.“[162] Důležitou roli zde hrají metadata, což jsou data, která poskytují informace o jiných datech. „*Obsahují doplňující informace o dokumentu, například dobu jeho pořízení, kdo*

---

[161] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 706–708. ISBN 978-80-7380-720-7.

[162] Ibid., s. 709.

jej pořídil, jaká verze jakého programu jej vytvořila."[163] V běžném případě je možné metadata modifikovat (snadným přepsáním příslušného atributu v textovém editoru), což znamená, že na ně při dokazování nelze spoléhat. Stejný problém nastává i v oblasti e-mailové korespondence, kdy lze pozměnit údaje v databázi e-mailů, stejně tak jako hlavičky jednotlivých e-mailových zpráv. Co se týče adres v kyberprostoru, je problematické zjistit, kdo se za danou IP adresou skrývá. Problémem je již výše zmiňované užívání VPN, ale také připojení se na veřejné Wi-Fi sítě, které v daný okamžik mohou používat stovky lidí a dohledání konkrétní osoby je velmi obtížné.[164]

Průkaznost důkazů je rovněž problematická. Jedná se zejména o postupy kriminalistů či odborníků, které mohou být nekvalifikované, nejednotné či prováděné pod nedostatečně implementovanou metodikou. Z hlediska digitálních stop může dojít k nedostatečnému zaevidování všech provedených úkonů, nebo dokonce ke zničení stop a nezachování integrity dané stopy.[165]

Zvláštnosti předmětu vyšetřování

V § 89 odst. 1 TŘ je vymezen předmět dokazování, který má ale pro oblast kyberkriminality svá specifika. Je potřeba zjišťovat, zejména zda se jedná o jeden či více skutků; informace o vlastním útoku; informace o počítačovém systému; informace o datech; informace o pachateli; okolnosti, které umožnily spáchání trestného činu; informace o nastavených oprávněních. V rámci těchto jednotlivých bodů se zjišťují všechny konkrétní aspekty činu, jako je například struktura a délka útoku, zda vznikla škoda, jaká je její výše, na kterém počítači byl útok proveden, jaká je verze operačního systému, povaha dat a případná manipulace s nimi, zda se na činu podílelo více osob, rozsah znalostí pachatele o výpočetní technice, jeho motiv apod.[166] „*Společnou zvláštností dokazování (...) kybernetické kriminality je dále to, že její charakter nelze*

---

[163] POLČÁK, Radim, František PÚRY a Jakub HARAŠTA. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, s. 95. ISBN 978-80-210-8073-7.

[164] SMEJKAL, Vladimír a Michal VALÁŠEK. Co všechno lze falzifikovat v ICT aneb důkazy nejsou vždy důkazy. In: *Sborník příspěvků z mezinárodní vědecké kriminalistické konference Pokroky v kriminalistice 2017 konané na Policejní akademii České republiky v Praze ve dnech 12. a 13. září 2017*. Praha: Policejní akademie České republiky, 2018, s. 253–272. ISBN 978-80-7251-485-4.

[165] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 715–716. ISBN 978-80-7380-720-7.

[166] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z.s.p.o., 2016, s.406–407. ISBN 978-80-88168-18-8.

dovodit ze skutkové podstaty trestného činu aplikovaného na daný skutek. Charakter kybernetické kriminality je dovozován ze způsobu spáchání (modus operandi).“[167]

Zvláštnosti podnětů k vyšetřování

Kybernetická kriminalita se vyznačuje vysokým stupněm latence. V mnohých případech, jak již bylo zmiňováno výše, napadené instituce (např. banky, školy) neoznamují spáchání trestného činu, protože by to mohlo způsobit paniku klientů a poškození dobré pověsti. Aby mohla být kybernetická trestná činnost odhalena a dostatečně účinně potírána, je třeba, aby byly trestné činy oznámeny. Podněty k vyšetřování mohou být rozděleny do těchto kategorií: (1) výsledky operativně pátrací činnosti orgánů činných v trestním řízení, (2) oznámení kontrolních, inspekčních a revizních orgánů různých institucí, (3) oznámení fyzických či právnických osob, (4) ostatní oznámení (anonymní, bezpečnostní a detektivní organizace). V rámci činnosti orgánů činných v trestním řízení může být využíváno také činnosti informátorů, která ale „*ve většině případů naráží na bankovní tajemství (…) či jinou zákonnou povinnost mlčenlivosti (…), a tím jsou potřebné informace sloužící jako podnět trestního řízení v době před zahájením trestního stíhání prakticky nedostupné.*“[168] Co se týče oznámení přímo od obyvatelstva, tak ta jsou, vzhledem k nedostatečným znalostem oznamovatele v oblasti kybernetické kriminality, nekonkrétní a obsahují jen velmi málo informací, a je poměrně těžké s nimi nadále pracovat.

Před zahájením trestního stíhání (prověřování)

Na základě vlastních poznatků, trestních oznámení či podnětů jiných osob je v souladu s § 158 TŘ třeba, aby policejní orgán zahájil úkony trestního řízení a sepsal o tom záznam. Je také možné postupovat v souladu s § 160 odst. 4 TŘ a provést neodkladné či neopakovatelné úkony, mezi něž patří například vydání a odnětí věci, ohledání místa činu nebo vyhledávání digitálních stop. V prvních fázích bude třeba využití veškerých dostupných sil a dostatečného množství prostředků, aby mohli vyšetřovatelé zasáhnout na co nejvíce místech najednou a využít tak moment překvapení.[169] Mezi počáteční úkony

---

[167] PORADA, Viktor a Jiří STRAUS. *Kriminalistika: (výzkum, pokroky, perspektivy)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013, s. 523. ISBN 978-80-7380-477-0.

[168] Ibid., s. 528–530.

[169] PORADA, Viktor a Jiří STRAUS. *Kriminalistika: (výzkum, pokroky, perspektivy)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013, s. 532. ISBN 978-80-7380-477-0.

patří „*(1) ohledání místa činu, (2) domovní prohlídka a prohlídka jiných prostor, (3) zajišťovací úkony pro počítačovou expertizu a vyhledávání počítačových stop a důkazů*.“[170]

Velmi často se stává, že podstatné informace a data požívají ochrany státem uznávaného tajemství. Ochranu utajovaných informací pak upravuje zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti. V těchto případech je vyšetřování zkomplikováno tím, že je nutné získat souhlas příslušného orgánu pro zajištění dat. V souladu s § 99 TŘ nesmí být svědek vyslechnut o okolnostech týkajících se utajovaných informací a každý, kdo se na daném vyšetřování podílí, musí být v souladu s § 51b TŘ poučen o utajovaných informacích.[171]

Jak již bylo zmiňováno v kapitole 3.3, je třeba již od začátku postupovat rychle a všechny důkazy, data a podstatné informace pečlivě zaznamenat, zachovat a zabránit jejich zničení a narušení jejich integrity. Podstatným krokem je identifikace počítačového systému a zjištění IP adresy i data a času připojení systému do sítě. „*Díky své jedinečnosti a unikátnosti je právě IP adresa jedním z klíčových identifikátorů sloužících k identifikaci pachatele kyberkriminality.*“[172] Vzhledem k přítomnosti sofistikovaných technologií je zpravidla potřeba přibrání odborníka či přímo konzultanta dle § 157 odst. 3 TŘ.[173]

---

[170] KONRÁD, Zdeněk et al. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování*. 2015, s. 351-352.

[171] „*Při výkonu prohlídky jiných prostor, pro jejíž nařízení byly splněny zákonné podmínky, lze jako věci důležité pro trestní řízení zajistit i výpočetní techniku a záznamová media, případně jejich kopie, i když existuje možnost, že zajištěné nosiče informací obsahují vedle záznamů o skutečnostech důležitých pro trestní řízení i informace o skutečnostech, které se netýkají probíhajícího trestního řízení a ke kterým se váže státem uložená nebo uznaná povinnost mlčenlivosti*. (…) *Je-li prohlídka jiných prostor (stejně jako domovní prohlídka) prováděna s cílem nalézt a zajistit předměty, které se mohou stát věcnými důkazy ve smyslu § 112 odst. 1 trestního řádu, a je-li tohoto cíle dosahováno postupem dle příslušných ustanovení trestního řádu, nelze považovat za nedovolené porušení povinnosti mlčenlivosti skutečnost, že nosiče informací obsahují i údaje pro probíhající trestní řízení nepodstatné a nepoužitelné, neboť tento cíl nebyl provedením prohlídky sledován, jedná se pouze o vedlejší produkt prohlídky, kterému nebylo možno zabránit, a nikoliv o záměrné získávání údajů chráněných povinností mlčenlivosti způsobem, který by byl v rozporu s předpisy upravujícími prolomení povinnosti mlčenlivosti*.“ In: Usnesení Ústavního soudu ze dne 28. 3. 2002, sp. zn. IV. ÚS 2/02 (U 11/25 SbNU 385).

[172] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z. s. p. o., 2016, s. 411. ISBN 978-80-88168-18-8.

[173] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 725–726. ISBN 978-80-7380-720-7.

Domovní prohlídka a prohlídka jiných prostor

Dle § 82 TŘ domovní prohlídku lze vykonat, je-li důvodné podezření, že v bytě nebo v jiné prostoře sloužící k bydlení nebo v prostorách k nim náležející (obydlí) je věc nebo osoba důležitá pro trestní řízení. Domovní prohlídka je „*vážným, ale ústavně předpokládaným zásahem do základního lidského práva na nedotknutelnost obydlí*“[174] a dle čl. 12 LZPS je přípustná jen pro účely trestního řízení, a to na písemný odůvodněný příkaz soudce. Soudy je povolována pouze jako subsidiární prostředek.

Při domovní prohlídce je primárním cílem počítač a jeho software, ale je nutné najít i další zařízení, jako jsou mobilní telefony, tablety, pevné disky, switche, USB disky, CD a DVD, případně diskety, servery, datová úložiště a dnes poměrně populární síťová datová úložiště (NAS), herní konzole, tiskárny a televize. Osvědčily se i klasické metody, kdy je třeba hledat poznámkové bloky, papíry s poznámkami, telefonní diáře, dopisy a výpisy z účtu. Nejdůležitější je využít momentu překvapení, a předejít tak jakékoliv manipulaci podezřelého s technikou, a rovněž se na prohlídku dobře připravit a využít znalosti plánů daných prostor.[175]

Při domovní prohlídce[176] je s ohledem na možné provázání jednotlivých kybernetických útoků (typu phishing, pharming, spam a malware) „*vhodné specifikovat příkaz k domovní prohlídce (…) tak, aby bylo možné zajistit veškeré věci (…), které mohou s kybernetickou činností souviset (…). V případě, že by příkaz k prohlídce byl konkretizován pouze na prověřovanou věc, tedy na konkrétní kybernetický trestný čin (např. na zajištění věcí*

---

[174] ODEHNALOVÁ, Jana. Ústavnost domovní prohlídky a nedotknutelnost obydlí. *Právní rozhledy*. 2019, (8), 287–291.

[175] PORADA, Viktor a Jiří STRAUS. *Kriminalistika: (výzkum, pokroky, perspektivy)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013, s. 532–533. ISBN 978-80-7380-477-0.

[176] „*Neodkladnost a neopakovatelnost úkonu sice nebyly v příkazu soudu dostatečně podrobně odůvodněny, nicméně vyplývají z podstaty věci týkající se tzv. počítačové kriminality, kde je třeba vždy takový úkon z hlediska časových souvislostí jeho provedení vždy pečlivě naplánovat. Proto zmíněný formální nedostatek odůvodnění neodkladnosti a neopakovatelnosti tohoto úkonu sám o sobě nemůže znamenat nezákonnost domovní prohlídky a nepoužitelnost důkazů při ní opatřených. Zásah do softwarového či hardwarového vybavení počítače nebo úprava na něm uložených dat před tím, než by byl odborně zjištěn a zadokumentován jeho reálný stav, by znamenal zmaření objasňování skutečností závažných pro trestní stíhání. Toto závažné riziko dostatečně odůvodňuje kvalifikaci napadeného úkonu jako neodkladného a neopakovatelného*.“ In: Usnesení Nejvyššího soudu ze dne 15. 12. 2010, sp. zn. 5 Tdo 1312/2010.

souvisejících s porušováním práv autorských), pak by při nálezu dalších materiálů (např. dětské pornografie) bylo třeba tento příkaz rozšířit."[177]

Zajišťovací úkony

K zajišťovacím úkonům v oblasti kyberkriminality je třeba mít dostatečné technické vybavení a co nejvíce informací týkající se dané techniky. Zejména je nutné vědět výrobce počítačového systému a jeho konkrétní typ, na jakém operačním systému daný počítač běží, jaké se v něm nacházejí pevné disky a jaká je jejich kapacita, v jaké síti je zapojen a zda se v dané síti nacházejí i jiná zařízení a dále je potřeba vědět, jaké všechny programy a další softwarové nástroje se v daném počítači nacházejí. Všechny tyto aspekty analyzuje expert z oboru informačních technologií a je to právě on, kdo určí, jak se bude na místě postupovat. Mnohdy se spolupracuje s dalšími odborníky na konkrétní typ užitých technologií.[178]

K zajištění věcí pro důkazní účely patří také vydání a odnětí věci dle § 78 a § 79 TŘ. Typicky se bude jednat o počítač a veškeré jeho příslušenství a další zařízení již zmiňovaná výše (mobilní telefon, hard disk, USB disk, switch, NAS apod.). Některé věci ale mají specifickou povahu a je nutné k nim i specificky přistupovat. Co se týče dat, tak ty lze jako věc zajistit, a to bez ohledu na to, kde se fyzicky nacházejí. Stejně tak lze udělat zálohu nějakého obsahu (typicky se bude jednat o cloudové úložiště).[179]

Dne 1. února 2019 byl do TŘ přidán § 7b upravující urychlené uchování dat (angl. *data preservation*) z důvodu zajištění implementace čl. 16 a 29 Úmluvy o počítačové kriminalitě. Dle § 7b TŘ je předseda senátu a v přípravném řízení státní zástupce nebo policejní orgán oprávněn vydat příkaz osobě, která uvedená data drží nebo je má pod svojí kontrolou, k uchování dat v nezměněné podobě po stanovenou dobu, a to v případě, že je zapotřebí zabránit ztrátě, zničení nebo pozměnění dat důležitých pro trestní řízení, která jsou uložena v počítačovém systému nebo na nosiči informací. Dané ustanovení je ale formulováno poněkud nešťastně a dostává se do rozporu s úpravou odposlechu telekomunikačního provozu, kdy lze zpětně požadovat jen údaje o telekomunikačním

---

[177] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z. s. p. o., 2016, s. 428. ISBN 978-80-88168-18-8.

[178] PORADA, Viktor a Jiří STRAUS. *Kriminalistika: (výzkum, pokroky, perspektivy)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013, s. 533–535. ISBN 978-80-7380-477-0.

[179] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z.s.p.o., 2016, s.421–422. ISBN 978-80-88168-18-8.

provozu, nikoliv však obsah komunikace. Při užití daného ustanovení je ale možné získat „zamrazená“ data obsahující právě i obsah komunikace. Postupem dle tohoto paragrafu „*orgány činné v trestním řízení zcela obcházejí zákonnou úpravu získání dat telekomunikačního provozu a zneužívají institut součinnosti nepřípustným způsobem*.“[180]

Problematické je též zajišťování e-mailové korespondence, čemuž se v minulosti věnoval Nejvyšší soud[181] a také Nejvyšší státní zastupitelství ve svém výkladovém stanovisku[182]. Samotnou e-mailovou zprávu lze vyžádat podle § 78 TŘ, e-mailovou komunikaci uskutečněnou po zajištění datového nosiče lze zajistit v reálném čase, a to postupem dle § 88 TŘ a aktuální obsah e-mailové schránky je možné zjišťovat postupem dle § 158d odst. 3 TŘ.

Odposlech a záznam telekomunikačního provozu

Pro vyšetřování kybernetické kriminality je stěžejní institut odposlechu a záznamu telekomunikačního provozu. V první řadě je nutné vymezit pojem „telekomunikační provoz“, což tak činí zákon č. 127/2005 Sb., o elektronických komunikacích, dále i trestní zákoník, Úmluva o počítačové kriminalitě a trestní řád. Dle Dostála je ale třeba „*pojem telekomunikační provoz interpretovat tak, že zahrnuje vše chráněné tajemstvím dopravovaných zpráv dle čl. 13 Listiny, tedy elektronický přenos jakýchkoli neveřejných zpráv a záznamů mezi nějakými osobami*.“[183] Jen díky tomu je možné pod provoz podřadit i služby jako je Viber, WhatsApp či Messenger. Odposlech některých platforem komunikace (zejména WhatsApp) však v praxi naráží na nedostatek technických prostředků pro dešifrování zpráv. U určitých osob je dle § 97 zákona o elektronických komunikacích stanovena povinnost zřídit rozhraní, v rámci kterého by v dané

---

[180] TLAPÁK NAVRÁTILOVÁ, Jana a Ingrid GALOVCOVÁ. Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení? *Bulletin advokacie*. 2019, (11), 36–39.

[181] Usnesení Nejvyššího soudu ze dne 21. 5. 2009, sp. zn. 11 Tdo 349/2009.

[182] Stanovisko Nejvyššího státního zastupitelství ze dne 26. 1. 2015, sp. zn. 1 SL 760/2014, ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek.

[183] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – odposlech a údaje o komunikaci (2. díl). *Trestněprávní revue*. 2019, (4), 77–83.

komunikační síti bylo možno odposlouchávat i šifrované zprávy. Zrovna společnost WhatsApp mezi tyto osoby ale nepatří.[184]

Dle § 88 TŘ je možné zajistit obsah přenášených informací včetně provozních a lokalizačních údajů. Ačkoliv kybernetické trestné činy nesplňují podmínku stanovenou ve větě první § 88 odst. 1 a ani nejsou v daném paragrafu výslovně uvedeny, bude možné provádět odposlech, protože ke stíhání těchto činů zavazuje mezinárodní smlouva, v tomto případě Úmluva o počítačové kriminalitě a její dodatkový protokol. Tento paragraf umožňuje: *„(1) zajištění dat doposud neuskutečněné (budoucí, či probíhající) komunikace online, (2) zajištění obsahu budoucí e-mailové elektronické komunikace (online), (3) zjištění obsahu e-mailové elektronické komunikace v zajištěném datovém nosiči uskutečněné v době po jeho zajištění orgány činnými v trestním řízení (tzn. online).*“[185]

Dle § 88a TŘ je možné zajistit pouze údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat. Oproti § 88 TŘ není zjišťován obsah zpráv, ale jen provozní a lokalizační či další systémové údaje. Tyto údaje lze zjistit jak do minulosti, tak do budoucnosti.[186] Typicky budou zjišťovány údaje, jako je IP adresa (zda je statická či dynamická), MAC adresa, log přístupu do e-mailové schránky, k telefonní službě a na webové stránky a mnoho dalších údajů.[187] V rámci tohoto institutu neprovádí odposlech orgán Policie ČR, ale data musí vydat jejich příslušný držitel. Praxe často naráží na ustanovení § 97 odst. 3 zákona o elektronických komunikacích, ve kterém je stanovena šestiměsíční lhůta, po kterou musí právnické či fyzické osoby uchovávat provozní a lokalizační údaje.

---

[184] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – odposlech a údaje o komunikaci (2. díl). *Trestněprávní revue*. 2019, (4), 77–83.

[185] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z.s.p.o., 2016, s.437–442. ISBN 978-80-88168-18-8.

[186] Dostál zastává opačný názor, kdy lze zjišťovat údaje pouze do minulosti, a nikoliv i do budoucnosti, protože pokud mají nějaké údaje být vydány, logicky již musejí existovat. In: DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – odposlech a údaje o komunikaci (2. díl). *Trestněprávní revue*. 2019, (4), 77–83. Lze se přiklonit spíše k názoru Koloucha, který se opírá o jazykový výklad daného ustanovení a o vývoj dikce daného ustanovení. Dříve bylo v § 88a TŘ uvedeno „*o uskutečněném telekomunikačním provozu*“, nyní pouze „*o telekomunikačním provozu*“.

[187] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z.s.p.o., 2016, s.442–446. ISBN 978-80-88168-18-8.

V roce 2015 se Nejvyšší soud taktéž zabýval problematikou ustanovení § 88 a § 88a TŘ, a to hlavně z toho důvodu, že státní zástupci postupovali nekonzistentně při vydávání příkazů podle příslušných ustanovení a s ohledem na jejich novelizaci bylo třeba sjednotit výkladová stanoviska.[188] „*Nelze přisvědčit právnímu závěru, že text § 88a odst. 1 trestního řádu „údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat“ by bylo možné interpretovat i tak, že na základě § 88a odst. 1 trestního řádu by bylo možno navrhovat vydání soudního příkazu ke zjištění jiných, než provozních a lokalizačních údajů uchovávaných podle § 93 odst. 3, 4 ZEK, tj. i ke zjištění obsahu elektronické komunikace*.“[189] Pokud bude datový nosič již zajištěn (a příjemce tak nebude mít možnost se s komunikací seznámit) a bude třeba zjistit obsah elektronické komunikace, bude zapotřebí vydat soudní příkaz dle § 88 TŘ a jakékoliv návrhy na vydání soudního příkazu dle § 88a odst. 1 TŘ by bylo nutno považovat za nepřípustný extenzivní výklad daného ustanovení.[190] Oba dva instituty mají odlišnou genezi – § 88 slouží k ochraně tajemství dopravovaných zpráv a záznamů dle čl. 13 LZPS, zatímco § 88a vznikl v reakci na nařízené shromažďování dat. Ustanovení § 88a tak nelze vykládat na základě podobnosti s § 88. „*Zatímco u odposlechu a záznamu obsahu komunikace se zdá případným chápat nezbytnost povolení soudce dle § 88 co nejšířeji, u § 88a se naproti tomu jeví být nutnost jeho užití závislá na míře intenzity zásahu do soukromí, který je tím činěn*.“[191] Zásadní otázkou je, zda příslušná komunikace probíhá v reálném čase či nikoliv. Od toho se poté odvíjí, jaký institut bude použit. „*Příkaz k odposlechu a záznamu může nařizovat výhradně zajištění obsahu komunikačního provozu, který se teprve po jeho vydání soudem uskuteční. Nelze jej využít k získání obsahu zpráv a záznamů, jejichž přenos již proběhl*.“[192]

---

[188] Usnesení Nejvyššího soudu ze dne 21. 5. 2009, sp. zn. 11 Tdo 349/2009.

[189] Stanovisko Nejvyššího státního zastupitelství ze dne 26. 1. 2015, sp. zn. 1 SL 760/2014, ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek, s. 8.

[190] Ibid., s. 9.

[191] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – odposlech a údaje o komunikaci (2. díl). *Trestněprávní revue*. 2019, (4), 77–83.

[192] Ibid.

Ústavní soud se mimo jiné zabýval způsobem získání informací o IP adrese, které dle stěžovatele nebyly získány postupem v souladu s ustanovením § 88a TŘ. Dle ÚS lze údaje o IP adrese řadit mezi tzv. provozní a lokalizační údaje, ale i přesto nemusí být vždy při jejich získávání postupováno dle § 88a TŘ, „*neboť mezi jednu z podmínek aplikace tohoto ustanovení (...) náleží také podmínka tzv. subsidiarity, dle níž k využití tohoto institutu lze přistoupit, pokud sledovaného účelu nelze dosáhnout jinak nebo by jinak bylo jeho dosažení podstatně ztížené. Touto formulací zákon vyjadřuje soulad se zásadou přiměřenosti a zdrženlivosti vymezenou v ustanovení § 2 odst. 4 trestního řádu, shodně jako u odposlechu a záznamu telekomunikačního provozu (...). Požadované údaje orgány činné v trestním řízení získaly jiným legálním způsobem*“[193] a k užití § 88a TŘ nebyl dán důvod. ÚS se vyjádřil v tom směru, „*že bylo naopak správně, že [orgán činný v trestním řízení] postupoval pouhou žádostí, jakožto instrumentem (oproti v § 88a) zdrženlivějším*.“[194]

Operativně pátrací prostředky

Pro oblast kyberkriminality je významný zejména § 158d odst. 3 TŘ (sledování osob a věcí), který umožňuje zjistit obsah již uskutečněné e-mailové komunikace.[195] Je možné zajistit „*zprávy, které se aktuálně v e-mailové schránce nacházejí, jsou odeslané, odstraněné (nikoli permanentně), rozepsané, přijaté (doručené). (...) Analogicky je možné využít toto ustanovení i na kontakty, službu kalendář aj., pokud je uživateli ponechána možnost objektivní správy svého úču.*“[196] V rámci kyberkriminality lze využít i § 158e TŘ a použít agenta, který se může například infiltrovat do sítě dark web a odhalovat tam probíhající trestnou činnost.

---

[193] Usnesení Ústavního soudu ze dne 15. 2. 2017, sp. zn. II. ÚS 4211/16.

[194] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – odposlech a údaje o komunikaci (2. díl). *Trestněprávní revue*. 2019, (4), 77–83.

[195] Usnesení Ústavního soudu ze dne 3. 10. 2013, sp. zn. III. ÚS 3812/2012 (U 10/71 SbNU 573).

[196] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z. s. p. o., 2016, s. 448. ISBN 978-80-88168-18-8.

Součinnost státních orgánů, fyzických a právnických osob

Pro usnadnění průběhu trestního řízení a jeho urychlení je v rámci § 8 odst. 1 TŘ umožněno dožádání. Typicky bude využíváno směrem k ISP, ke zjištění všech aspektů IP adresy, e-mailové služby, webových stránek či chatu. V rámci tohoto institutu však nelze zjistit provozní a lokalizační či obsahové údaje a je třeba využít právě § 88 či § 88a TŘ.

Znalecký posudek

Při vyšetřování kybernetické kriminality mají soudní znalci a znalecké posudky nezastupitelnou úlohu. Jejich činnost se řídí zákonem č. 36/1967 Sb., o znalcích a tlumočnících, a také vyhláškou č. 37/1967 Sb., k provedení zákona o znalcích a tlumočnících. „*Znalecký posudek je samostatným důkazním prostředkem, kterým si orgány činné v trestním řízení nebo strany (...) opatřují od osob nebo orgánů k tomu zvláště odborně způsobilých – znalců odborné skutkové poznatky. Znalce je třeba přibrat i tehdy, jestliže pro složitost posuzované otázky není postačující vyžádat odborné vyjádření*.“[197]

Znalci budou zpravidla vybíráni z oboru kybernetika, odvětví výpočetní technika, souběžně s nimi pak mohou být jmenováni znalci z oboru elektronika či kriminalistika. „*Problémem je, když se vyžaduje zodpovězení otázek víceoborovou kvalifikací znalce. Tak například odpověď na otázky, jaký software se v počítači nachází a jaká by byla odměna, která by byla obvyklá za získání takové licence v době neoprávněného nakládání s dílem (...) požaduje, aby znalec měl přinejmenším kvalifikaci v oboru kybernetika, odvětví výpočetní technika, ale rovněž v oboru ekonomika – odvětví ceny a odhady*.“[198]

Při znaleckém zkoumání v oblasti kybernetické kriminality se poměrně často objevují různé chyby a problémy. Jedná se například o nedostatečnou kvalifikaci znalce, nedostatek informací o technologiích, nedostatečné programové vybavení, špatné

---

[197] FENYK, Jaroslav, Tomáš GŘIVNA a Dagmar CÍSAŘOVÁ. *Trestní právo procesní*. 6. Praha: Wolters Kluwer, 2015, s. 384. ISBN 978-80-7478-750-8.

[198] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 733. ISBN 978-80-7380-720-7.

interpretace dat či prodleva při přivolání znalce, kdy v mezidobí mohlo dojít ke smazání relevantních informací.[199] Dotazy směřované na znalce mohou mít například tuto podobu:

1) „*Proveďte základní popis a výpis hardwarové konfigurace zkoumaného počítačového systému.*
2) *Zadokumentujte veškerou nalezenou e-mailovou komunikaci, proveďte export veškerých zpráv.*
3) *Zadokumentujte historii navštívených webových stránek v internetových prohlížečích včetně k tomuto připojených dat.*
4) *Vyjádřete se k zabezpečení počítačového systému ohledně možného průniku z vnějšku. Popište, jestli zajištěný počítačový systém jevil stopy po takovémto proniknutí, jaké mohly mít následky, či s jakým cílem bylo do tohoto systému proniknuto.*“[200]

Znalecký posudek hraje velmi významnou roli v trestním řízení a znalecké závěry jsou prostředníkem mezi zajištěnými důkazy a dokazováním před soudem. Klíčové je vybrat znalce ze správného oboru a dostatečně přesně a jasně mu položit takové otázky, které umožní prokázat vinu obviněného.

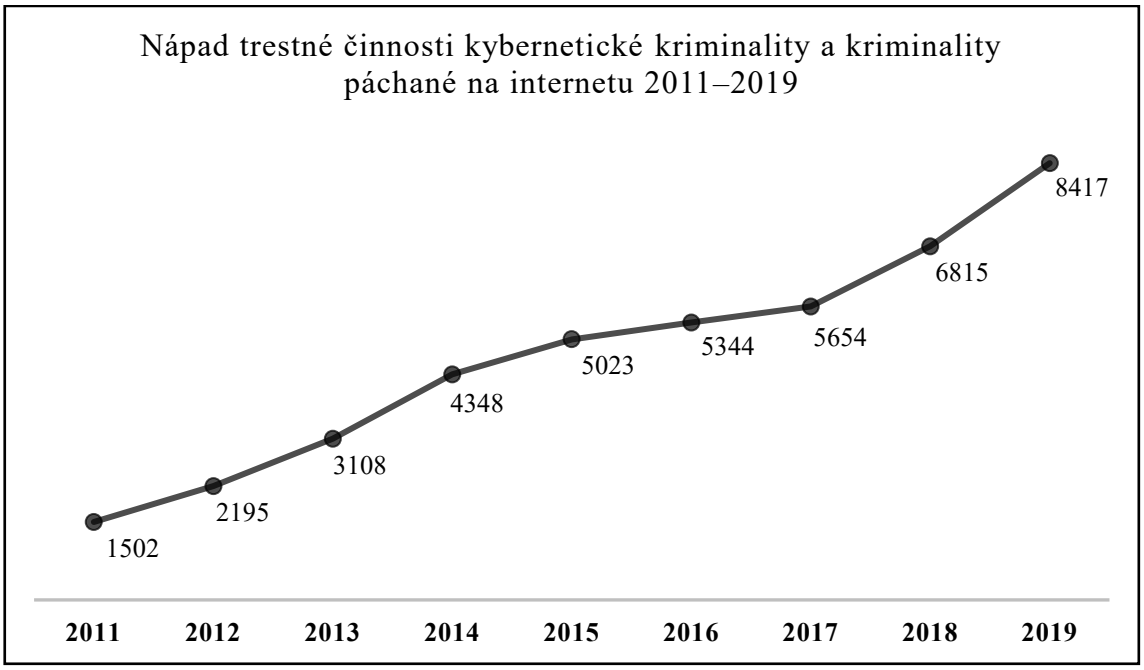
---

[199] Ibid., s. 744.

[200] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z.s.p.o., 2016, s.453–455. ISBN 978-80-88168-18-8.

5. SOUČASNÁ ČESKÁ PRÁVNÍ ÚPRAVA

Současná česká právní úprava vychází z implementace Úmluvy o počítačové kriminalitě. V roce 2019 bylo spácháno 8 417 trestných činů v oblasti kyberkriminality. Největší podíl představují podvodná jednání, zároveň roste počet případů hackingu (celkem 930 skutků). „*Zajímavý je také vysoký nárůst trestné činnosti spojené s neoprávněným provozováním hazardní hry ve virtuálním prostředí. Významné zastoupení má stále mravnostní kriminalita (777 skutků), kde znepokojivě roste počet pachatelů do 18 let věku v poměru ke zletilým pachatelům. Pachatelů do věku 18 let je u mravnostních trestných činů více, než v ostatních druzích kybernetické kriminality dohromady*.“[201]



Graf 1 Nápad trestné činnosti kybernetické kriminality a kriminality páchané na internetu 2011–2019[202]

V letech 1993–1997 byla počítačová kriminalita mnohem nižší. „*Pro ilustraci lze uvést přehled o počtu zjištěných trestných činů zahrnutých pod pojem počítačová kriminalita na území ČR*:“[203]

---

[201] POLICIE ČR. Kyberkriminalita. *Policie.cz* [online]. [vid. 2020-02-05]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx?q=cHJuPTE%3d

[202] Ibid.

[203] PORADA, Viktor a Zdeněk KONRÁD. *Metodika vyšetřování počítačové kriminality*. Praha: Policejní akademie České republiky, 1998, s. 8. ISBN 978-80-85981-75-9.

Tabulka 3 Počet zjištěných trestných činů zahrnutých pod pojem počítačová kriminalita v letech 1993-1997[204]

Rok	**1993**	**1994**	**1995**	**1996**	**1997**
Poškození a zneužití záznamu na nosiči informací § 257a TZ	12	4	10	14	9
Porušování předpisů o nakládání s kontrolovaným zbožím a technologiemi § 124c odst. 2 TZ	0	0	0	1	0
Zkreslování údajů hospodářské a obchodní evidence § 125 odst. 2 TZ	24	22	23	22	28
Provozování nepoctivých her a sázek § 250a TZ	221	31	11	8	2

Lze pozorovat, že v letech 1993–1997 bylo velmi malé množství trestných činů, které by bylo možné zařadit pod počítačovou kriminalitu. Až na výjimku v roce 1993, kdy bylo zjištěno 221 trestných činů provozování nepoctivých her a sázek, se každý rok vyskytlo průměrně 46 trestných činů.

Skutkové podstaty lze rozdělit dle několika kritérií. Prvním kritériem je charakter páchání trestné činnosti, dle kterého se skutkové podstaty dělí do pěti skupin (zásahy do počítačového systému a dat; šíření závadného obsahu; porušení autorských práv a práv souvisejících s právem autorským; nakládání se zařízením k páchání kybernetické trestné činnosti; kybernetické pronásledování).[205] Druhým kritériem je dělení podle toho, zda se jedná o trestné činy, při jejichž páchání představují prostředky ICT předmět ochrany (tedy jsou terčem útoku), nebo o trestné činy, při jejichž páchání jsou ICT použity k spáchání trestného činu.

[204] Ibid.

[205] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo*. 2010, (7–8), 19–43.

Tabulka 4 Dělení skutkových podstat do pěti skupin

Zásahy do počítačového systému a dat	**Šíření závadného obsahu**	**Porušení autorských práv a práv souvisejících s právem autorským**	**Nakládání se zařízením k páchání kybernetické trestné činnosti**	**Kybernetické pronásledování**
§ 180	*§ 191*	**§ 270**	*§ 231*	*§ 354*
§ 182 | **§ 182**	*§ 192*		**§ 234**	
§ 183	*§ 355*		*§ 236*	
§ 230 | **§ 230**	*§ 356*		*§ 348*	
§ 232	*§ 403*			
§ 311	*§ 407*			
	§ 184			
	§ 345			
	§ 287			

Legenda**:** Kurzívou vyznačeny – *prostředky ICT jako prostředek ke spáchání trestného činu*; tučně vyznačeny – **prostředky ICT jako terč útoku**

Skutkové podstaty je také možné rozdělit v souladu s rozdělením v Úmluvě o počítačové kriminalitě: trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systému; trestné činy související s počítačem; trestné činy související s obsahem; trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským. V dalších kapitolách jsou skutkové podstaty kybernetických trestných činů řazeny podle systematiky TZ a zároveň dle četnosti. Přehledná tabulka se všemi trestnými činy se nachází v Příloze 2.

5.1 Trestné činy proti majetku

5.1.1 Podvod (§ 209 TZ)

Jak již bylo zmíněno výše, podvodná jednání patří mezi nejčastější formu páchání kybernetické kriminality. Jedná se o typický příklad toho, kdy je zařízení ICT užito jako nástroj pro páchání trestné činnosti. Objektem skutkové podstaty je ochrana majetkových práv bez ohledu na druh a formu vlastnictví. Objektivní stránka spočívá v jednání pachatele, který se obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti. Pachatelem může být kterákoli fyzická či právnická osoba, tedy subjekt je obecný a z hlediska subjektivní stránky je třeba úmyslného zavinění.[206]

Vzhledem k pochybnostem vyskytujícím se v praxi v souvislosti se zásahy do počítačových a dalších technických zařízení bylo v trestním zákoníku toto jednání upřesněno v § 120, který stanoví, že uvést někoho v omyl či využít něčího omylu lze i provedením zásahu do počítačových informací nebo dat, zásahu do programového vybavení počítače nebo provedením jiné operace na počítači, zásahu do elektronického nebo jiného technického zařízení, včetně zásahu do předmětů sloužících k ovládání takového zařízení, anebo využitím takové operace či takového zásahu provedeného jiným. Zvláště významné jsou předměty sloužící k ovládání takového zařízení, pod nimiž si lze představit ovladače (tzv. drivery), které umožňují provedení útoků, jako je keylogger, a také instalaci různých špionážních programů zaznamenávajících údery na klávesnici uživatele.[207]

Podvodné jednání bude nejčastěji naplněno útoky, jako je phishing a pharming, ale velmi často se bude jednat o kombinace různých útoků. Phishingové útoky nejčastěji míří do oblasti internetového bankovnictví, kdy jsou rozesílané podvodné e-maily, které se snaží získat od uživatelů přihlašovací údaje do internetového bankovnictví případně do účtů různých internetových poskytovatelů finančních služeb, jako je dnes velmi populární PayPal. Uživatelé mají velmi často uložené své platební metody na e-shopech, takže se

---

[206] ŠÁMAL, Pavel. § 209 [Podvod]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2051–2052. ISBN 978-80-7400-428-5.

[207] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 194. ISBN 978-80-7380-720-7.

podvodníci snaží vylákat i přihlašovací údaje do internetových obchodů, jako je eBay, Amazon, ale i mnoho dalších.

Podvodné jednání se velmi často vyskytuje na internetových obchodech, jako je Bazoš či Aukro, kdy pachatel nabízí zboží, požaduje platbu předem na účet, ale zboží nikdy nehodlá reálně odeslat. Existují i podvodné e-shopy[208], podvodné loterie nebo podvodné lákání peněz prostřednictvím falešných faktur. V dnešní době se velmi často objevují podvody související s mobilními platbami. Asi nejznámějším případem je vylákání zaslaného autorizačního kódu k provedení platby. Pachatel poté oběti zavolá a pod nějakou záminkou, zpravidla účasti v soutěži, chce zjistit daný kód. Pomocí něj autorizuje platbu z účtu dané osoby.[209]

5.1.2 Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ)

§ 230 odstavec 1

V tomto odstavci je chráněna důvěrnost počítačových dat a počítačového systému a objektem je ochrana před neoprávněným vniknutím do počítačového systému. Integrita a dostupnost počítačových dat a systémů je chráněna až sekundárně.[210] Pachatel musí překonat bezpečnostní opatření a zároveň s tím získat neoprávněný přístup k počítačovému systému.

Bezpečnostní opatření je „*jakékoli opatření, které slouží k zabránění volného přístupu k počítačovému systému*.“[211] Nejčastěji se bude jednat o překonání hesla, které může pachatel snadno uhodnout nebo k prolomení užije nějaký softwarový či hardwarový nástroj. Důležité je, že dané bezpečnostní opatření nemusí být nijak složité (např. je heslo někde poblíž napsáno na papírku nebo je užíváno snadné heslo jako *admin*, či *1234*),

---

[208] Seznam podvodných e-shopů vede a pravidelně aktualizuje Česká obchodní inspekce In: Rizikové e-shopy. *Česká obchodní inspekce* [online]. [vid. 2020-04-03]. Dostupné z: https://www.coi.cz/pro-spotrebitele/rizikove-e-shopy/

[209] POLICIE ČR. Pozor na podvodníky! *Policie.cz* [online]. [vid. 2020-04-03]. Dostupné z: https://www.policie.cz/clanek/pozor-na-podvodniky-346746.aspx

[210] GŘIVNA, Tomáš. § 230 [Neoprávněný přístup k počítačovému systému a nosiči informací]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2304 ISBN 978-80-7400-428-5.

[211] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z. s. p. o., 2016, s. 345. ISBN 978-80-88168-18-8.

aby došlo k naplnění této skutkové podstaty. Jde pouze o překonání překážky. Získání přístupu znamená zjednání volné dispozice s daným systémem a s jeho obsahem, kdy tento přístup musí být neoprávněný (v rozporu s právem) a lze tak učinit i na dálku. Pro subjekt nejsou stanoveny žádné zvláštní požadavky a je tedy obecný a z hlediska subjektivní stránky trestného činu je vyžadován úmysl.[212]

V mnohých případech je tato činnost páchána s pouhým cílem samotného překonání bezpečnostního opatření. Typicky se bude jednat o nováčky, kteří si zkouší a testují své hackerské znalosti, anebo nějaké vysloužilé hackery, jejichž cílem je pouhé splnění výzvy a pohlazení ega.

Problematickým aspektem tohoto ustanovení se může jevit to, že nezahrnuje takové získání neoprávněného přístupu, při kterém nedochází k překonání nějakého bezpečnostního opatření.[213] Může se jednat například o využití nepozornosti daného uživatele. V těchto případech ale postačí uplatnění odpovědnosti podle jiného právního předpisu – typicky podle zákona č. 89/2012 Sb., občanský zákoník.[214]

V roce 2017 se Krajský soud v Praze zabýval případem, kdy se obžalovaný několikrát připojil do internetového bankovnictví poškozené a převedl si na svůj účet tři tisíce korun, následně účet opakovaným zadáváním špatného hesla zablokoval. Obžalovaný znal přihlašovací údaje včetně hesla k účtu poškozené, a proto se soud zabýval oprávněností přístupu obžalovaného do internetového bankovnictví. „*Byť je státní zástupce shodného názoru jako okresní soud ohledně primárního postihu jednání, na něž dopadá ustanovení § 230 trestního zákoníku, tj. především na sofistikované hackerské útoky, přesto je třeba konstatovat, že stejně tak musí být postihováno i jednání, kdy pachatel využije předchozí znalosti přihlašovacích údajů do internetového bankovnictví, a bez vědomí a svolení jeho majitele získá pomocí těchto dat k němu přístup.*“[215]

---

[212] GŘIVNA, Tomáš. § 230 [Neoprávněný přístup k počítačovému systému a nosiči informací]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2307–2308. ISBN 978-80-7400-428-5.

[213] Článek 2 stanoví, že postačuje „*neoprávněný přístup k celému počítačovému systému nebo jeho jakékoli části*.“ In: Úmluva o počítačové kriminalitě. In: *Sbírka mezinárodních smluv České republiky*. 2013, částka 56, s. 10785-10837.

[214] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z.s.p.o., 2016, s.344–347. ISBN 978-80-88168-18-8.

[215] Usnesení Krajského soudu v Praze ze dne 29. 6. 2017, sp. zn. 9To 227/2017-379.

Útoky, které naplňují tuto skutkovou podstatu, se většinou označují jako hacking (resp. cracking) a patří sem prolamování hesel, keylogger, ale i phishing, pharming, sniffing, spoofing či phreaking.

§ 230 odstavec 2

V odstavci druhém tohoto ustanovení je chráněna integrita a dostupnost počítačových dat a systémů. K naplnění objektivní stránky skutkové podstaty musí dojít získáním přístupu k počítačovému systému nebo nosiči informací a zároveň naplněním jedné z dalších okolností alternativně uvedených pod písmeny a) až d). Pro subjekt nejsou stanoveny žádné zvláštní požadavky a je tedy obecný a z hlediska subjektivní stránky trestného činu je vyžadován úmysl. Oproti odstavci 1 se zde nově objevuje pojem nosič informací, který zahrnuje zařízení, jako jsou pevné disky, USB disky, CD, DVD nebo mobilní telefony. Není podstatné, jakým způsobem pachatel získal přístup k danému systému – zda neoprávněně, či zda legálním způsobem (může znát heslo, systém nemusí být zaheslovaný apod.).[216]

V písm. a) je nutné, aby pachatel neoprávněně užil data, která jsou v daném systému nebo na daném nosiči uložená. Takové jednání je nazýváno počítačová špionáž. V písm. b) musí dojít k vymazání, zničení, poškození, změně, potlačení či snížení kvality dat nebo k tomu, že jsou data učiněna neupotřebitelná. Hmotným předmětem útoku jsou hlavně data, která jsou v daném systému uložená. Takové jednání se dá označit jako počítačová sabotáž. Tato skutková podstata bude nejčastěji naplněna použitím malwaru.[217] Skutková podstata uvedená v § 230 odst. 2 písm. c) spočívá v padělání nebo pozměnění dat, která jsou uložená v počítačovém systému nebo na nosiči dat. „*Jde o obdobu padělání listin (nejen veřejných). Vychází se z myšlenky, že stále více informací má dnes elektronickou podobu, a proto je zapotřebí chránit je před paděláním. Zatímco padělaná listina je mnohdy rozeznatelná od originální, při změně dat není padělání zjevné. O to je nebezpečnější*.“[218] V písm. d) se jedná o neoprávněné vložení dat nebo

---

[216] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 569. ISBN 978-80-7380-720-7.

[217] GŘIVNA, Tomáš. § 230 [Neoprávněný přístup k počítačovému systému a nosiči informací]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2309. ISBN 978-80-7400-428-5.

[218] Ibid., s. 2311.

učinění jiného zásahu do programového nebo technického vybavení počítače. Jde o další případ počítačové sabotáže, kdy dojde k ochromení činnosti počítače, zablokování funkce programů nebo přístupu k datům. V § 230 odst. 3 písm. b) se vyskytuje kvalifikovaná skutková podstata, která obsahuje okolnost zvláště přitěžující.[219]

Ačkoliv trestní zákoník se na většině míst již přiklonil k užití pojmu data, pojem „nosič informací“ je nadále užíván namísto termínu „nosič dat“. Data jsou obsahově užší než informace a až složením většího množství dat vzniká informace, která může být komunikována lidem a zároveň je jimi i pochopena. Nosič informací slouží k zaznamenání dat a k jejich následnému přečtení. Nejčastěji jím bývá pevný disk, USB flash disk či mobilní telefon. V minulosti byla hojně užívaná i CD, DVD a diskety.[220]

5.1.3 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ)

V ustanovení § 231 TZ je chráněna společnost a osoby „*před možným ohrožením vyplývajícím z nekontrolovaného opatření a přechovávání zařízení, nástrojů a prostředků, jež primárně slouží ke spáchání trestných činů porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2*.“[221] Na rozdíl od § 230 TZ v tomto případě postačí jakékoliv opatření či přechování prostředků, kterým lze spáchat trestné činy podle § 182 a § 230 TZ, svým způsobem se jedná o přípravu nástrojů k páchání trestné činnosti.[222]

Pro subjekt nejsou stanoveny žádné zvláštní požadavky a je tedy obecný a z hlediska subjektivní stránky trestného činu je vyžadován úmysl. Pojem „přechovávání“ uvedený v § 231 odst. 1) TZ je třeba vykládat stejně, jako je tomu u § 192 TZ (výroba a jiné

---

[219] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z. s. p. o., 2016, s. 357. ISBN 978-80-88168-18-8.

[220] GŘIVNA, Tomáš. § 230 [Neoprávněný přístup k počítačovému systému a nosiči informací]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2303 a 2308. ISBN 978-80-7400-428-5.

[221] GŘIVNA, Tomáš. § 231 [Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2317. ISBN 978-80-7400-428-5.

[222] SOKOL, Tomáš a Vladimír SMEJKAL. Postih počítačové kriminality podle nového trestního zákoníku. *Právní rádce*. 2009, XVII (7).

nakládání s dětskou pornografií) a postačí, aby měl pachatel nástroj ve své moci – postačuje i uložení v cloudovém úložišti. Prostředky páchání trestné činnosti jsou rozděleny do dvou skupin: § 231 odst. 1) písm. a) by se dal souhrnně označit jako hardware a software a § 231 odst. 1) písm. b) představuje hesla, kódy a data.[223]

5.1.4 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZ)

Ustanovení § 232 TZ bylo nad rámec Úmluvy o počítačové kriminalitě zařazeno do našeho trestního zákoníku na základě požadavků praxe. „*Objektem trestného činu podle § 232 je ochrana dat a technického či programového vybavení počítače (jiného technického zařízení pro zpracování dat) před nedbalostním poškozovacím jednáním, pokud je těmito zásahy způsobena značná škoda*.“[224] Pachatel musí jednat z hrubé nedbalosti, musí porušit povinnost vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté, a na cizím majetku musí způsobit značnou škodu. Ve většině případů se bude jednat o obecnou povinnost opatrovat nebo spravovat majetek, která je blíže upravena pracovní smlouvou případně vnitřním předpisem zaměstnavatele. „*Lze tedy dovodit, že připojením zařízení, které si zaměstnanec donese v rámci momentálně módního trendu BYOD*[225]*, k počítači zaměstnavatele bez jeho souhlasu, čímž způsobí značnou škodu, by právě došlo k naplnění skutkové podstaty podle § 232 odst. 1*.“[226]

---

[223] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 582. ISBN 978-80-7380-720-7.

[224] GŘIVNA, Tomáš. § 232 [Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2322. ISBN 978-80-7400-428-5.

[225] BYOD – Bring Your Own Device je současný trend, kdy si zaměstnanci nosí do práce vlastní zařízení, na kterém pracují. Tento trend může představovat riziko v podobě ohrožení vnitropodnikové sítě a citlivých informací.

[226] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 586–587. ISBN 978-80-7380-720-7.

5.2 Trestné činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství

Porušení tajemství dopravovaných zpráv (§ 182 TZ)

Ustanovení § 182 TZ má za cíl ochránit tajemství přepravovaných zpráv. Porušením tajemství je třeba rozumět „*jakoukoli činnost pachatele, která směřuje k neoprávněnému seznámení se s obsahem přepravované zásilky v podobě přepravované zprávy v síti elektronických komunikací nebo neveřejného přenosu počítačových dat*."[227] Zprávy doposud nedoručené či ty, které jsou pouze rozepsané a nikoliv odeslané, nejsou chráněny.

Co se týče kybernetické trestné činnosti, tak je relevantní zejména odst. 1 písm. b) a písm. c) ustanovení § 231 TZ. Dle písm. c) je chráněn neveřejný přenos dat, kdy se tento znak vztahuje pouze na způsob přenosu. „*Může tedy nastat případ, kdy bude neveřejně přenášena veřejně známá a dostupná informace, i v tomto případě by se pachatel dopustil, za splnění dalších podmínek uvedených v § 182 TZ, tohoto trestného činu*."[228] Je třeba upřesnit některé pojmy týkající se ustanovení § 182. Účastníkem je dle § 2 písm. a) zákona o elektronických komunikacích každý, kdo uzavřel s podnikatelem poskytujícím veřejně dostupné služby elektronických komunikací smlouvu na poskytování těchto služeb, a uživatelem je dle § 2 písm. b) každý, kdo využívá nebo žádá veřejně dostupnou službu elektronických komunikací. Dle Koloucha je problematické, že jsou dané pojmy vykládány takto restriktivně a dochází tak ke zúžení působnosti trestního zákoníku na zásah pouze v rámci veřejných poskytovatelů připojení. Dané ustanovení by potom nesloužilo k ochraně jiných subjektů, které provozují připojení, jako jsou například vysoké školy či různé podnikové sítě.[229]

Nejčastěji je tajemství dopravovaných zpráv porušováno státem (Policií ČR, BIS, Vojenským zpravodajstvím), a to v rámci provádění odposlechu a záznamu telekomunikačního provozu v souladu s § 88 a § 88a TŘ. S danou problematikou souvisí i uchovávání provozních a lokalizačních dat v souladu s § 97 zákona o elektronických

---

[227] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z. s. p. o., 2016, s. 351. ISBN 978-80-88168-18-8.

[228] Ibid., s. 352.

[229] Ibid., s. 350.

komunikacích a s ním souvisejícím prováděcím předpisem – vyhláškou č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů. Na úrovni EU byla v roce 2006 přijata směrnice Evropského parlamentu a Rady 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí (tzv. směrnice Data Retention), která byla ale v roce 2014 SDEU prohlášena za neplatnou z důvodu zvlášť závažného zásahu do základních práv zakotvených v článcích 7 a 8 LZPEU.[230]

Na vnitrostátní úrovni ale zůstala implementovaná právní úprava zachována, kdy lze tento „*stav plošného uchovávání provozních a lokalizačních údajů považovat sice za právně neudržitelný, leč nepřekvapivě udržovaný.*“[231] Této problematice se v roce 2019 věnoval i Ústavní soud[232], který shledal potřebnost této zákonné úpravy k objasnění kybernetické kriminality, kdy hromadné uchovávání formou data retention umožní rychlé a efektivní odhalování kybernetické kriminality. „*Dle jeho vysloveného názoru (bod 104 nálezu) sice plošné shromažďování data retention představuje zásah do soukromí osob, zůstává však otázkou, zda by při absenci principu data retention nedocházelo k využití jiných, invazivnějších metod k získání informací*.“[233]

S ustanovením § 182 TZ úzce souvisí i § 183 TZ, ve kterém je uveden trestný čin porušení tajemství listin a jiných dokumentů uchovávaných v soukromí. Dané ustanovení doplňuje ochranu zajišťovanou ustanovením § 182 TZ a rozšiřuje ji o listiny a jiné dokumenty uchovávané v soukromí. Objektem je „*listovní tajemství a tajemství jiných písemností*

---

[230] Rozsudek SDEU ze dne 8.4.2014, spojené věci C-293/12 a C-594/12 *Digital Rights Ireland a další*.

[231] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 326. ISBN 978-80-7380-720-7.

[232] Nález ÚS ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17.

[233] PŘÍKAZSKÁ, Lenka a Michal MOHELSKÝ. Současná právní úprava data retention je dle Ústavního soudu ústavně konformní a tedy přípustná. *EPRAVO.CZ* [online]. 2019 [vid. 2020-03-22]. Dostupné z: https://www.epravo.cz/top/clanky/soucasna-pravni-uprava-data-retention-je-dle-ustavniho-soudu-ustavne-konformni-a-tedy-pripustna-110069.html

uchovávaných v soukromí, zaručené čl. 13 LZPS.“[234] V obou ustanoveních nejsou žádné speciální požadavky na subjekt (je tedy obecný) a je vyžadováno úmyslné zavinění.

5.3 Trestné činy proti České republice, cizímu státu a mezinárodní organizaci

Teroristický útok (§ 311 (1) (a), § 311 (1) (e) TZ)

Tato právní úprava byla do našeho právního řádu implementována na základě zajištění souladu se směrnicí Evropského parlamentu a Rady 2017/541 o boji proti terorismu a je účinná až od 1. února 2019. Směrnice „*rozšiřuje chápání teroristického trestného činu o jednání spočívající v kybernetických útocích se specifickým teroristickým úmyslem*.“[235] Pachatel musí jednat v úmyslu poškodit ústavní zřízení nebo obranyschopnost České republiky, narušit nebo zničit základní politickou, hospodářskou nebo sociální strukturu České republiky nebo mezinárodní organizace, závažným způsobem zastrašit obyvatelstvo nebo protiprávně přinutit vládu nebo jiný orgán veřejné moci nebo mezinárodní organizaci, aby něco konala, opominula nebo trpěla. Jedná se o zvlášť závažný zločin, u něhož je trestná i příprava.

Je obtížné definovat, co je to terorismus, protože má mnoho různých projevů. Autoři Weston a Innes definovali určité společné znaky, které se objevují ve většině (ne-li dokonce ve všech) projevech terorismu. Jedná se o politické násilí, komunikativní násilí a asymetrii moci.[236] „*Při definování pojmu terorismus pro účely trestního práva musíme také dbát na subjektivní stránku činu. Musí tu být zvláště orientovaný úmysl pachatele a speciální pohnutka. Úmysl pachatelů při tomto druhu trestné činnosti zejména bývá vzbudit strach u široké veřejnosti, pocit úzkosti, bezmoci, ohrožení a za*

---

[234] ŠÁMAL, Pavel. § 183 [Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 1820. ISBN 978-80-7400-428-5.

[235] Důvodová zpráva k zákonu č. 287/2018 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony, č. 287/2018 Dz.

[236] MORGAN, Rodney, Robert REINER a Mike MAGUIRE, ed. *The Oxford handbook of criminology*. 5th ed. New York, NY: Oxford University Press, 2012, s. 662. ISBN 978-0-19-959027-8.

jejich pomoci vyvolat destabilizaci ústavního zřízení, politického, hospodářského zřízení státu, oslabení jeho obranyschopnosti, rozvrácení struktury soudnictví apod.“[237]

Odstavec 1 písm. a) nyní postihuje jednání spočívající ve zničení nebo poškození ve větší míře počítačového systému, na jehož fungování závisí zařízení, systém nebo plošina blíže specifikované v daném ustanovení, a to s cílem vydat majetek v nebezpečí škody velkého rozsahu.[238] Odstavec 1 písm. e) postihuje provedení (1) útoku proti počítačovému systému, jehož narušení by mělo závažný dopad na fungování státu, zdraví osob, bezpečnost, hospodářství nebo zajištění základních životních potřeb obyvatel, (2) útok s dopadem na větší počet počítačových systémů s využitím počítačového programu vytvořeného nebo přizpůsobeného pro takový útok a nebo (3) útok, kterým způsobí značnou škodu. Všechny tyto útoky musí být provedený jedním z následujících způsobů:

- vložení dat do počítačového systému nebo na nosič informací;
- vymazání či jiné zničení, poškození, změna nebo potlačení dat uložených v počítačovém systému nebo na nosiči informací;
- snížení kvality dat nebo učinění jich neupotřebitelnými.

Teroristické útoky v kyberprostoru jsou pak označovány jako kyberterorismus a jedná se o jednu z největších aktuálních hrozeb.

5.4 Trestné činy proti lidské důstojnosti v sexuální oblasti

Výroba a jiné nakládání s dětskou pornografií (§ 192 TZ)

Objektem tohoto trestného činu je ochrana mravního vývoje dětí a ochrana před jejich sexuálním zneužíváním. V odstavci 1 je kriminalizováno jednání pachatele spočívající v přechovávání dětské pornografie. S tím souvisí i odborná diskuze, zda „*toto ustanovení postihuje i držení tzv. virtuální dětské pornografie, tj. pornografie, kde je dítě vyobrazeno např. prostřednictvím animace. Vycházeje z objektu tohoto trestného činu, jak to činí teleologický výklad, kterým je ochrana dítěte před jeho zneužitím k výrobě pornografie,*

---

[237] FOJT, Dominik. Terorismus v rámci Evropské unie. *Trestněprávní revue*. 2020, (1), 28–33.

[238] Článek 3 odst. 1. písm. i) směrnice Evropského parlamentu a Rady 2017/541 o boji proti terorismu: „*neoprávněné zasahování do informačních systémů podle článku 4 směrnice Evropského parlamentu a Rady 2013/40/EU v případech, kdy se použije čl. 9 odst. 3 nebo čl. 9 odst. 4 písm. b) nebo c) uvedené směrnice, a neoprávněné zasahování do údajů podle článku 5 uvedené směrnice v případech, kdy se použije čl. 9 odst. 4 písm. c) uvedené směrnice*“.

lze dospět k závěru, že na tento druh pornografického zobrazení by se toto ustanovení vztahovat nemělo."[239] Stejně na to pohlíží i Herczeg, kdy opět vzhledem k objektu tohoto trestného činu „*jakákoliv fantazijní či virtuální dětská pornografie je mimo dosah toho ustanovení. (...) Virtuální dětská pornografie by totiž mohla být pro řadu pedofilů alternativou, která by jim umožnila realizovat své potřeby na úrovni masturbačních fantazií, a tím by se snížilo riziko, že své potřeby skutečně realizují.*"[240]

Částečně byl tento problém vyřešen, když byla do daného ustanovení přidána kontroverzní formulace „*(...) pornografické dílo, které zobrazuje nebo jinak využívá (...) osobu, jež se jeví být dítětem*". V kontextu článku 9 odst. 2 Úmluvy o počítačové kriminalitě[241] je třeba toto slovní spojení vykládat i tak, že dané pornografické dílo zobrazuje „*neexistující dítě, avšak realisticky znázorněné.*"[242] Vzhledem k tomu, že jsou dnes informační technologie velmi vyspělé a mnohdy může být virtuální pornografie nerozeznatelná od té reálné, je nasnadě, aby takové jednání bylo kriminalizováno.

Z hlediska kybernetické kriminality je nejvíce relevantní odstavec 2 tohoto ustanovení, který byl do našeho právního řádu implementován až novelou č. 141/2014 Sb. z důvodu nutnosti provedení článku 5 odst. 3 směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii.[243] Jednání pachatele spočívá v získání přístupu k dětské pornografii prostřednictvím informační nebo komunikační technologie. „*Trestný je tak již ten, kdo usedne k počítači a zadá v internetovém vyhledávači jakékoli klíčové slovo,*

---

[239] DRAŠTÍK, Antonín, Robert FREMR, Tomáš DURDÍK, Miroslav RŮŽIČKA, Alexander SOTOLÁŘ a ČESKO. *Trestní zákoník: komentář*. 2015, s. § 192. ISBN 978-80-7478-790-4.

[240] GŘIVNA, Tomáš. Trestné činy proti lidské důstojnosti v sexuální oblasti v novém trestním zákoníku. *Bulletin advokacie*. 2009, (10), 67–72.

[241] Článek 9 odst. 2 Úmluvy o počítačové kriminalitě stanoví, že pro účely výše uvedeného odstavce 1 „dětská pornografie" bude zahrnovat pornografický materiál, který vizuálně znázorňuje (…) c) realistické zobrazení představující nezletilou osobu, která se účastní sexuálně jednoznačného chování. In: Úmluva o počítačové kriminalitě. In: *Sbírka mezinárodních smluv České republiky*. 2013, částka 56, s. 10785-10837.

[242] Druhou možností je zobrazení osoby starší osmnácti let, která má však vzhled dítěte. In: GŘIVNA, Tomáš. § 192 [Výroba a jiné nakládání s dětskou pornografií]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2.vyd. Praha: C. H. Beck, 2012, s. 1891. ISBN 978-80-7400-428-5.

[243] Článek 5 odst. 3 směrnice zní: „*Vědomé získávání přístupu k dětské pornografii prostřednictvím informačních a komunikačních technologií se trestá odnětím svobody s horní hranicí trestní sazby nejméně jeden rok.*"

které mu umožní získat přístup k dětské pornografii (např. mladé školačky apod.), aniž by přístup k dětské pornografii skutečně získal. Jde tak vlastně o pokus, který je povýšen na dokonaný trestný čin (předčasně dokonaný trestný čin)."[244] Herczeg ve svém článku odkazuje na Musila, který upozorňuje na riziko takovéto trestněprávní úpravy. „*Takovou velmi problematickou tendencí (vedle zavádění abstraktních ohrožovacích deliktů) je tzv. předsunutí trestní odpovědnosti (v německé odborné literatuře označované jako „Vorverlagerung der strafrechtlichen Verantwortlichkeit", tj. kriminalizace takových jednání, která časově daleko předcházejí vlastnímu nebezpečnému jednání (pokusu nebo dokonání činu) a nezpůsobují žádný okamžitý škodlivý následek*."[245] Autor dále uvádí, že se v právní úpravě čím dál častěji objevují tzv. předčasně dokonané delikty (např. § 230 a § 231 TZ), které právě podporují trend předsunutí trestní odpovědnosti a mají v některých případech negativní důsledky. Typově se totiž jedná spíše o bagatelní delikty s nízkou společenskou závažností.[246]

Problematické jsou též situace, kdy uživatel při prohlížení internetu omylem narazí na stránky s dětskou pornografií, kdy se v rámci cookies souborů uloží data o dané webové stránce a jejím obsahu do vyrovnávací paměti počítače. Takové jednání nelze považovat za přechovávání. „*Sporné je, zda lze za přechovávání považovat případy, kdy bude uživatel cíleně a pravidelně prohlížet určité stránky s dětskou pornografií*."[247] Pak by zřejmě naplňoval skutkovou podstatu § 192 odst. 2 TZ, kdy uživatel získá přístup k dětské pornografii. Problematické je, jak rozlišit „*přístup náhodný a nevědomý od přístupu úmyslného*."[248] Takovou otázku vyřeší až judikatura.

V odstavci 4 daného ustanovení je problematický pojem „veřejně přístupná počítačová síť". Otázkou toho, zda pod daný pojem spadá i soukromá e-mailová korespondence mezi

---

[244] HERCZEG, Jiří. Několik poznámek k novele trestního zákona č. 141/2007 Sb. *Trestněprávní revue*. 2015, (7–8), 173–175.

[245] MUSIL, Jan. Přestává platit v českém trestním právu princip odpovědnosti za zavinění? *Trestněprávní revue*. 2014, (11–12), 251–255.

[246] Ibid.

[247] GŘIVNA, Tomáš. § 192 [Výroba a jiné nakládání s dětskou pornografií]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 1892. ISBN 978-80-7400-428-5.

[248] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 288. ISBN 978-80-7380-720-7.

uživateli, se zabýval i Nejvyšší soud. „*Rozesílání pornografických děl prostřednictvím elektronické pošty mezi tzv. e-mailovými schránkami, chráněnými individuálními přístupovými hesly, nenaplňuje znak „veřejně přístupná počítačová síť“ ve smyslu § 191 odst. 3 písm. b) a § 192 odst. 3 písm. b)*[249] *tr. zákoníku*.“[250] Stejnou otázkou se zabýval i Ústavní soud, který se vyjádřil i k většímu počtu adresátů: „*Jinak by tomu bylo, kdyby uživatel zveřejnil přístupové údaje k tzv. e-mailové schránce dalším osobám, nebo rozesílal datovou zprávu obsahující dětskou pornografii širšímu okruhu osob*.“[251] Nejvyšší soud ve svém rozhodnutí uvedl, že rozeslání pornografických děl např. 163 adresátům naplňuje znak „jiným obdobně účinným způsobem“ ve smyslu § 192 odst. 4 písm. b) TZ.

Existuje velké množství útoků naplňujících skutkovou podstatu tohoto trestného činu. Mimo jiné jde například o sexting. Zajímavým fenoménem dnešní doby je tzv. revenge porn, neboli nekonsensuální pornografie, což je „*zpřístupnění obrazového záznamu konkrétní osoby se sexuálním obsahem bez jejího souhlasu*“.[252]

Navazování nedovolených kontaktů s dítětem (§ 193b TZ)

Objektem tohoto trestného činu je ochrana zdravého mravního vývoje dětí a ochrana před jejich zneužíváním. Jedná se o trestný čin, který byl do naší právní úpravy implementován na základě čl. 6 odst. 1 směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii.[253] Naše úprava jde částečně nad rámec směrnice, neboť postihuje navazování nedovolených kontaktů s dítětem obecně a neomezuje se pouze na kontakty navazované prostřednictvím ICT.[254]

---

[249] Nyní se jedná o § 192 odst. 4 písm. b) TZ.

[250] Stanovisko NS ze dne 30. 1. 2013, sp. zn. Tpjn 300/2012, č. 3/2013 Sb. rozh. obč.

[251] Nález ÚS ze dne 20. 8. 2013, sp. zn. I. ÚS 1428/13 (N 150/70 SbNU 389).

[252] GARGULÁK, Michal. Kriminalizace nekonsensuální pornografie v České republice. *Trestněprávní revue*. 2018, (2), 30–35.

[253] Článek 6 odst. 1 směrnice zní: „*Členské státy přijmou opatření nezbytná k zajištění trestnosti tohoto úmyslného jednání: Navrhne-li dospělá osoba prostřednictvím informačních a komunikačních technologií setkání dítěti, které nedosáhlo věku pohlavní dospělosti, s cílem spáchat trestný čin uvedený v čl. 3 odst. 4 a čl. 5 odst. 6 a učiní-li po tomto návrhu konkrétní kroky vedoucí k tomuto setkání, trestá se tento návrh odnětím svobody s horní hranicí trestní sazby nejméně jeden rok.*“

[254] Důvodová zpráva k zákonu č. 141/2014 Sb., č. 141/2014 Dz.

Jednání pachatele spočívá v navrhnutí setkání dítěti mladšímu 15 let v úmyslu spáchat trestný čin pohlavní zneužití, výroba a jiné nakládání s dětskou pornografií, zneužití dítěte k výrobě pornografie, svádění k pohlavnímu styku či jiný sexuálně motivovaný trestný čin. Dle Koloucha je tato právní úprava nedostatečná a měla by zahrnovat i ochranu dětí mladších osmnácti let, stejně tak jako to činí § 192 a § 193 TZ, na které dané ustanovení odkazuje.[255] Typickým útokem naplňujícím tuto skutkovou podstatu je kybergrooming.

5.5 Trestné činy hospodářské

Neoprávněné opatření, padělání a pozměnění platebního prostředku (§ 234 TZ)

Objektem tohoto trestného činu je ochrana platebního prostředku, a to jak českého, tak i cizozemského, a zároveň ochrana řádného fungování celého zejména bezhotovostního platebního styku. Objektivní stránka spočívá v opatření, zpřístupnění, příjmu nebo přechovávání platebního prostředku jiného. Typickým platebním prostředkem je platební karta, dále elektronické peníze, příkaz k úhradě, inkasu, šeky, směnky, akreditivy a další. Objektivní stránka v odstavci 2 spočívá v opatření, zpřístupnění, příjmu nebo přechovávání padělaného platebního prostředku. V odstavci 3 pachatel buď padělá nebo pozmění platební prostředek v úmyslu použít jej jako pravý nebo platný, nebo padělaný nebo pozměněný platební prostředek použije jako pravý nebo platný.[256]

Z hlediska kybernetické kriminality je významné zejména ustanovení týkající se elektronických peněz, které mohou být snadno terčem útoku. Jejich definice je uvedená v § 4 zákona č. 370/2017 Sb., zákon o platebním styku. Elektronické peníze jsou peněžní hodnota, která a) představuje pohledávku vůči tomu, kdo ji vydal, b) je uchovávána elektronicky, c) je vydávána proti přijetí peněžních prostředků za účelem provádění platebních transakcí a d) je přijímána jinou osobou než tím, kdo ji vydal. Slouží zejména pro usnadnění platebního styku při užívání tzv. mikro plateb. Na evropské úrovni byla vydána směrnice[257], která blíže upravuje vydávání elektronických peněz.

---

[255] KOLOUCH, Jan. *CyberCrime*. 1. Praha: CZ.NIC, z. s. p. o., 2016, s. 371. ISBN 978-80-88168-18-8.

[256] ŠÁMAL, Pavel. § 234 [Neoprávněné opatření, padělání a pozměnění platebního prostředku]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2363–2365. ISBN 978-80-7400-428-5.

[257] Směrnice Evropského parlamentu a Rady 2009/110/ES ze dne 16. září 2009 o přístupu k činnosti institucí elektronických peněz, o jejím výkonu a o obezřetnostním dohledu nad touto činností.

Od elektronických peněz musíme rozlišovat kryptoměnu, což je digitální měna založená na principu blockchainu. Mezi nejznámější patří Bitcoin, Ethereum a EOS. Bitcoin je svobodná a decentralizovaná měna, která zajišťuje anonymitu a díky silnému šifrování i vysokou bezpečnost transakcí.

Dalším útokem naplňujícím tuto skutkovou podstatu je tzv. skimming. V současné době ale pomalu odpadá používání fyzických platebních karet a nahrazují je služby, jako je Apple Pay a Google Pay, kdy je platební karta nahrána do mobilního telefonu a pomocí něj jsou platby prováděny. Daná osoba vůbec nepotřebuje mít u sebe platební kartu. Tyto platby jsou mnohem bezpečnější, protože každá platba je šifrována a nelze ukrást platební údaje. Stejně tak je zvýšená bezpečnost díky identifikaci pomocí otisku prstu, skenu obličeje či zadání přístupového kódu.

Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270 TZ)

Dané ustanovení má za cíl ochránit „*vědeckou a literární, hudební, výtvarnou, audiovizuální a jinou uměleckou tvůrčí činnost a požitky z ní plynoucí, ale i práva výrobců zvukového záznamu a zvukově obrazového záznamu, dále práva rozhlasového a televizního vysílatele a práva pořizovatele databáze*.“[258] Objektivní stránka spočívá v nikoli nepatrném neoprávněném zásahu do zákonem chráněných práv. Právě pojem „nikoli nepatrný“ zásah je předmětem diskuzí. „*Je třeba zvažovat okolnosti konkrétního případu, především intenzitu takového zásahu, způsob provedení činu, jeho následky, zejména ve formě a závažnosti zasažení osobních a majetkových práv autorů (...). Bez významu není ani osoba pachatele, míra jeho zavinění, jeho pohnutka atd*. (…)“[259] Méně závažné případy budou postihovány jako přestupek či jiný správní delikt dle § 105a-105c autorského zákona.

Z hlediska subjektivní stránky je třeba úmyslného zavinění a úmysl se „*musí vztahovat na pachatelovo vědomí, že jde o dílo jako výsledek tvůrčí činnosti autora, jako duševní výtvor spočívající v individuálním ztvárnění myšlenky (...). Není však nutné, aby pachatel*

---

[258] ŠÁMAL, Pavel. § 270 [Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2737. ISBN 978-80-7400-428-5.

[259] Ibid., s. 2752.

znal přesný rozsah uvedených práv autora (...). Postačí, že pachatel si je alespoň v hrubých rysech vědom toho, že nakládá s dílem, výkonem výkonného umělce, zvukovým či obrazovým záznamem nebo rozhlasovým či televizním pořadem anebo databází, které jsou chráněny autorským právem."[260]

Jedná se o blanketní normu odkazující na zákon č. 121/2000 Sb., autorský zákon a případně i na další zákony, které tento zákon provádějí. V této oblasti je významná směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů. Právě počítačový program je totiž dle § 2 odst. 2 autorského zákona považován za dílo chráněné tímto zákonem.

Útoky naplňující tuto skutkovou podstatu jsou nejčastěji cracking, Warez, file hosting a internetové pirátství. Dalším druhem útoku je šíření díla prostřednictvím tzv. embedded linku. K této problematice se již několikrát vyjádřil Nejvyšší soud. „*Pokud jde o sdělování díla veřejnosti prostřednictvím internetu, je zde třeba rozlišovat mezi prostým odkazováním na tato díla (resp. jejich rozmnoženiny) na straně jedné a jejich zpřístupněním pomocí metody vloženého kódu (tzv. embeddingem) na straně druhé*." [261] V prvním případě jde o pouhé informování o existenci daného díla a jeho umístění, zatímco v případě embedded linku uživatel přímo zpřístupní obsah daného díla. Podle Nejvyššího soudu jde o přímý prostředek sdělování díla nebo jeho rozmnoženiny veřejnosti. Pokud je takové jednání činěno bez souhlasu autora díla, lze dovodit trestní odpovědnost za trestný čin podle § 270 TZ.[262] Obdobně rozhodl již dříve v roce 2013 Nejvyšší soud, kdy konstatoval, že „*za neoprávněný zásah do zákonem chráněných práv ve smyslu § 270 odst. 1 tr. zákoníku lze považovat i takové jednání pachatele, který na Internetu v prostoru vyhrazeném pro své internetové stránky umístí odkazy (tzv. embedded linky) umožňující neoprávněný přístup k rozmnoženinám děl (např. filmových a televizních) umístěných na externích serverech tak, že kdokoli k nim může mít prostřednictvím takové internetové stránky přístup, aniž by k tomu měl souhlas*

---

[260] Ibid., s. 2753.

[261] ŠELLENG, Dalibor. K některým aspektům trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 270 trestního zákoníku. *Acta MUP – Právní ochrana duševního vlastnictví*. 2018, (2), 37–45. ISSN 1804-6932.

[262] Usnesení Nejvyššího soudu ze dne 29. 5. 2013, sp. zn. 5 Tdo 271/2013.

nositelů autorských práv."[263] Vzhledem k tomu, že pachatel není vlastníkem rozmnoženiny díla, porušuje tak autorská práva ve smyslu § 18 odst. 1, 2 autorského zákona.

Otázce se věnuje i judikatura SDEU, kdy ve věci BestWater International SDEU s odkazem na dříve uveřejněné rozhodnutí v případě Svensson[264] konstatoval, že pouhá skutečnost, že chráněné dílo, volně dostupné na webové stránce, je vloženo na jinou webovou stránku pomocí tzv. framingu, nelze kvalifikovat jako „sdělování veřejnosti" ve smyslu čl. 3 odst. 1 směrnice Evropského parlamentu a Rady 2001/29/ES[265], pokud dané dílo není sdělováno nové veřejnosti a ke sdělování nedochází za použití specifické technologie, odlišné od technologie původního sdělování.[266]

V roce 2016 SDEU ve věci GS Media BV dospěl k závěru, že „*za účelem posouzení, zda umístění hypertextových odkazů na internetové stránce na chráněná díla, která jsou volně dostupná na jiné internetové stránce bez souhlasu nositele autorského práva, představuje „sdělování veřejnosti" ve smyslu [čl. 3 odst. 1 směrnice], je třeba určit, zda byly tyto odkazy poskytnuty nikoli za účelem dosažení zisku osobou, která nevěděla nebo nemohla rozumně vědět o protiprávní povaze zveřejnění těchto děl na této jiné internetové stránce, nebo zda naopak byly poskytnuty za účelem dosažení zisku, v kterémžto případě musí být taková znalost presumována*." [267]

V obou těchto případech soud rozhodoval primárně ohledně hypertextových odkazů, kdy se tato úprava vztahovala i na embedded linky. V dlouho očekávaném rozsudku v tzv. případu Cordoba SDEU navázal na předchozí dvě rozhodnutí s tím, že oblast tzv. embedded linku doznala změny. Hlavním rozdílem mezi hypertextovým odkazem a embedded linkem je dle SDEU to, že pokud primární zdroj odstraní dané autorské dílo, tak ani pomocí hypertextového odkazu umístěného na jiné webové stránce již nebude možné autorské dílo zobrazit. To ale neplatí u embedded linků, kdy zpřístupnění díla online na internetových stránkách vede „*k novému sdělení nezávislému na sdělení, ke*

---

[263] Usnesení Nejvyššího soudu ze dne 27. 2. 2013, sp. zn. 8 Tdo 137/2013.

[264] Rozsudek ze dne 13. 2. 2014, Nils Svensson a další, C-466/12.

[265] Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti.

[266] Usnesení ze dne 21. října 2014, BestWater International GmbH, C-348/13.

[267] Rozsudek ze dne 8. září 2016, GS Media BV, C-160/15.

kterému bylo původně uděleno svolení. V důsledku tohoto zpřístupnění online by takové dílo mohlo být nadále dostupné na posledně uvedených stránkách bez ohledu na předchozí svolení autora a navzdory jakémukoli jednání, kterým by se autor rozhodl již nesdělovat své dílo na internetových stránkách, na kterých bylo toto dílo prvotně sděleno s jeho svolením."[268]

SDEU tak nyní odlišuje mezi hypertextovým odkazem a embedded linkem, což pro běžného uživatele žádný rozdíl nepředstavuje. „*Internetové odkazy by neměly být regulovány a měly by i nadále fungovat jako základní stavební kámen internetu. Na druhou stranu není možné zavírat oči před zásadními rozdíly mezi prostým hyperlinkem a embedovaným odkazem a schovávat se v případě posouzení jejich autorskoprávních dopadů výhradně za technický způsob fungování. (...) Zatímco jednání uživatele, který stáhne na internetu veřejně dostupný a oprávněně zveřejněný obsah, tento nahraje na server a umístí jej na stránky, je dle SDEU sdělováním díla veřejnosti, postup, kdy uživatel nalezne na internetu stejný obsah a vloží jej na své stránky prostřednictvím embedovaného odkazu (čímž dosáhne fakticky stejného efektu), sdělováním díla veřejnosti není*."[269]

V dnešní době je velký rozmach streamovacích služeb v oblasti seriálů, filmů i hudby, jako je HBO GO, Netflix, Apple TV, Amazon Prime, Spotify, Apple Music a další platformy. Právě díky větší dostupnosti těchto služeb je možné, že naplňování skutkové podstaty § 270 TZ by mohlo být na ústupu.

---

[268] Rozsudek ze dne 7. srpna 2018, Land Nordrhein-Westfalen, C-161/17.

[269] KUKLINCA, Ján a Martin BARTOŇ. Embedovaný odkaz ve světle nové rozhodovací praxe. *EPRAVO.CZ* [online]. 2018 [vid. 2020-05-02]. Dostupné z: https://www.epravo.cz/top/clanky/embedovany-odkaz-ve-svetle-nove-rozhodovaci-praxe-108176.html

5.6 Trestné činy proti pořádku ve věcech veřejných

Nebezpečné pronásledování (§ 354 TZ)

Objektem tohoto trestného činu je „*ochrana nerušeného mezilidského soužití*“.[270] Objektivní stránka spočívá v dlouhodobém pronásledování jiného, které je prováděno v taxativně stanovených formách jednání, které jsou způsobilé v jiném vzbudit důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých. Z hlediska subjektivní stránky je třeba úmyslného zavinění a subjekt je obecný. Nebezpečné pronásledování je v zahraničí zpravidla označováno jako stalking.[271]

Kyberstalking je pak stalking prováděný v kyberprostoru, spočívající v zasílání nevyžádaných e-mailových zpráv, zpráv na Messengeru či Instagramu, komentování příspěvků s cílem oběť pomluvit či jinak poškodit, zasílání spamu, a také v cílených útocích na data oběti a jejich následném zneužití. Útočníci mohou využívat i diskuzní fóra, sociální sítě či jiné internetové platformy.[272] Dle Sýkory lze kyberstalking „*považovat za důmyslnější, nebezpečnější a pro oběť ponižující způsob pachatelova působení na pronásledovaného, tedy za formu výhodnější pro pachatele se závažnějšími dopady na oběť*.“[273] To je dáno zejména možností skrýt svou identitu, měnit ji nebo jich mít několik. Dále může útočník své útoky rafinovaně stupňovat a mnohem pravděpodobněji si troufne na slabší oběť. Vše ulehčuje snadná dostupnost prostředků, a tím i okamžitost útoků.[274]

„*Jak vyplývá i z pouhého textu zákona, bude jednání odpovídající cyberstalkingu podřaditelné zejména pod písmeno c) odstavce 1, odpovídající alternativně vytrvalému kontaktu prostřednictvím prostředků elektronických komunikací*.“[275] Na toto jednání se

---

[270] VÁLKOVÁ, Helena. § 354 [Nebezpečné pronásledování]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vyd. Praha: C. H. Beck, 2012, s. 3293. ISBN 978-80-7400-428-5.

[271] Ibid., s. 3292.

[272] KUCHTA, Josef. Aktuální problémy počítačové kriminality včetně její prevence. *Časopis pro právní vědu a praxi*. 2016, (1), 5–19.

[273] SÝKORA, Michal. Trestní postih cyberstalkingu. *Acta Universitatis Carolinae - Iuridica 4*. 2012, (4), 95–104. ISSN 0323-0619.

[274] Ibid.

[275] Ibid.

vztahují obecné znaky skutkové podstaty. Co se týče požadavku na dlouhodobost jednání, pak dle Vantucha by mělo jít o více než 10 pokusů o kontakt v období minimálně čtyř týdnů.[276] Období jednoho měsíce se objevuje i v komentářové literatuře s tím, že závažnost jednání spočívá právě v opakování a dlouhodobosti. „*Může jít o řadu vynucených kontaktů nebo pokusů o ně. (...) Ojedinělé nebo nahodilé projevy, byť jinak nežádoucího chování, tyto požadavky nesplňují*."[277] Vytrvalý kontakt, jako znak skutkové podstaty dle písmene c), lze pak chápat jako synonymum k dlouhodobosti a zřejmě je v daném ustanovení uveden nadbytečně.[278]

Dle Nejvyššího soudu se důvodnou obavou rozumí „*obava objektivně způsobilá vyvolat vyšší stupeň obav, úzkosti nebo jiného tísnivého pocitu ze zla, kterým je na poškozeného působeno, přičemž však není nutné, aby takový pocit v poškozeném skutečně vyvolala*."[279] Tato důvodná obava nemusí u oběti ani vzniknout, ale musí existovat možnost, že reálně vznikne. Proto je třeba hodnotit intenzitu a závažnost jednání, a odlišit tak nebezpečné pronásledování od méně závažných projevů.[280]

---

[276] VANTUCH, Pavel. K postihu stalkingu (nebezpečného pronásledování) podle § 354 trestního zákoníku. *Trestní právo*. 2011, (2), 5–13.

[277] DRAŠTÍK, Antonín, Robert FREMR, Tomáš DURDÍK, Miroslav RŮŽIČKA, Alexander SOTOLÁŘ a ČESKO. *Trestní zákoník: komentář*. 2015, s. § 354. ISBN 978-80-7478-790-4.

[278] SÝKORA, Michal. Trestní postih cyberstalkingu. *Acta Universitatis Carolinae - Iuridica 4*. 2012, (4), 95–104. ISSN 0323-0619.

[279] Usnesení NS ze dne 8. 9. 2011, sp. zn. 8 Tdo 1082/2011.

[280] VÁLKOVÁ, Helena. § 354 [Nebezpečné pronásledování]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vyd. Praha: C. H. Beck, 2012, s. 3298. ISBN 978-80-7400-428-5.

6. SOUČASNÉ TECHNOLOGICKÉ TRENDY

Velmi rychlý rozvoj technologií přináší mnoho výzev ve všech oblastech našeho života. Výjimkou není ani oblast trestního práva, která se nyní musí vypořádat s celou řadou otázek týkajících se nových technologií, jako je umělá inteligence, autonomní řízení vozidel, cloudová uložiště, virtuální měny a internet věcí. Vzhledem k turbulentnímu vývoji technologií je potřeba na nové trendy rychle a účinně reagovat, a zajistit tak účinné stíhání trestných činů v této oblasti. Současné technologické trendy nepochybně představují výzvu pro trestní právo.

6.1 Umělá inteligence

Umělá inteligence (angl. *Artificial Intelligence*, AI) je v současné době na obrovském vzestupu. Státy se předhánějí v tom, který z nich vytvoří účinnější a lepší systémy. Umělá inteligence se objevuje i v klíčových strukturách státu, jako je zdravotnictví, doprava či výroba. To vše představuje obrovský risk, protože jsou tyto systémy zranitelné a náchylné k sofistikovaným hackerským útokům. Podoblastí umělé inteligence je strojové učení (angl. *machine learning*) a také hluboké učení (angl. *deep learning*)[281]. Útočník může do systému vložit záměrně upravené vstupy (angl. *adversarial examples*), které jsou přímo vytvořeny tak, aby stroj udělal chybu. Stačí drobná změna obrazu a na satelitním snímku se pak nemocnice jeví jako vojenské letiště. Útočníci nepotřebují přístup ke vstupním datům ani k algoritmu systému.[282] V poslední době se rovněž začínají objevovat útoky, za kterými stojí umělá inteligence. I v tomto případě bude složité zjistit, kdo je za daný útok odpovědný. Nejčastěji se objevují botnety ovládané AI, které následně páchají DDoS útoky na servery.[283]

---

[281] Strojové učení je oblast umělé inteligence, která využívá algoritmy k tomu, aby se počítačový systém učil bez přímých instrukcí, a tím zefektivnil svou funkci. Hluboké učení stejně jako lidský mozek využívá neuronové sítě a dokáže analyzovat velké množství dat ve více vrstvách. S časem se algoritmus sám vylepšuje. Hluboké učení je využíváno v oblasti rozpoznávání řeči, obličeje, překladů textu a dalších oblastech.

[282] SCHARRE, Paul. Killer Apps. *Foreign Affairs* [online]. 2020 [vid. 2020-08-29]. ISSN 0015-7120. Dostupné z: https://www.foreignaffairs.com/articles/2019-04-16/killer-apps

[283] BOCETTA, Sam. Has an AI Cyber Attack Happened Yet? *InfoQ* [online]. 10. březen 2020 [vid. 2020-08-30]. Dostupné z: https://www.infoq.com/articles/ai-cyber-attacks/

Umělá inteligence je poměrně často využívána v oblasti tvorby autorských děl. Může fungovat jako specializovaný software, pomocí kterého je dílo přímo vytvářeno, nebo může být umělá inteligence integrovanou součástí interaktivní platformy. Zde je potřeba se zaměřit na otázku odpovědnosti umělé inteligence z hlediska trestněprávního. S tím souvisí otázka aplikace právní osobnosti na umělou inteligenci. Dle Zibnera „*je možné přiznat umělé inteligenci právní osobnost v rozsahu nutném pro přiznání autorství, čímž by se umělá inteligence v tomto rozsahu zařadila do kategorie jiných právnických osob, a byla tak nositelem autorství*."[284] V současné době však taková úprava není naším právním řádem předpokládána a na umělou inteligenci pohlížíme pouze jako na objekt právního vztahu. Subjektem odpovědnostního vztahu by pak byl vlastník umělé inteligence.[285]

Není úplně snadné definovat, co je to umělá inteligence. Mnoho autorů[286] se o to v minulosti pokoušelo, například Haugeland uvedl, že umělá inteligence je „*vzrušující nová snaha vedoucí k tomu, aby počítače přemýšlely*"[287], Night a Rich ji definovali jako „*studium toho, jak přinutit počítače dělat takové věci, ve kterých jsou v daný moment lidé lepší*".[288] Hallevy pak shrnuje, že systémy umělé inteligence jsou takové systémy, které (a) se chovají jako lidé, (b) myslí jako lidé, (c) uvažují racionálně a (d) chovají se racionálně.[289] Expertní skupina na umělou inteligenci přišla v roce 2019 s vlastní definicí umělé inteligence, která zní:

> „*Umělá inteligence (AI) označuje systémy, které zobrazují inteligentní chování tím, že analyzují jejich prostředí a provádějí akce – s určitou mírou autonomie – za účelem dosažení konkrétních cílů. Systémy založené na AI mohou*

---

[284] ZIBNER, Jan. Akceptace právní osobnosti v případě umělé inteligence. *Revue pro právo a technologie*. 2018, **9**(17), 19–49.

[285] ZIBNER, Jan. Otázky odpovědnosti umělé inteligence za zásah do autorského práva. *Revue pro právo a technologie*. 2019, **10**(20), 65–90.

[286] HALLEVY, Gabriel. *Liability for crimes involving artificial intelligence systems*. New York: Springer, 2014, s. 6–7. ISBN 978-3-319-10123-1.

[287] HAUGELAND, John. *Artificial intelligence: the very idea*. Cambridge, Mass: MIT Press, 1985, s. 2. ISBN 978-0-262-08153-5.

[288] RICH, Elaine, Kevin KNIGHT a Shivashankar NAIR B. *Artificial Intelligence*. 3. B.m.: Gardners Books, 2004, s. 3. ISBN 978-0-07-008770-5.

[289] HALLEVY, Gabriel. *Liability for crimes involving artificial intelligence systems*. New York: Springer, 2014, s. 7. ISBN 978-3-319-10123-1.

být založeny čistě na softwaru, fungující ve virtuálním světě (např. hlasoví asistenti, software pro analýzu obrazu, vyhledávače, systémy pro rozpoznávání řeči a obličeje), nebo může být AI zakomponovaná přímo v hardwaru (např. pokročilí roboti, autonomní automobily, drony, aplikace internetu věcí).“[290]

Hallevy uvádí tři odpovědnostní modely umělé inteligence. Prvním z nich je model odpovědnosti spáchané prostřednictvím jiného (angl. *The Perpetration-via-Another Liability Model*), druhým je model odpovědnosti s přirozenou pravděpodobností následku (angl. *The Natural-Probable-Consequence Liability Model*) a posledním je model přímé odpovědnosti (angl. *The Direct Liability Model*). Tyto tři modely mohou být aplikovány jak samostatně, tak i ve vzájemné kombinaci.[291]

Podle modelu odpovědnosti spáchané prostřednictvím jiného je umělá inteligence strojem, a nikoliv lidskou bytostí, a slouží pouze jako instrument pro spáchání trestného činu buď programátorem AI nebo uživatelem. Tento model nelze aplikovat v případě, že samotná AI se rozhodla spáchat trestný čin na základě jejího vlastního dosaženého poznání. Nicméně je vhodný pro případy, kdy programátor či uživatel využívá AI bez jejích pokročilých možností s tím, že za spáchání trestného činu je odpovědný právě programátor či uživatel.

Model s přirozenou pravděpodobností následku spočívá v tom, že programátor se podílí na každodenních aktivitách AI, ale nemá žádný úmysl spáchat trestný čin. Model předpokládá dva různé scénáře. V prvním z nich se programátor (resp. uživatel) dopustil nedbalosti, ale neměl žádné kriminální záměry spáchat jakýkoliv trestný čin. V tomto případě se jedná o čistou nedbalost. V druhé situaci programátor (resp. uživatel) naprogramoval či použil AI vědomě a záměrně za účelem spáchání trestného činu, ale AI sama spáchala jiný trestný čin. Příkladem může být situace, kdy AI byla naprogramována pro spáchání loupeže v bance, ale nebyla naprogramována tak, aby někoho zabila. I přesto ale AI někoho zabije. Tentokrát bude programátor odpovědný za čin spáchaný AI, tedy

---

[290] INDEPENDENT HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE. *A definition of AI: Main capabilities and scientific disciplines* [online]. B.m.: European Commission. 8. duben 2019. Dostupné z: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341

[291] HALLEVY, Gabriel. The Criminal Liability of Artificial Intelligence Entities. *SSRN Electronic Journal* [online]. 2010. Dostupné z: doi:10.2139/ssrn.1564096

za loupež i zabití, přestože je k takovému spáchání třeba úmyslného zavinění. Samotná AI by v tomto případě měla být také trestně odpovědná entita.

Poslední model představuje přímou odpovědnost AI, která se od odpovědnosti lidí příliš neliší a je třeba naplnění jak subjektivní, tak objektivní stránky. Z hlediska objektivní stránky trestného činu je třeba jednání, jako projev vůle ve vnějším světě, a následek, tedy porušení či ohrožení zákonem chráněného zájmu. Při jednání dochází ke spojení složky psychické (vůle) a fyzické (projev vůle). Vyvstává otázka, zda dokáže umělá inteligence mít psychickou vůli. AI na základě naučených znalostí provádí analýzu všech podnětů (např. data z různých receptorů pro zrak, zvuk, dotek či fyzický kontakt), což se dá přirovnat k lidskému porozumění. Pokročilé algoritmy AI se snaží napodobit lidský kognitivní proces. Projev vůle navenek zde jistě nastane, protože například v případě robota dochází k pohybu jeho částí těla. Z hlediska subjektivní stránky trestného činu je pak třeba zavinění, což je vnitřní psychický vztah pachatele k určitým skutečnostem, které zakládají trestný čin. Takový psychický vztah se dá naprogramovat a AI nepochybně je schopná se ho sama naučit.[292] Mikeš se domnívá, že co se týče zavinění, tak „*připustit, že vůlí a schopností ji projevit je nadána i zcela jiná entita, než je člověk (...) může být chápáno i jako zpochybnění lidství a lidstva jako takového*“, a s takovými koncepty je třeba zacházet citlivě a opatrně.[293]

Měla by tedy být umělé inteligenci do budoucna přiznána právní osobnost a mělo by být možné umělé inteligenci přičítat trestné činy? S takovými otázkami se právo bude muset v blízké budoucnosti vypořádat, protože se objevuje čím dál více situací, kdy je umělá inteligence využívána a kdy může být jejím prostřednictvím spáchán trestný čin nebo způsobena škoda. Pokud bychom umělou inteligenci skutečně zařadili do právního řádu například v podobě elektronické osoby[294], nastává otázka, jakým způsobem by docházelo k trestání. Evropský parlament v roce 2017 ve svém usnesení navrhuje „*vytvoření zvláštního právního statutu robota v dlouhodobém výhledu, aby alespoň ti nejsložitější autonomní roboti mohli mít status elektronické osoby odpovědné za náhradu jimi*

---

[292] Ibid.

[293] MIKEŠ, Stanislav. Právo ve věku inteligentních strojů. *Bulletin advokacie*. 2018, (4), 17–22.

[294] KIDMAN, David a Stephen TURNER. Electronic persons: time for a new legal personality? *New Law Journal* [online]. 2017, (Issue 7758) [vid. 2020-08-30]. Dostupné z: https://www.newlawjournal.co.uk/content/electronic-persons-time-new-legal-personality-0

způsobené škody, a možné použití elektronické osoby v případech, kdy roboti činí autonomní rozhodnutí nebo jsou jiným způsobem samostatně v kontaktu se stranami“.[295]

Dle Mikeše by do budoucna měl být pojem umělá inteligence v našem právním řádu upraven a zároveň by měla být zavedena specifická kategorie škody způsobené umělou inteligencí. Umělou inteligenci by bylo možné „*definovat např. jako útvar odlišný od člověka nadaný schopností samostatně rozhodovat a jednat, potažmo jako umělý útvar nadaný právní osobností od svého vzniku do svého zániku, obdobně jako je tomu u právnické osoby*.“[296]

V současné době lze na umělou inteligenci pohlížet jako na věc v souladu s § 134 TZ, případně jako na software z pohledu autorského práva. Zatím nebylo třeba řešit mnoho situací, kdy umělá inteligence způsobila spáchání trestného činu, a tedy nebylo nutné se zamýšlet nad změnou právního řádu. Nejpalčivějším tématem je pak autonomní řízení vozidel, které se pomalu, ale jistě rozšiřuje na světovém trhu a je jen otázka času, kdy se objeví u nás. Zcela nepochybně se začnou objevovat případy způsobení škody, případně trestné činy s řízením související, a bude třeba se vyrovnat s tím, kdo je za tento čin odpovědný. Do úvahy přichází hned několik subjektů, prvním z nich je tvůrce algoritmu umělé inteligence, tedy programátor. Dále se zde může vyskytovat nějaký vlastník umělé inteligence, který poskytuje licence dalším uživatelům. Následně přichází do úvahy samotný uživatel a případně někdo, kdo vykonává dohled či obsluhu daného stroje.

Najít tu správnou a skutečně odpovědnou osobu je velmi obtížné, zejména z toho důvodu, že umělá inteligence může mít díky strojovému učení takříkajíc vlastní vůli a její aktivity pak nelze ovlivňovat. Bude pak třeba najít příčinnou souvislost mezi jednáním umělé inteligence, jednáním další osoby (programátora, uživatele apod.) a následkem takového jednání. I z těchto důvodů by bylo vhodné zavést nějaký právní rámec, který by alespoň do určité míry tuto problematiku upravoval. Evropská komise vytvořila dokument zabývající se odpovědností umělé inteligence[297], kde mezi klíčová zjištění patří fakt,

---

[295] Usnesení Evropského parlamentu ze dne 16. února 2017 obsahující doporučení Komisi o občanskoprávních pravidlech pro robotiku (2015/2103(INL)), bod 59 písm. f), [ÚV C 252/239].

[296] MIKEŠ, Stanislav. Právo ve věku inteligentních strojů. *Bulletin advokacie*. 2018, (4), 17–22.

[297] EUROPEAN COMMISSION a DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS. *Liability for artificial intelligence and other emerging digital technologies.* [online]. 2019 [vid. 2020-08-30]. ISBN 978-92-76-12959-2. Dostupné z: https://op.europa.eu/publication/manifestation_identifier/PUB_DS0319853ENN

že pro účely odpovědnosti není třeba, aby autonomní systémy měly právní osobnost. Jedním z důvodů je velké množství etických otázek[298] v této oblasti, dále je pak zpravidla možné škodu přičíst fyzickým či právnickým osobám, tedy již existujícím kategoriím osob. Problematické je též vymáhání škody od umělé inteligence jako subjektu, což by zřejmě podléhalo vyplacení nějaké pojistky. Podrobně je pak v dokumentu upraveno, který subjekt je za jednání dané technologie odpovědný. Důraz je kladen na zavedení důkladného záznamu (angl. *logging*) veškeré činnosti umělé inteligence pro případné možné nalezení chyby a zjištění sledu událostí.

Napříč Evropou se k dané problematice přistupuje vždy trochu jinak. Za způsobenou škodu autonomně řízeného vozidla (např. jeho náraz do stromu) může alternativně odpovídat několik subjektů. Auto mohlo být již od počátku špatně navrženo, a to jak z hlediska softwaru, tak z hlediska hardwaru. V tomto případě by nejspíše jako odpovědný přicházel do úvahy programátor, který umělou inteligenci vytvořil. Dále mohlo dojít ke špatnému přečtení či vyhodnocení dat, kdy by zřejmě byla odpovědná samotná umělá inteligence či její autor. Další možnosti je poskytnutí špatné aktualizace od původního výrobce či od nějaké třetí strany. Samotný uživatel rovněž mohl selhat při instalaci aktualizace.[299] Pokud do dané situace vstupuje větší množství faktorů a není zcela jasné, kdo z daných subjektů je odpovědný, pak jsou dvě možnosti. V první z nich nebude odpovědný nikdo, protože nebude možné nikomu prokázat vinu, v druhém případě budou odpovědné všechny subjekty společně a nerozdílně, k čemuž se přiklání většina odborníků.[300]

V současné době bude tedy za jednání umělé inteligence odpovědná fyzická či právnická osoba, ať už to bude autor daného algoritmu, vlastník AI či jiná osoba vykonávající dohled nad daným strojem. Do budoucna bude třeba upravit právní postavení AI jako

---

[298] Etickou otázkou ve vztahu k AI se zabývá dokument vydaný Evropskou komisí v roce 2019. In: INDEPENDENT HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE. *Ethics Guidelines for Trustworthy AI*. B.m.: European Commission. 8. duben 2019

[299] EUROPEAN COMMISSION a DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS. *Liability for artificial intelligence and other emerging digital technologies.* [online]. 2019, s. 22 [vid. 2020-08-30]. ISBN 978-92-76-12959-2. Dostupné z: https://op.europa.eu/publication/manifestation_identifier/PUB_DS0319853ENN

[300] WINIGER, Bénédict, Håkan ANDERSSON a ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN, ed. *Essential cases on natural causation*. Wien ; New York: SpringerWienNewYork, 2007, s. 387. Digest of European tort law, v. 1. ISBN 978-3-211-36957-9.

samostatného subjektu, vzhledem k tomu, že je již dnes možné, aby projevovala vlastní vůli, a chovala se tak úplně jinak, než zamýšlel její autor. S tím úzce souvisí úprava náhrady škody, kterou AI jako taková pochopitelně nebude moci uhradit. Jedná se o velice složitou problematiku a nebude vůbec jednoduché náš právní řád adaptovat změnám, ke kterým v oblasti AI velmi rychle dochází.

6.2 Cloudová úložiště

Cloud computing je „*model umožňující všudypřítomný, pohodlný, na vyžádání dostupný síťový přístup k sdílenému fondu konfigurovatelných výpočetních prostředků (např. sítě, servery, úložiště, aplikace a služby), které mohou být rychle opatřeny a uvolněny s minimálním úsilím na jejich správu anebo interakci ze strany poskytovatele služby*."[301] Existuje několik modelů využití cloudu – Software as a Service (SaaS), Platform as a Service (PaaS) a Infrastructure as a Service (IaaS). V poslední době se velmi rozšířila platforma Cybercrime as a Service (CaaS), na kterou lze analogicky pohlížet jako na cloudovou platformu. Jedná se o rozsáhlou velmi dobře zorganizovanou síť zahrnující leadery, inženýry, osoby zajišťující samotné psaní škodlivého softwaru (nazývaní jako pěchota) a také pašeráky peněz. V rámci CaaS je pak poskytována celá škála produktů, jako útočné nástroje a metody, poradenství, služby, reklama a samozřejmě obrovské množství různých programů umožňujících páchání kyberzločinů. V nabídce se vyskytuje například nastavení botnetů, zajištění šíření počítačového viru, zajištění DDoS útoku, cloud cracking[302] a půjčování či leasing hackerských nástrojů.[303]

Z hlediska trestního práva je problematické zejména vyšetřování a v rámci něj zajišťování dat nacházejících se na cloudovém úložišti. Servery, na kterých jsou uložená data se mnohdy nacházejí v jiných státech a zpravidla je třeba znát přihlašovací údaje do daného

---

[301] MELL, Peter a Timothy GRANCE. *The NIST Definition of Cloud Computing* [online]. B.m.: National Institute of Standards and Technology. 2011. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[302] Cloud cracking je vysoce výkonné prolomení hesel za nízkou cenu. Zhruba 300 milionů pokusů, které trvají přibližně 20 minut, stojí zhruba 17 dolarů. In: KORLAM, Gautam. *Password Cracking in the Cloud* [online]. B.m., 2012 [vid. 2020-08-31]. Department of Computer Science, UC Santa Barbara. Dostupné z: https://silo.tips/download/password-cracking-in-the-cloud

[303] MANKY, Derek. Cybercrime as a service: a very modern business. *Computer Fraud & Security* [online]. 2013, **2013**(6), 9–13. ISSN 1361-3723. Dostupné z: doi:10.1016/S1361-3723(13)70053-8

účtu. Protože se pevné disky většinou nachází na neznámém místě a nelze je fyzicky zajistit, bylo by možné od provozovatele úložiště dožádat pouze konkrétní data uživatele uložená v cloudu v souladu s § 78 a násl. TŘ ve spojení s § 8 odst. 5 TŘ. Disky tvořící cloudové servery budou velkokapacitní a budou obsahovat data velkého množství subjektů, což by komplikovalo dodání celých disků jako důkazního materiálu. Pokud by policejní orgán zajistil v rámci domovní prohlídky počítač, kdy by z něj bylo možné prostřednictvím uložených hesel získat přístup k datům na cloudovém úložišti, bylo by nutné pojem počítačový systém vykládat velice široce a zahrnout do něj právě i cloudové úložiště. Vzhledem k tomu, že je fyzicky umístěno někde jinde a tvoří samostatný systém, ještě obvykle chráněný přihlašovacími údaji, nelze se k takovému výkladu přiklonit. Pro přístup do takového úložiště je proto potřeba oddělený zajišťovací úkon.[304]

S takovým přístupem však nesouhlasí Dostál, argumentující tím, že není podstatné, zda cloud tvoří samostatný počítačový systém či nikoliv. Pokud při dané prohlídce bude možné získat přístup i do cloudového úložiště, pak již není třeba samostatný zajišťovací úkon. Při zajišťování dat z tohoto úložiště, a vůbec při vyšetřování tohoto typu trestných činů, je třeba postupovat rychle a efektivně. Tomu nasvědčuje i ustanovení čl. 19 odst. 2 Úmluvy o počítačové kriminalitě, které zakotvuje urychlené rozšíření prohlídky v případě potřeby získat data z jiného počítačového systému. Při velké prodlevě mezi provedením prohlídky a získáním souhlasu soudce se zajištěním dat z cloudu hrozí nebezpečí znehodnocení důkazů, protože k úložišti lze přistoupit odkudkoliv a pachatel může data vymazat. Pro účinné zajištění dat z cloudu je vhodné dostatečně široce formulovat prohlídku prostor a zahrnout do ní výslovně i vzdálená úložiště.[305]

Pro zajištění obsahu cloudového úložiště samostatně bez provedení prohlídky bude možné použít ustanovení § 158d odst. 3 TŘ, i s ohledem na výše rozebírané rozhodnutí Ústavního soudu.[306] Tento institut lze použít pouze za předpokladu, že má policejní orgán do daného úložiště přístup, ať už z počítačového systému zajištěného v rámci předchozí prohlídky, nebo díky nalezeným přístupovým údajům. Problematické budou situace, kdy

---

[304] HLAVÁČOVÁ, Kateřina a Oliver CHORVÁT. Přístup orgánů činných v trestním řízení k datům uloženým v cloudu. *Revue pro právo a technologie*. 2016, (14), 3–24.

[305] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. díl). *Trestněprávní revue*. 2019, (3), 66–71.

[306] Usnesení Ústavního soudu ze dne 3. 10. 2013, sp. zn. III. ÚS 3812/2012 (U 10/71 SbNU 573).

policejní orgán nebude znát tyto údaje a bude muset požádat provozovatele úložiště o poskytnutí těchto údajů, a to v režimu dožádání dle § 8 odst. 1 TŘ.[307]

Autoři Maxwell a Wolf poskytují srovnání právních úprav jednotlivých států v této oblasti. Přestože je článek z roku 2012, lze předpokládat, že nedošlo k natolik velkým změnám, a přehled poslouží i k účelům této práce.[308] V Austrálii, Kanadě i Dánsku je vyžadován samostatný příkaz k prohlídce (angl. *search warrant*) pro získání dat z cloudového úložiště. Ve Francii je pak v trestním řádu v článku 57-1 výslovně stanoveno, že lze využít přístup do počítačového systému, který je napojený na počítačový systém nalezený v rámci prohlídky.[309]

V mnohých případech bude třeba využití mezinárodní justiční spolupráce, což proces dokazování značně zpomaluje a prodlužuje. Zde je relevantní zejména článek 31 Úmluvy o počítačové kriminalitě, který upravuje vzájemnou pomoc týkající se vyšetřovacích pravomocí, kde je stanoveno, že strana může požádat jinou stranu, aby ohledně dat, uložených prostřednictvím počítačového systému umístěného na území dožádané strany, včetně dat uchovaných podle článku 29, provedla prohlídku nebo k nim podobným způsobem získala přístup, zabavila je nebo je podobným způsobem zajistila a zpřístupnila. V daném ustanovení se předpokládá i možnost urychleného vyřízení žádosti. V našem právním řádu je daná problematika upravena v § 62 zákona č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních.

---

[307] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – úložiště, e-maily, telefony, sociální sítě a logy (4. díl). *Trestněprávní revue*. 2019, (6), 123–127.

[308] MAXWELL, Winston a Christopher WOLF. A Global Reality: Governmental Access to Data in the Cloud. *A Hogan Lovells White Paper* [online]. 2012 [vid. 2020-08-31]. Dostupné z: https://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf

[309] Francouzský Code de procédure pénale, article 57-1: Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

Závěrem lze shrnout, že současné instituty trestního řádu lze považovat za dostačující. Objevují se určité výkladové problémy, u kterých je ale předpoklad, že se postupně vyřeší s přibývajícím počtem případů. Nejproblematičtějším aspektem je nutnost mezinárodní justiční spolupráce v této oblasti, která kvůli velkému množství případů značně zpomaluje proces vyšetřování trestných činů.

6.3 Virtuální měny

Virtuální měny neboli kryptoměny jsou v současné době velmi populární. Jsou užívány jako prostředek směny a uchovatel hodnoty a dá se pomocí nich dnes koupit téměř cokoliv. Koupě a používání kryptoměny je zcela anonymní, a proto je velmi často využívána pro nelegální činnost, zejména v oblasti dark webu. Z hlediska trestního práva je obtížné zjištění totožnosti pachatele. Kryptoměna umožňuje snadnou legalizaci výnosů z trestné činnosti. Nejznámější kryptoměnou je bezpochyby bitcoin (BTC), což je software fungující na principu peer-to-peer. Kód vytvořil v roce 2008 Satoshi Nakamoto. Je předem známo konečné množství bitcoinů, které budou uvolněny do oběhu. Bitcoiny jsou získávány těžbou (angl. *mining*), která probíhá tak, že dochází k poměrně náročným počítačovým výpočtům. Správa bitcoinu se uskutečňuje na bázi digitální peněženky, která je uložena v počítači daného uživatele a je chráněna silným heslem. Nejdůležitějším aspektem bitcoinu je absence centrální autority a anonymita.

Bitcoin funguje na technologii tzv. blockchainu, což je řetězec digitálních podpisů. Každý vlastník převede minci na dalšího vlastníka tím, že digitálně podepíše hash[310] předchozí transakce a veřejný klíč dalšího vlastníka, a obojí připojí na konec dané mince. Příjemce může podpisy ověřit, a tím ověřit i celý řetězec vlastnictví.[311] Dle Fincka blockchain představuje sdílenou a synchronizovanou digitální databázi, která je udržována algoritmem a je uložena na více uzlech (počítače, na kterých jsou uloženy lokální verze distribuované účetní knihy). Blockchainy si lze představit jako peer-to-peer síť,

---

[310] Hash je unikátním otiskem, který představuje informaci jako řetězec znaků a čísel. In: FINCK, Michèle, ed. Blockchain Technology. In: Michèle FINCK, ed. *Blockchain Regulation and Governance in Europe* [online]. Cambridge: Cambridge University Press, 2018, s. 1–33. ISBN 978-1-108-47475-7. Dostupné z: doi:10.1017/9781108609708.001

[311] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* [online]. [vid. 2020-09-04]. Dostupné z: https://bitcoin.org/bitcoin.pdf

kdy jednotlivé uzly slouží jako různé peers.[312] „*Distribuovaná účetní kniha je ve skutečnosti záznamem konsenzu kryptografických auditních stop ověřených poté, co vzešly z jednotlivých uzlů. V případě bitcoinů účastníci odesílají hodnotu prostřednictvím sítě. Převodce je vybaven soukromým klíčem k tomu, aby jeho bitcoiny vstoupily do systému, zatímco nabyvatel disponuje veřejným klíčem s přístupem k síti, kde mohou být ověřené elektronické „hodnotové zprávy" zaslány na jeho adresu*."[313] Zjednodušeně lze říci, že blockchain je digitální, distribuovaná databáze umožňující kontrolu v rámci řetězení záznamů bez jakékoliv centrální autority.

> „*Bitcoiny jsou vytvářeny vyřešením kryptografické úlohy, která vede k vytvoření bloku BTC, což vyžaduje vysoký výpočetní výkon. Náročnost této úlohy navíc s časem (resp. s počtem vytěžených bloků) stoupá. Jako odměnu za vytvoření validního bloku dostane jeho tvůrce, takzvaný miner, určité množství nově vytvořených bitcoinů*."[314]

V roce 2018 vydala ČNB stanovisko „K obchodování s tzv. převodními tokeny", ve kterém pod převodními tokeny jsou spatřovány právě kryptoměny a dle tohoto stanoviska převodní tokeny „*nejsou penězi v ekonomickém ani právním smyslu*."[315] Obchodování s bitcoiny nevyžaduje povolení a ani nepodléhá dohledu ČNB. Nejedná se ani o peněžní prostředky ve smyslu zákona č. 284/2009 Sb., zákon o platebním styku. Definici virtuální měny v našem právním řádu nalezneme v § 2 odst. 1 písm. l) zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (dále jen „AML zákon"), kde je uvedeno, že virtuální měnou se rozumí „*elektronicky uchovávaná jednotka bez ohledu na to, zda má nebo nemá emitenta, a která není peněžním prostředkem podle zákona o platebním styku, ale je přijímána jako*

---

[312] FINCK, Michèle, ed. Blockchain Technology. In: Michèle FINCK, ed. *Blockchain Regulation and Governance in Europe* [online]. Cambridge: Cambridge University Press, 2018, s. 1–33. ISBN 978-1-108-47475-7. Dostupné z: doi:10.1017/9781108609708.001

[313] KULMS, Rainer. Úvod do práva blockchainů. *Obchodněprávní revue*. 2020, (1), 39–48.

[314] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 789. ISBN 978-80-7380-720-7.

[315] *K obchodování s tzv. převodními tokeny* [online]. B.m.: ČNB. 19. listopad 2018. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/casto-kladene-dotazy/.galleries/stanoviska_a_odpovedi/pdf/k_obchodovani_s_prevodnimi_tokeny.pdf

platba za zboží nebo služby i jinou osobou odlišnou od jejího emitenta." Stejně jako je tomu u umělé inteligence, můžeme bitcoin vnímat jako věc ve smyslu § 134 TZ.[316]

Bitcoiny se zcela jistě mohou stát předmětem útoku. Jak bychom tedy mohli kvalifikovat takový trestný čin? Pokud na bitcoiny budeme pohlížet jako na věc, pak by se jejich odcizení dalo kvalifikovat jako krádež dle § 205 TZ. Ostatně již jednou se k takovému výkladu přiklonil Krajský soud v Brně ve svém rozhodnutí ze dne 9. 10. 2017, č.j. 50 T 4/2017-3857.[317] Obžalovaný Tomáš Jiřikovský provozoval anonymizované tržiště s názvem Sheep Marketplace a v rámci něj získal přístup k privátním klíčům uživatelů a odcizil od nich celkem 840,70 BTC, které převedl na svou soukromou bitcoinovou adresu.

Otázkou je, zda by se bitcoiny daly označit jako samostatný počítačový systém. Pokud ano, pak bychom jakýkoliv útok na digitální peněženku s bitcoiny mohli posuzovat dle § 230 TZ jako neoprávněný přístup k počítačovému systému a nosiči informací. Dále by se kvalifikace odvíjela od konkrétních skutkových okolností, zda došlo k pouhému přístupu do digitální peněženky, či zda byly skutečně převedeny nějaké bitcoiny na jiný účet a jak vysoká vznikla škoda. Útočník může mít fyzicky v moci počítač s uloženou peněženkou, případně si může pomocí škodlivého softwaru zřídit dálkový přístup a k peněžence se dostat vzdáleně. V obou případech bude muset překonat zabezpečení peněženky. Vyvstává otázka, zda by byl možný souběh trestného činu krádeže dle § 205 TZ s trestným činem neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ.

Vzhledem k tomu, že bitcoin funguje na technologii blockchainu, který je označován jako databáze, se lze přiklonit k tomu, že se jedná o počítačový systém. Pachatel musí překonat bezpečnostní opatření, aby do peněženky a k bitcoinu získal přístup. Často se bude jednat o případy, kdy se k bitcoinové peněžence pachatel dostane již v rámci jiného útoku na daný počítač, kde je peněženka uložena, například hacking, phishing či malware. Není důvod, proč by nemohlo být odcizení bitcoinů z peněženky kvalifikováno jako trestný čin

---

[316] MATOCHA, Jakub. Virtuální měny a trestní právo. *Právní prostor* [online]. 2016 [vid. 2020-09-04]. Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/virtualni-meny-a-trestni-pravo

[317] Případem se později zabýval i Nejvyšší soud, který se přiklonil k tomu, že by měl být daný případ posouzen spíše jako zpronevěra dle § 206 TZ. In: Usnesení Nejvyššího soudu ze dne 7. 3. 2019, sp. zn. 11 Tdo 1428/2018.

krádeže a nikde nebyl ani výslovně vyloučen souběh těchto dvou trestných činů. V komentáři se naopak objevuje, že „*ve vztahu k zaknihovaným cenným papírům, které jsou považovány za věci (§ 134 odst. 1) a mají podobu záznamu v příslušné evidenci vedené i na nosičích informací, pak přichází v úvahu vedle trestného činu podvodu podle § 209 i souběh s trestnými činy krádeže a zpronevěry podle § 205 a § 206*.“[318] Dle tohoto výkladu nic nebrání tomu, aby odcizení bitcoinů bylo kvalifikováno podle § 230 TZ v souběhu s § 205 TZ.

Velmi často se objevuje útok zvaný cryptojacking (známý také pod pojmem cryptomining), který využívá výpočetní výkon počítače uživatele pro těžbu virtuální měny. Objevují se dva možné způsoby tohoto útoku. V prvním případě je pomocí phishingu do počítače nainstalován škodlivý kód, který umožní, aby na pozadí běžel skript provádějící těžbu kryptoměny bez jakékoliv znalosti uživatele. V druhém případě probíhá těžba v rámci internetového prohlížeče, tedy uživatel pouze navštíví nějaké stránky, ve kterých je přímo implementován škodlivý kód. Pozorný uživatel si může všimnout, že je jeho procesor nadmíru využíván, že je počítač zpomalený a případně se přehřívá. Tento útok by bylo nejspíše možné kvalifikovat podle § 230 TZ.

Jak již bylo zmíněno výše, bitcoiny představují riziko zejména v oblasti tzv. praní špinavých peněz. Dle důvodové zprávy k zákonu AML jsou virtuální měny velmi rizikové, protože s jejich využitím lze přerušit stopu převáděných prostředků.[319] Vyšetřování trestného činu legalizace výnosu z trestné činnosti dle § 216 TZ ztěžují virtuální prádelny peněz. „*Uživatelé jednoduše postupují tak, že tam pošlou své Bitcoiny, aplikace je zamíchá s Bitcoiny od jiných uživatelů a následně vrátí původním majitelům jiné Bitcoiny stejné hodnoty*.“[320] Bitcoiny lze velice snadno převádět napříč státy, což bude velmi ztěžovat zjištění původu peněz. Významným aspektem je poměrně snadná směna bitcoinu za hotovost či jinou virtuální měnu. V případě tohoto trestného činu

---

[318] GŘIVNA, Tomáš. § 230 [Neoprávněný přístup k počítačovému systému a nosiči informací]. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 2315. ISBN 978-80-7400-428-5.

[319] Důvodová zpráva k zákonu č. 253/2018 Sb., sněmovní tisk 752/0, s. 46.

[320] VRBÍK, Marek. Regulace open-source P2P platební sítě Bitcoin. *EPRAVO.CZ* [online]. 2014 [vid. 2020-09-04]. Dostupné z: https://www.epravo.cz/top/clanky/regulace-open-source-p2p-platebni-site-bitcoin-93971.html

nebude problematická jeho právní kvalifikace, ale vyšetřování a prokázání původu finančních prostředků.

Čím dál častěji se lze setkat s ransomware, což je škodlivý software, který napadne počítačový systém a zašifruje data na disku uživatele. Aby se uživatel mohl ke svým datům opět dostat, musí zaplatit výkupné v bitcoinech.[321] Tím je opět ztíženo vyšetřování tohoto trestného činu, který je zpravidla možné kvalifikovat jako trestný čin vydírání dle § 175 TZ, ale bude možné jej kvalifikovat i jako podvod dle § 209 TZ nebo neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 TZ.

Napříč státy se samozřejmě liší právní úprava virtuálních měn. V USA je bitcoin regulován jako komodita a v oblasti Plattsburghu je dokonce regulována jeho těžba. V Číně platí zákaz pro obchodování s bitcoiny a objevují se i jisté informace o zákazu těžby. Česká republika je označována jako domov společnosti SlushPool, což je největší těžařské uskupení (angl. *mining pool*) na světě. Jeho zakladatelem je Marek Palatinus a jen díky němu je Česká republika řazena mezi státy, které jsou nejvíce nakloněné užívání a těžbě kryptoměny. Podobně vhodné prostředí pro bitcoiny představuje Kanada, která dokonce nabízí výhodné tarify elektřiny pro usnadnění těžby virtuálních měn.[322]

Virtuální měny mají opravdu veliký potenciál v kriminální oblasti. V našem právním řádu zatím není tato oblast úplně regulována a bylo by vhodné nějaký právní rámec zavést. Zejména by bylo vhodné definovat ty rizikové činnosti, ve kterých by bylo potřeba implementovat centralizovaný dohled, a zajistit tak právní jistotu. Z hlediska kvalifikace trestných činů v této oblasti zpravidla není problém a je možné je pod nějakou skutkovou podstatu zařadit.

6.4 Internet věcí

Internet věcí (angl. *Internet of Things*), známý hlavně pod zkratkou IoT, je rychle rostoucím fenoménem dneška a hlavně budoucnosti. IoT propojuje velké množství věcí prostřednictvím sítě. Všechna připojená zařízení vzájemně komunikují a mohou si mezi

---

[321] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 806. ISBN 978-80-7380-720-7.

[322] JENKINSON, Gareth. Regulatory Overview of Crypto Mining in Different Countries. *Cointelegraph* [online]. 2019 [vid. 2020-09-04]. Dostupné z: https://cointelegraph.com/news/regulatory-overview-of-crypto-mining-in-different-countries

sebou předávat data, následně je vyhodnocovat a podle aktuální situace se i „zachovat“. Mnohdy není třeba jakéhokoliv pokynu uživatele. Do konce roku 2025 by součástí IoT mělo být celkem až 75 miliard zařízení.[323]

Nejtypičtějším příkladem IoT je tzv. chytrá domácnost, kde jsou do sítě zapojené domácí spotřebiče, ovládání světel, žaluzií, vytápění, klimatizace, televize, počítače, síťová úložiště, routery, alarmy, kamerové systémy, mobilní telefony, chytré hodinky a cokoliv dalšího. Nejvíce problematické je, že celou chytrou domácnost je možné ovládat z jednoho zařízení, typicky z chytrého telefonu. Pokud útočník získá přístup do tohoto zařízení, otevírají se mu velmi široké možnosti útoku. IoT je využíváno i v oblasti výroby, zdravotnictví či dopravy. Objevují se i koncepty tzv. smart cities, což jsou města, ve kterých je na síť připojena převážná většina infrastruktury (osvětlení, chytré lavičky, kamerové systémy, elektrárny, odpadkové koše, dopravní prostředky apod.).

IoT s sebou přináší poměrně velká rizika. Prvním z nich je vysoká zranitelnost a náchylnost ke kyberútokům. Pokud není síť dostatečně zabezpečena, může se stát, že bude hacker na dálku ovládat zařízení domácnosti, a ohrožovat tak i životy lidí. Vzhledem k tomu, že zařízení zapojená v IoT shromažďují velké množství dat, včetně citlivých údajů, existuje zde riziko zneužití získaných dat, ať už hackery nebo i samotnými společnostmi, která dané zařízení provozují.

IoT může sloužit nejen jako terč útoku, ale i jako dobrý nástroj k provádění dalších útoků. Vzhledem k tomu, že zabezpečení zařízení není prioritou výrobců, není třeba tolik technických znalosti pro jejich napadení. Příkladem využití IoT jako nástroje je Mirai, což je malware, který napadá zranitelná zařízení zapojená v systému IoT, jako jsou webkamery, modemy a routery, a z každého z nich udělá botnet. Mirai se poprvé objevil v roce 2016 a rychle se stal vhodným malwarem pro provádění rozsáhlých útoků, včetně masivního DDoS útoku, který vyřadil z provozu celý stát Libérie, a také DDoS útoku proti firmě Dyn zajišťující internetovou infrastrukturu.[324]

---

[323] PENG, Sheng-Lung, Souvik PAL a Lianfen HUANG, ed. *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm* [online]. Cham: Springer International Publishing, 2020, s. 552 [vid. 2020-09-06]. Intelligent Systems Reference Library. ISBN 978-3-030-33595-3. Dostupné z: doi:10.1007/978-3-030-33596-0

[324] *Cyber Attack Trends Analysis Report* [online]. B.m.: Check Point Software Technologies Ltd. Dostupné z: https://www.checkpointdirect.co.uk/media/downloads/check-point-2019-security-report-volume-1.pdf

V průběhu roku 2020 by měly být spuštěny 5G sítě, které mají za cíl reagovat na požadavky nových technologií jako je například IoT. 5G sítě poskytují rychlejší připojení pro stále se zvyšující počet zařízení neustále připojených na internet. Z hlediska kyberbezpečnosti ale představují určité riziko tím, že umožňují simultánně stahovat data z většího množství zdrojů, a proto bude velmi obtížné vyšetřování komunikace v těchto sítích. Vyšetřování bude také ztíženo tím, že v 5G sítích budou mít zařízení pouze dočasný identifikátor, zatímco v současných 4G sítích má každé zařízení přiřazeno unikátní identifikační kód, pomocí kterého je možné zařízení dohledat.[325]

IoT otevírá široké možnosti útoků, právě díky rychlosti sítě 5G a nízké latenci, kterou tato síť poskytuje. Mezi nejpravděpodobnější útoky patří již výše zmiňovaný DDoS, dále s tím související vytváření botnetů, sociální inženýrství, MITM attack a tzv. AI „Habitat“, což je červ založený na umělé inteligenci, který dokáže infikovat celou infrastrukturu. V oblasti IoT je rovněž vysoký potenciál využití technologie blockchainu, například pro vytvoření seznamu zařízení IoT, což by znemožnilo regulačním orgánům vytvoření jejich vlastního systému IoT. Mezi nejčastější motivy patří hlavně vydírání, sledování, průmyslová špionáž, krádež identity a propaganda.[326]

IoT využívají standardně i nemocnice a jiná zdravotnická zařízení. Do jedné sítě jsou připojené všechny přístroje (např. rentgeny, plicní ventilátory, EKG), systém pro vedení elektronické kartotéky pacientů, vydávání e-receptů, e-neschopenek a další. Právě systémy zdravotnických zařízení představují nejvíce zranitelnou oblast, protože jejich vyřazení z provozu může ohrozit životy lidí a způsobit rozsáhlé škody. Terčem útoku se na konci roku 2019 stala také benešovská nemocnice, jejíž provoz byl útokem výrazně omezen. Podle dostupných informací se zřejmě jednalo o ruský ransomware Ryuk.[327]

---

[325] EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION. *Iocta, Internet Organised Crime Threat Assessment: 2018.* [online]. 2018, s. 60 [vid. 2020-09-06]. ISBN 978-92-95200-94-4. Dostupné z: http://dx.publications.europa.eu/10.2813/858843

[326] TZEZANA, Roey. High-probability and wild-card scenarios for future crimes and terror attacks using the Internet of Things. *Foresight* [online]. 2017, **19**(1), 1–14. ISSN 1463-6689. Dostupné z: doi:10.1108/FS-11-2016-0056

[327] MAGDOŇOVÁ, Jana. Na nemocnici v Benešově útočil ruský virus Ryuk. Jermanová odmítá, že by někdo požadoval výkupné. *iRozhlas* [online]. 2020 [vid. 2020-09-06]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/nemocnice-benesov-kyberneticky-utok-ransomware-vykupne-ochrana-osobnich-udaju_2001140615_cha

Do dnešního dne se nepodařilo najít pachatele tohoto útoku. Právě vyšetřování a nalezení pachatele je v této oblasti velmi obtížné. Útoky zpravidla směřují ze zahraničí, často se na nich podílí větší množství hackerů, většinou profesionálních, kteří umí své stopy dobře zamaskovat. Nejlepší obranou je v této oblasti prevence. V dubnu roku 2020 vydal Národní úřad pro kybernetickou bezpečnost varování před útoky na systémy zdravotnických zařízení, jejichž přípravná fáze měla spočívat ve spear phishingu.[328] Klíčová infrastruktura státu by měla být dostatečně dobře zabezpečena a připravena odrazit útoky na jejich sítě. Dle odborníka na kyberbezpečnost Miloslava Lujky je český stát zabezpečen pouze z 20 %.[329] Několik útoku na státní infrastrukturu se objevilo i v minulosti. Terčem útoku bylo například Ministerstvo zahraničních věcí, Psychiatrická nemocnice v Kosmonosech, Fakultní nemocnice Brno či Pražský hrad.

Při útocích na instituce je nejčastěji využíván útok typu DDoS, který zahltí systém, a vyřadí tak danou instituci z provozu. Takový útok naplňuje skutkovou podstatu trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ. Na tento útok bude většinou navázáno několik dalších trestných činů. Příkladem může být již výše zmiňovaný útok na nemocnici. V případě, že dojde k úplnému ochromení nemocničního systému a vypojení všech přístrojů, pak se může stát, že budou ohroženy životy pacientů. Kdo bude za případné úmrtí člověka odpovědný? Bude se daný čin kvalifikovat jako vražda nebo usmrcení z nedbalosti? Mohl a měl útočník počítat s tím, že může někdo zemřít? A v případě, že je útočníků více, budou odpovědní jako spolupachatelé? Může také dojít k situaci, kdy si útok někdo objednal v rámci CaaS. Na všechny tyto otázky se hledají odpovědi velmi těžko.

Při útoku na benešovskou nemocnici nedošlo k žádnému úmrtí v důsledku kyberútoku. Dá se předpokládat, že si lékaři umí s danou situací poradit a že všechny klíčové přístroje nejsou na danou síť připojeny. Situace, kdy někdo umře, pak budou výjimečné. Technologie se ale vyvíjí a do budoucna se může stát, že tomu bude jinak. Odpovědným subjektem by zřejmě měl být útočník, případně osoba, která si daný útok objednala.

---

[328] *Varování před hrozbou kybernetických útoků na nemocnice a jiné významné cíle ČR* [online]. B.m.: Národní úřad pro kybernetickou bezpečnost. 16. duben 2020. Dostupné z: https://www.nukib.cz/download/uredni_deska/Varovani_NUKIB_2020-04-16.pdf

[329] TITLBACH, Filip. Česká státní správa je zabezpečená na 20 procent, říká kyberspecialista. *Deník N* [online]. 2019. Dostupné z: https://denikn.cz/224271/studio-n-ceska-statni-sprava-je-zabezpecena-na-20-procent-rika-kyberspecialista

Vše bude záležet na důkladném vyšetřování trestného činu a prokázání viny. Právě vyšetřování je v oblasti IoT dost problematické, a to hned z několika důvodů.

Prvním důvodem je, že se v systému nachází obrovské množství dat a je poměrně obtížné určit, která jsou pro vyšetřování daného trestného činu relevantní, a rovněž určit, která zařízení byla užita pro spáchání útoku. Všechna zařízení jsou vzájemně propojená a každé z nich může mít úložiště lokální i v cloudu, navíc každé zařízení může mít úplně jiné cloudové úložiště. Na druhou stranu některé věci v IoT jsou mnohdy bez jakéhokoliv paměťového úložiště, což zase znemožňuje zajištění důkazů. Problematické je i určení jurisdikce a následné zajišťování důkazů z jiných států, což souvisí právě s užíváním cloudových úložišť. Zároveň je třeba se vypořádat s komplexností IoT a opravdu rozličného množství produktů, které se v dané síti nacházejí, s tím, že každý z nich může vyžadovat trochu odlišný přístup a technické znalosti.[330]

Klasické vyšetřovací metody budou zřejmě poměrně neefektivní a nebude možné je při vyšetřování útoků na systém IoT využívat. Proto by bylo třeba zavést nový právní rámec týkající se vyšetřování v této oblasti, zejména s ohledem na heterogenitu všech zařízení užívaných v IoT. Nejdůležitější je dostatečná prevence, protože jakmile již nějaký útok na systém IoT nastane, tak to může ohrozit fungování klíčových státních institucí, ale také zdraví a životy lidí. To se týká i útoků na tzv. chytré domácnosti, kde jsou ohrožena hlavně citlivá data uživatelů (zdravotní data, osobní údaje). Dále je ohrožen jejich majetek, protože při hacknutí systému chytré domácnosti je možné vypnout zabezpečovací systémy, vniknout do domu bez povšimnutí a z domácnosti odcizit věci. A v neposlední řadě mohou být ohroženy i životy a zdraví uživatelů, protože v rámci systému IoT je velmi snadné zjistit zvyklosti lidí, vysledovat, kde se v jakou dobu nachází a pak tyto informace využít ke spáchání závažnějších trestných činů.

---

[330] PENG, Sheng-Lung, Souvik PAL a Lianfen HUANG, ed. *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm* [online]. Cham: Springer International Publishing, 2020, s. 551–577 [vid. 2020-09-06]. Intelligent Systems Reference Library. ISBN 978-3-030-33595-3. Dostupné z: doi:10.1007/978-3-030-33596-0

ZÁVĚR

Kybernetická kriminalita je na vzestupu a lze očekávat, že do budoucna bude tato trestná činnost ještě četnější. Nahrává tomu i aktuální situace ohledně pandemie viru COVID-19, která způsobila, že se do kyberprostoru přesunulo velké množství každodenních činností, jako je práce, studium, nakupování apod. Zároveň hraje útočníkům do karet i poměrně velká neznalost uživatelů v této oblasti, kteří si neuvědomují, jaké dopady může mít jejich jednoduché heslo a slabé zabezpečení sítě. Kyberprostor se velmi rychle stává prostředím, kde dnes můžeme dělat úplně cokoliv. Jeho specifické aspekty, jako neomezenost, dostupnost nebo anonymita uživatelů, ztěžují vyšetřování trestné činnosti, která se v něm odehrává.

Vzhledem k místní neomezenosti kyberprostoru a vzhledem k tomu, že kyberkriminalita nezná hranic, je potřeba, aby probíhala účinná mezinárodní spolupráce a koordinace. K tomu slouží poměrně rozsáhlá právní úprava v mezinárodněprávní oblasti. Nejznámějším dokumentem je Úmluva o počítačové kriminalitě, která již přes 16 let slouží jako dobré vodítko pro stíhání trestných činů v oblasti kyberkriminality. V rámci mezinárodních organizací jako je EU, Rada Evropy, NATO i OSN jsou vytvořeny specializované orgány, které sdružují experty pro danou oblast a umožňují se s náročnými situacemi vypořádat. Každoroční pořádání konferencí a simulací kyberútoků tvoří velmi významnou platformu pro sdružování odborníků na kyberkriminalitu a na kyberbezpečnost, kteří se snaží adaptovat rychlým změnám v této oblasti, a zajistit tak co nejúčinnější obranu proti sofistikovanějším útokům.

Kyberútoky jsou dnes již na každodenním pořádku a často směřují na klíčové instituce infrastruktury státu. Rychlý růst technologií umožňuje hackerům pronikat do zařízení lidí a ohrožovat jejich soukromí a citlivá data. Největší rozmach zaznamenaly útoky typu DoS a DDoS, které umožňují v jeden moment napadnout obrovské množství zařízení. Hackerům ale velmi dobře poslouží i jednoduché kyberútoky, jako obyčejné prolomení hesla nebo phishing. S rozvojem sociálních sítí pak některé útoky získaly nový rozměr. Jedná se zejména o kybergrooming, kyberšikanu a kyberextremismus. Velmi závažný problém představuje oblast dětské pornografie a kyberterorismus.

Při odhalování trestné činnosti jsou vyšetřovatelé postaveni různým výzvám. Základním problémem je nakládání s elektronickými důkazy, a hlavně digitální forenzní analýza

živých systému, která je potřeba čím dál častěji. Zároveň je v rámci vyšetřování problematické najít rovnováhu mezi účinným nalezením vhodných důkazů pro odhalení trestné činnosti a právem na spravedlivý proces a s ním souvisejícím právem na ochranu soukromí. Stále stoupající množství dat znesnadňuje nalezení relevantních důkazů, stejně tak se musí vyšetřovatelé vypořádat s problémem určení jurisdikce a v mnohých případech přistoupit k mezinárodní justiční spolupráci. V tomto ohledu hraje významnou roli institut Evropského vyšetřovacího příkazu, který usnadňuje získávání důkazů napříč státy.

Současná česká právní úprava do jisté míry zareagovala na stoupající tendence kyberkriminality, a proto byly zavedeny nové druhy trestných činů týkající se neoprávněného přístupu k počítačovým systémům. Velké množství útoků lze zařadit pod skutkové podstaty podle § 230–232 TZ. Ostatní útoky zpravidla lze kvalifikovat jako trestné činy, které se přímo netýkají informačních systémů. Příkladem může být trestný čin podvodu nebo porušení autorského práva, práv souvisejících s právem autorským a práv k databázi.

Nové technologie, jako umělá inteligence, cloudová uložiště, virtuální měny, internet věcí a další trendy, vytváří nová úskalí v oblasti trestního práva. Vzhledem k rychlému vývoji je velmi obtížné na tyto změny flexibilně reagovat. Proces přijímání zákonů není tak rychlý a obvykle mu předchází dlouhé debaty odborníků. Určitý právní rámec poskytuje mezinárodní právo nebo právo EU. Umělá inteligence a její používání je problematické zejména s ohledem na zjištění, kdo ponese odpovědnost za způsobený trestný čin. Cloudová úložiště vytvářejí výzvu zejména v oblasti vyšetřování, konkrétně zajišťování důkazů. Kryptoměny se mohou stát předmětem útoků, ale také mohou velmi dobře posloužit k ukrytí peněz získaných z trestné činnosti. Jsou rovněž běžným platebním prostředkem na dark webu, kde si člověk může jakýkoliv kyberútok objednat. Internet věcí představuje budoucnost plnou otázek, které nebude snadné zodpovědět. Propojení všech věcí v rámci jedné sítě vytváří zranitelné struktury, které se mohou stát terčem útoku, nejtypičtěji ransomwaru.

Nové technologické trendy mohou ale na druhou stranu pomoci při vyšetřování trestných činů a v boji proti kyberútokům. Pomocí umělé inteligence a softwaru pro rozpoznávání obličeje je možné vyhledávat zločince. Stejně tak je možné vytvořit takové algoritmy, které budou zabezpečovat dané systémy, a bránit jejich napadení. Internet věcí, big data

a umělá inteligence mohou pomoci lépe detekovat a předvídat hrozby. Zároveň bude možné rychleji a účinněji analyzovat data, a tím pohotověji reagovat na nastalou situaci.

V dnešní době se nevede konvenční způsob války, ale především válka o informace. Většina útoků cílí na data, zejména na citlivá data uživatelů, která jsou následně zneužívána pro mediální účely. Do budoucna bude přibývat situací, kdy na straně útočníka bude umělá inteligence, ale zároveň bude umělá inteligence i na straně obrany. Bude tedy svým způsobem probíhat válka robotů s roboty, a to o informace, data a osobní údaje nás všech.

Domnívám se, že české trestní právo se s útoky na informační systémy umí poměrně dobře vypořádat. Ve většině případů postačují pro právní kvalifikaci již existující trestné činy, a není třeba právní úpravu měnit. Jako problematické se mi jeví vyšetřování kyberútoků, jelikož je k němu potřeba vysoce technicky vzdělaných odborníků, kterých je nedostatek. Velmi často je stíhání těchto trestných činů zpomalováno zbytečnými formalismy a nejasnostmi, zejména v oblasti domovních prohlídek a zajišťovacích prostředků.

Rozvoj nových technologií by zasloužil trochu větší pozornost. Dle mého názoru by bylo vhodné vytvořit nějaký právní rámec zejména v oblasti kryptoměn, a reflektovat tak jejich častější užívání jako běžného platebního prostředku. Obávám se, že se budeme čím dál tím více setkávat s autonomně řízenými vozidly, což bude komplikovat celou řadu trestněprávních aspektů. Zejména by bylo vhodné se zabývat odpovědností umělé inteligence, která skutečně bude moci projevovat svou vlastní vůli, a dopustit se tak zavinění trestného činu.

SEZNAM POUŽÍVANÝCH ZKRATEK

AI	Artificial Intelligence	Umělá inteligence
AIDP	Association Internationale De Droit Pénal	Mezinárodní společnost pro trestní právo
AML	Anti-money Laundering	Opatření proti praní špinavých peněz
BIS		Bezpečnostní informační služba
BTC	Bitcoin	
BYOD	Bring Your Own Device	Přinést si vlastní zařízení
C-PROC	Cybercrime Programme Office of the Council of Europe	Kancelář Rady Evropy pro počítačovou kriminalitu
CaaS	Cybercrime as a Service	Kyberkriminalita jako služba
CCD CoE	NATO Cooperative Cyber Defence Centre of Excellence	Centrum výjimečnosti NATO pro kyberobranu
CCPCJ	Commission on Crime Prevention and Criminal Justice	Komise OSN pro prevenci kriminality a trestní spravedlnost
CCTV	Closed-circuit television	Kamerový systém, záznamy z kamer
CERT-EU	Computer Emergency Response Team for the EU	Skupina pro reakci na počítačové hrozby
CIT	Cyber Intelligence Team	Tým pro zpravodajskou službu v oblasti kyberkriminality

CNP fraud	Card-Not-Present fraud	Podvod, kdy není přítomna platební karta
CoE	Council of Europe	Rada Evropy
COVID-19	Coronavirus disease 2019	Koronavirové onemocnění 2019
CyCon	The International Conference on Cyber Conflict	Mezinárodní konference zaměřená na kybernetické konflikty
CyOC	Cyberspace Operations Center NATO	Kybernetické operační centrum NATO
ČNB		Česká národní banka
ČR		Česká republika
DDoS	Distributed Denial of Service	Distribuované odmítnutí služby
DEFR	Digital Evidence First Responder	Fyzická osoba, která jako první přichází do styku s digitálním důkazem a je k nakládání s ním dostatečně odborně kvalifikována
DNS	Domain Name System	Systém doménových jmen
DoS	Denial of Service	Odmítnutí služby
EC3	European Cybercrime Centre	Evropské centrum pro boj proti kyberkriminalitě
EGM	Expert Group Meeting	Zasedání expertní skupiny
EKG		Elektrokardiografie
EndOCSEA	End Online Child Sexual Exploitation and Abuse	Stop sexuálnímu vykořisťování a zneužívání dětí online

ENISA	The European Union Agency for Cybersecurity	Agentura Evropské unie pro bezpečnost sítí a informací
EU	European Union	Evropská unie
Europol	European Police Office	Evropský policejní úřad
GDPR	General Data Protection Regulation	Nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
GLACY+	Global Action on Cybercrime Extended	Rozšíření globálního boje proti kyberkriminalitě
IaaS	Infrastructure as a Service	Infrastruktura jako služba
ICT	Information and Communication Technologies	Informační a komunikační technologie
IMEI	International Mobile Equipment Identity	Sériové číslo mobilního telefonu
IMSI	International Mobile Subscriber Identity	Sériové číslo SIM karty
INCYDER	International Cyber Developments Review	Interaktivní databáze dokumentů týkajících se kybernetické bezpečnosti
INTCEN	European Union Intelligence and Situation Centre	Zpravodajské a situační středisko EU
IOCTA	Internet Organized Crime Threat Assessment	Hodnocení hrozeb organizované trestné činnosti na internetu

IoT	Internet of Things	Internet věcí
IP	Internet Protocol Address	Adresa uživatele na internetovém připojení
ISIS	Islamic State of Iraq and Syria	Islámský stát
ISO/IEC 27037:2012		Technická norma (Informační technologie – Bezpečnostní techniky – Směrnice pro identifikaci, sběr, akvizici a uchovávání digitálních důkazů)
ISP	Internet Service Provider	Poskytovatel internetového připojení
IT	Information Technology	Informační technologie
J-CAT	Joint Cybercrime Action Taskforce	Společná pracovní skupina pro boj proti kyberkriminalitě
LTE	Long Term Evolution	Technologie pro vysokorychlostní internet v mobilních sítích
LZPEU		Listina základních práv EU
LZPS		Listina základních práv a svobod
MAC adresa	Media Access Control Address	Číslo, které slouží k identifikaci zařízení v počítačové síti
MITM	Man-in-the-middle	Nezvaný host ve dvoustranné komunikaci
NAS	Network Attached Storage	Síťové datové úložiště

NATO	North Atlantic Treaty Organization	Severoatlantická aliance
NCIRC	NATO Computer Incident Response Capability	Tým NATO pro reakci na počítačové incidenty
NIAS	NATO Information Assurance Symposium	Konference NATO na téma kybernetické bezpečnosti
NÚKIB		Národní úřad pro kybernetickou a informační bezpečnost
OECD	Organization for Economic Cooperation and Development	Organizace pro hospodářskou spolupráci a rozvoj
OSN		Organizace spojených národů
P2P	Peer-to-peer	Síť pro vzájemnou komunikaci jednotlivých uživatelů
PaaS	Platform as a Service	Platforma jako služba
RFID	Radio Frequency Identification	Identifikace na rádiové frekvenci
SaaS	Software as a Service	Software jako služba
SDEU		Soudní dvůr Evropské unie
SWGDE	Scientific Working Group on Digital Evidence	Vědecká pracovní skupina zabývající se digitálními důkazy
T-CY	Cybercrime Convention Committee	Výbor k Úmluvě o počítačové kriminalitě
TŘ		zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)

TZ		zákon č. 40/2009 Sb., trestní zákoník
UK	United Kingdom	Velká Británie
UNODC	United Nations Office on Drugs and Crime	Úřad OSN pro drogy a kriminalitu
USA	United States of America	Spojené státy americké
ÚS		Ústavní soud
VoIP	Voice over Internet Protocol	Volání prostřednictvím počítačové sítě
VPN	Virtual Private Network	Virtuální soukromá síť
Wi-Fi	Wireless Fidelity	Bezdrátová síť
ZEK		Zákon o elektronických komunikacích

SEZNAM POUŽITÝCH ZDROJŮ

Seznam použité literatury

AWAN, Imran. Cyber-Extremism: Isis and the Power of Social Media. *Society*. 2017, roč. 54, č. 2, s. 138–149. ISSN 1936-4725.

BERGMAN, Michael K. White Paper: The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing*. 2001, roč. 7, č. 1. ISSN 1080-2711. DOI: 10.3998/3336451.0007.104

CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the Internet*. 3rd ed. Waltham, MA: Academic Press, 2011. ISBN 978-0-12-374268-1.

CLOUGH, Jonathan. A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation. *Monash University Law Review*. 2014, roč. 40, č. 3, s. 698–736.

CLOUGH, Jonathan. *Principles of cybercrime*. Cambridge, UK; New York: Cambridge University Press, 2010. ISBN 978-0-521-89925-3.

ČERMÁK, Jiří. Ochrana autorského práva v prostředí peer to peer sítí typu BitTorrent s přihlédnutím k rozsudku ve věci The Pirate Bay. *Právní rozhledy*. 2010, č. 8, s. 272-280.

DE KIMPE, Lies et al. You've got mail! Explaining individual differences in becoming a phishing target. *Telematics and Informatics*. 2018, roč. 35, č. 5, s. 1277–1287. ISSN 0736-5853.

DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. díl). *Trestněprávní revue*. 2019, č. 3, s. 66–71.

DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – odposlech a údaje o komunikaci (2. díl). *Trestněprávní revue*. 2019, č. 4, s. 77–83.

DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – úložiště, e-maily, telefony, sociální sítě a logy (4. díl). *Trestněprávní revue*. 2019, č. 6, s. 123–127.

DRAŠTÍK, Antonín et al. *Trestní zákoník: komentář*. 2015. ISBN 978-80-7478-790-4.

DVOŘÁK, Marek. Phishing, pharming a jejich trestněprávní postih. *Trestněprávní revue*. 2018, č. 4, s. 84–89.

EFRONY, Dan a Yuval SHANY. A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. *American Journal of International Law* [Cambridge Core]. Cambridge University Press, 2018, roč. 112, č. 4, s. 583–657. ISSN 0002-9300.

FENYK, Jaroslav, Tomáš GŘIVNA a Dagmar CÍSAŘOVÁ. *Trestní právo procesní*. 6. vyd. Praha: Wolters Kluwer, 2015. ISBN 978-80-7478-750-8.

FENYK, Jaroslav, Tomáš GŘIVNA a Dagmar CÍSAŘOVÁ. *Trestní právo procesní*. 7. vyd. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-306-0.

FINCK, Michèle, ed. Blockchain Technology. In: FINCK, Michèle, ed. *Blockchain Regulation and Governance in Europe*. Cambridge: Cambridge University Press, 2018, s. 1–33. ISBN 978-1-108-47475-7. DOI: 10.1017/9781108609708.001

FOJT, Dominik. Terorismus v rámci Evropské unie. *Trestněprávní revue*. 2020, č. 1, s. 28–33.

FURNELL, S. M. The Problem of Categorising Cybercrime and Cybercriminals. In: *Survival in the e-economy: proceedings : 2nd Australian Information Warfare & Security Conference*. 2001. Churchlands, W.A.: Edith Cowan University, School of Management Information Systems, We-B Centre, 2001, s. 34–35. ISBN 978-0-7298-0499-8.

GARGULÁK, Michal. Kriminalizace nekonsensuální pornografie v České republice. *Trestněprávní revue*. 2018, č. 2, s. 30–35.

GIBSON, William. *Neuromancer*. 20th anniversary ed. vyd. New York: Ace Books, 2004. ISBN 978-0-441-01203-9.

GOLD, Steve. The rebirth of phreaking. *Network Security*. 2011, č. 6, s. 15-17. ISSN 1353-4858.

GORDON, Sarah. Virus writers: the end of the innocence? In: *10th Annual Virus Bulletin Conference (VB2000), Orlando, FL*. 2000.

GŘIVNA, Tomáš. Trestné činy proti lidské důstojnosti v sexuální oblasti v novém trestním zákoníku. *Bulletin advokacie*. 2009, č. 10, s. 67–72.

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

GUNKEL, David J. *Hacking cyberspace*. Boulder, Colo: Westview Press, 2001. Polemics. ISBN 978-0-8133-3669-5.

HALLEVY, Gabriel. The Criminal Liability of Artificial Intelligence Entities. *SSRN Electronic Journal*. 2010. Dostupné z: doi:10.2139/ssrn.1564096.

HALLEVY, Gabriel. *Liability for crimes involving artificial intelligence systems*. New York: Springer, 2014. ISBN 978-3-319-10123-1.

HAUGELAND, John. *Artificial intelligence: the very idea*. Cambridge, Mass: MIT Press, 1985. ISBN 978-0-262-08153-5.

HERCZEG, Jiří. Několik poznámek k novele trestního zákona č. 141/2007 Sb. *Trestněprávní revue*. 2015, č. 7–8, s. 173–175.

HLAVÁČOVÁ, Kateřina a Oliver CHORVÁT. Přístup orgánů činných v trestním řízení k datům uloženým v cloudu. *Revue pro právo a technologie*. 2016, č. 14, s. 3–24.

HOLOŠKA, Jiří a Marián SVETLÍK ST. Sedm hříchů digitální forenzní analýzy. *Digital Forensic Journal*. 2014, č. 2. ISSN 2336-4769.

CHIESA, Raoul, Stefania DUCCI a Silvio CIAPPI. *Profiling hackers: the science of criminal profiling as applied to the world of hacking*. Boca Raton: Auerbach Publications, 2009. ISBN 978-1-4200-8693-5.

CHRISTOU, George. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. 2016. ISBN 978-1-137-40052-9.

INDEPENDENT HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE. *Ethics Guidelines for Trustworthy AI*. European Commission, 2019.

JENSEN, Eric Talbot. The Tallinn Manual 2.0: Highlights and Insights International Justice: Where We Stand, Where We Fall, and Where We Need to Be. *Georgetown Journal of International Law*. 2016, roč. 48, č. 3, s. 735–778.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Praha: Policejní akademie ČR v Praze: Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0.

JÎRLĂIANU, Silviu. Computer Related Forgery, Between Concept And Reality. *International conference KNOWLEDGE-BASED ORGANIZATION*. 2015, roč. 21.

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

KESSLER, Oliver a Wouter WERNER. Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare International Legal Theory: Symposium: Expertise, Uncertainty, and International Law. *Leiden Journal of International Law*. 2013, roč. 26, č. 4, s. 793–810.

KOLOUCH, Jan. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8.

KONRÁD, Zdeněk et al. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování*. 2015. ISBN 978-80-7380-547-0.

KOPECKÝ, Kamil a René SZOTKOWSKI. Cyberbullying, cyber aggression and their impact on the victim – The teacher. *Telematics and Informatics*. 2017, roč. 34, č. 2, s. 506–517. ISSN 0736-5853.

KORLAM, Gautam. *Password Cracking in the Cloud*. 2012, Department of Computer Science, UC Santa Barbara.

KUCHTA, Josef. Aktuální problémy počítačové kriminality včetně její prevence. *Časopis pro právní vědu a praxi*. 2016, č. 1, s. 5–19.

KULMS, Rainer. Úvod do práva blockchainů. *Obchodněprávní revue*. 2020, č. 1, s. 39-48.

MANKY, Derek. Cybercrime as a service: a very modern business. *Computer Fraud & Security*. 2013, roč. 2013, č. 6, s. 9–13. ISSN 1361-3723.

MCQUADE, Samuel C., ed. *Encyclopedia of cybercrime*. Westport, Conn: Greenwood Press, 2009. ISBN 978-0-313-33974-5.

MIKEŠ, Stanislav. Právo ve věku inteligentních strojů. *Bulletin advokacie*. 2018, č. 4, s. 17–22.

MORGAN, Rodney, Robert REINER a Mike MAGUIRE, eds. *The Oxford handbook of criminology*. 5th ed. vyd. New York, NY: Oxford University Press, 2012. ISBN 978-0-19-959027-8.

MUSIL, Jan. Přestává platit v českém trestním právu princip odpovědnosti za zavinění? *Trestněprávní revue*. 2014, č. 11–12, s. 251–255.

ODEHNALOVÁ, Jana. Ústavnost domovní prohlídky a nedotknutelnost obydlí. *Právní rozhledy*. 2019, č. 8, s. 287–291.

PENG, Sheng-Lung, Souvik PAL a Lianfen HUANG, ed. *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm* [online]. Cham: Springer International Publishing, 2020. Intelligent Systems Reference Library. ISBN 978-3-030-33595-3. Dostupné z: doi:10.1007/978-3-030-33596-0

POLČÁK, Radim, František PÚRY a Jakub HARAŠTA. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8073-7.

PORADA, Viktor a Eduard BRUNA. Digitální svět a dokazování obsahu elektronických dokumentů. *Bezpečnostní technologie, systémy a management*. 2013, č. 3

PORADA, Viktor a Zdeněk KONRÁD. *Metodika vyšetřování počítačové kriminality*. Praha: Policejní akademie České republiky, 1998. ISBN 978-80-85981-75-9.

PORADA, Viktor a Jiří STRAUS. *Kriminalistika: (výzkum, pokroky, perspektivy)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN 978-80-7380-477-0.

RAK, Roman a Viktor PORADA. Vlastnosti digitálních stop a jejich dopady na forenzní šetření. *Soudní inženýrství*. 2005, roč. 16, č. 4, s. 183–192.

RICH, Elaine, Kevin KNIGHT a Shivashankar NAIR B. *Artificial Intelligence*. 3. vyd. Gardners Books, 2004. ISBN 978-0-07-008770-5.

ROGERS, Marcus K. *The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach*. 2005.

SHEMA, Mike. *Hacking web apps: detecting and preventing web application security problems*. Amsterdam; Boston: Syngress, 2012. ISBN 978-1-59749-951-4.

SCHELL, Bernadette H a Clemens MARTIN. *Cybercrime: a reference handbook*. Santa Barbara, Calif.: ABC-CLIO, 2004. ISBN 978-1-85109-683-1.

SIMONATO, Michele. Defence rights and the use of information technology in criminal procedure. *Revue internationale de droit pénal* [Cairn.info]. 2014, roč. 85, č. 1–2, s. 261-310. ISSN 9782749242224.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. ISBN 978-80-7380-720-7.

SMEJKAL, Vladimír a Michal VALÁŠEK. *Co všechno lze falzifikovat v ICT aneb důkazy nejsou vždy důkazy*. Praha: Policejní akademie České republiky, 2018. ISBN 978-80-7251-485-4.

SOKOL, Tomáš a Vladimír SMEJKAL. Postih počítačové kriminality podle nového trestního zákoníku. *Právní rádce*. 2009, roč. XVII, č. 7

SÝKORA, Michal. Trestní postih cyberstalkingu. *Acta Universitatis Carolinae - Iuridica 4*. roč. 2012, č. 4, s. 95–104. ISSN 0323-0619.

ŠÁMAL, Pavel a kolektiv. *Trestní zákoník*. 2. vydání. Praha: C. H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5.

ŠELLENG, Dalibor. K některým aspektům trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 270 trestního zákoníku. *Acta MUP – Právní ochrana duševního vlastnictví*. roč. 2018, č. 2, s. 37–45. ISSN 1804-6932.

TIKK, Eneken. Global Cybersecurity–Thinking About the Niche for NATO. *SAIS Review*. 2010, roč. 30, s. 105–119.

TLAPÁK NAVRÁTILOVÁ, Jana a Ingrid GALOVCOVÁ. Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení? *Bulletin advokacie*. 2019, č. 11, s. 36–39.

TRIEU, Khoa a Yi YANG. Artificial Intelligence-Based Password Brute Force Attacks. *MWAIS 2018 Proceedings*. 2018, č. 39, s. 8.

TULI, Preeti a Priyanka SAHU. System Monitoring and Security Using Keylogger. *International Journal of Computer Science and Mobile Computing*. 2013, roč. 2, č. 3, s. 6. ISSN 2320-088X.

TZEZANA, Roey. High-probability and wild-card scenarios for future crimes and terror attacks using the Internet of Things. *Foresight*. 2017, roč. 19, č. 1, s. 1–14. ISSN 1463-6689.

UNITED NATIONS, ed. *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August-7 September 1990: report*. New York: United Nations, 1991. ISBN 978-92-1-130143-4.

VANTUCH, Pavel. K postihu stalkingu (nebezpečného pronásledování) podle § 354 trestního zákoníku. *Trestní právo*. 2011, (2), 5–13.

VEBER, Jaromír, Zdeněk SMUTNÝ a Ladislav VYSKOČIL. Practice of Digital Forensic Investigation in the Czech Republic and ISO/IEC 27037:2012 [in Czech]. *Acta Informatica Pragensia*. 2015, roč. 4, s. 242–257.

VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo*. 2010, č. 7–8, s. 19–43.

WARREN, Samuel D. a Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review* [JSTOR]. 1890, roč. 4, č. 5, s. 193–220. ISSN 0017811X.

WIENER, Norbert. *The Human Use of Human Beings: Cybernetics and Society*. London: Free Association Books, 1989. ISBN 978-1-85343-075-6.

WINIGER, Bénédict, Håkan ANDERSSON a ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN, eds.*Essential cases on natural causation*. Wien; New York: SpringerWienNewYork,2007. Digest of European tort law v.1.ISBN 978-3-211-36957-9.

ZAVRŠNÍK, Aleš. Cybercrime – Definitional Challenges and Criminological Particularities. *Masaryk University Journal of Law and Technology*. 2009, roč. 2, č. 2, s. 1–29. ISSN 1802-5951.

ZIBNER, Jan. Akceptace právní osobnosti v případě umělé inteligence. *Revue pro právo a technologie*. 2018, roč. 9, č. 17, s. 19–49.

ZIBNER, Jan. Otázky odpovědnosti umělé inteligence za zásah do autorského práva. *Revue pro právo a technologie*. 2019, roč. 10, č. 20, s. 65–90.

Seznam použitých internetových zdrojů

10 Most Notorious Hackers of All Time [online]. 2015 [cit. 03.01.2020]. Dostupné z: https://hacked.com/hackers/

BARLOW, John Perry. A Declaration of the Independence of Cyberspace. In: *Electronic Frontier Foundation* [online]. 20. 1. 2016 [cit. 31.03.2019]. Dostupné z: https://www.eff.org/cyberspace-independence

BEDNARZ, Ann. Profiling cybercriminals: A promising but immature science. *NETWORKWORLD* [online]. 29. listopad 2004 [vid. 2020-01-02]. Dostupné z: https://www.networkworld.com/article/2327820/profiling-cybercriminals--a-promising-but-immature-science.html

BOCETTA, Sam. Has an AI Cyber Attack Happened Yet? In: *InfoQ* [online]. 10. 3. 2020 [cit. 30.08.2020]. Dostupné z: https://www.infoq.com/articles/ai-cyber-attacks/

BRENT, Laura. NATO's role in cyberspace. In: *NATO Review* [online]. 12. 2. 2019 [cit. 20.08.2020]. Dostupné z: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

COPE, James. What's a Peer-to-Peer (P2P) Network? In: *Computerworld* [online]. 8. 4. 2002 [cit. 01.11.2019]. Dostupné z: https://www.computerworld.com/article/2588287/networking-peer-to-peer-network.html

Cyber Attack Trends Analysis Report [online]. Check Point Software Technologies Ltd. Dostupné z: https://www.checkpointdirect.co.uk/media/downloads/check-point-2019-security-report-volume-1.pdf

DELANEY, Darragh. File hosting services and their data leakage risks. In: *Computerworld* [online]. 14. 6. 2011 [cit. 01.11.2019]. Dostupné z: https://www.computerworld.com/article/2470038/file-hosting-services-and-their-data-leakage-risks.html

Digital Evidence Law and Legal Definition. *USLegal, Inc.* [online]. [vid. 2019-11-22]. Dostupné z: https://definitions.uslegal.com/d/digital-evidence/

ENISA. About ENISA – The European Union Agency for Cybersecurity. In: *ENISA* [online] [cit. 05.08.2020]. Dostupné z: https://www.enisa.europa.eu/about-enisa/about-enisa

EUROPEAN COMMISSION a DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS. *Liability for artificial intelligence and other emerging digital technologies.* [online]. 2019 [cit. 30.08.2020]. ISBN 978-92-76-12959-2. Dostupné z: https://op.europa.eu/publication/manifestation_identifier/PUB_DS0319853ENN

European Cybercrime Centre – EC3. In: *Europol* [online] [cit. 07.08.2020]. Dostupné z: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION. *Iocta, Internet Organised Crime Threat Assessment: 2018.* [online]. 2018 [cit. 06.09.2020]. ISBN 978-92-95200-94-4. Dostupné z: http://dx.publications.europa.eu/10.2813/858843

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION. *Iocta, Internet Organised Crime Threat Assessment: 2019.* [online]. 2019. Dostupné z: https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

EVROPSKÁ UNIE. Evropský vyšetřovací příkaz, vzájemná právní pomoc a společné vyšetřovací tým. In: *Portál evropské e-Justice* [online] [cit. 07.03.2020]. Dostupné z: https://e-justice.europa.eu/content_european_investigation_order_mutual_legal_ assistance_and_joint_investigation_teams-92--maximize-cs.do

FRANKENFIELD, Jake. Hacktivism. In: *Investopedia* [online] [cit. 02.01.2020]. Dostupné z: https://www.investopedia.com/terms/h/hacktivism.asp

GREENBERG, Andy. Kevin Mitnick, Once the World's Most Wanted Hacker, Is Now Selling Zero-Day Exploits. *WIRED* [online]. 24. září 2014 [vid. 2020-01-02]. Dostupné z: https://www.wired.com/2014/09/kevin-mitnick-selling-zero-day-exploits/

GROOTERS, Howard J. Territorial Jurisdiction in Cyberspace. *Oregon Review of International Law* [online]. 2002. Dostupné z: https://heinonline.org/HOL/ P?h=hein.journals/porril4&i=5

HAKMEH, Joyce a Allison PETERS. A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet. In: *Council on Foreign Relations* [online] [cit. 19.08.2020]. Dostupné z: https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet

History of the International Association of Penal Law. *Association Internationale De Droit Pénal* [online]. [vid. 2020-01-02]. Dostupné z: http://www.penal.org/en/node/168

CHERTOFF, Michael a Tobby SIMON. The Impact of the Dark Web on Internet Governance and Cyber Security. [online]. 2015 [cit. 01.11.2019]. Dostupné z: https://www.cigionline.org/publications/impact-dark-web-internet-governance-and-cyber-security

Christchurch Call | to eliminate terrorist and violent extremist content online. [cit. 05.02.2020]. Dostupné z: https://www.christchurchcall.com/

INDEPENDENT HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE. *A definition of AI: Main capabilities and scientific disciplines* [online]. European Commission, 2019. Dostupné z: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341

JENKINSON, Gareth. Regulatory Overview of Crypto Mining in Different Countries. *Cointelegraph* [online]. 2019 [cit. 04.09.2020]. Dostupné z: https://cointelegraph.com/news/regulatory-overview-of-crypto-mining-in-different-countries

K obchodování s tzv. převodními tokeny [online]. ČNB, 2018. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/casto-kladene-dotazy/.galleries/stanoviska_a_odpovedi/pdf/k_obchodovani_s_prevodnimi_tokeny.pdf

KAGAN, Julia. Card-Not-Present Fraud Definition. In: *Investopedia* [online] [cit. 08.08.2020]. Dostupné z: https://www.investopedia.com/terms/c/cardnotpresent-fraud.asp

Keyloggers: How they work and how to detect them (Part 1) | Securelist. In: [cit. 02.09.2019]. Dostupné z: https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/

KIDMAN, David a Stephen TURNER. Electronic persons: time for a new legal personality? *New Law Journal* [online]. 2017, Issue 7758 [cit. 30.08.2020]. Dostupné z: https://www.newlawjournal.co.uk/content/electronic-persons-time-new-legal-personality-0

KUKLINCA, Ján a Martin BARTOŇ. Embedovaný odkaz ve světle nové rozhodovací praxe. *EPRAVO.CZ* [online]. 2018 [cit. 02.05.2020]. Dostupné z: https://www.epravo.cz/top/clanky/embedovany-odkaz-ve-svetle-nove-rozhodovaci-praxe-108176.html

MAGDOŇOVÁ, Jana. Na nemocnici v Benešově útočil ruský virus Ryuk. Jermanová odmítá, že by někdo požadoval výkupné. *iRozhlas* [online]. 2020 [cit. 06.09.2020]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/nemocnice-benesov-kyberneticky-utok-ransomware-vykupne-ochrana-osobnich-udaju_2001140615_cha

MATOCHA, Jakub. Virtuální měny a trestní právo. *Právní prostor* [online]. 2016 [cit. 04.09.2020]. Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/virtualni-meny-a-trestni-pravo

MAXWELL, Winston a Christopher WOLF. A Global Reality: Governmental Access to Data in the Cloud. *A Hogan Lovells White Paper* [online]. 2012 [cit. 31.08.2020]. Dostupné z: https://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf

Megaupload sharing site shut down. *BBC News* [online]. 2012 [cit. 01.11.2019]. Dostupné z: https://www.bbc.com/news/technology-16642369

MELL, Peter a Timothy GRANCE. *The NIST Definition of Cloud Computing* [online]. National Institute of Standards and Technology, 2011. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* [online] [cit. 04.09.2020]. Dostupné z: https://bitcoin.org/bitcoin.pdf

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Podvodné e-maily nebo zprávy na sociálních sítích na míru: spear-phishing a jak se před ním chránit* [online]. 3. duben 2020 [vid. 2020-04-26]. Dostupné z: https://nukib.cz/download/publikace/doporuceni/Doporuceni_spear_phishing_2.0.pdf

PLANTERA, Federico. NATO CCDCOE – Expertise and cooperation make our cyber space safer. In: *e-Estonia* [online]. 16. 10. 2018 [cit. 20.08.2020]. Dostupné z: https://e-estonia.com/nato-ccdcoe-expertise-cyber-space-safer/

POLICIE ČR. Kyberkriminalita. *Policie.cz* [online] [vid. 05.02.2020]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx?q=cHJuPTE%3d

POLICIE ČR. Pozor na podvodníky! *Policie.cz* [online]. [vid. 2020-04-03]. Dostupné z: https://www.policie.cz/clanek/pozor-na-podvodniky-346746.aspx

POLICIE ČR. Skimming. *Policie.cz* [online]. [vid. 2019-10-05]. Dostupné z: https://www.policie.cz/clanek/ncoz-skimming.aspx

POLLITT, M. Mark. *Who is SWGDE and what is the history?* [online]. 2003 [cit. 28.02.2020]. Dostupné z: https://www.swgde.org/pdf/2003-01-22%20SWGDE%20History.pdf

PŘÍKAZSKÁ, Lenka a Michal MOHELSKÝ. Současná právní úprava data retention je dle Ústavního soudu ústavně konformní a tedy přípustná. *EPRAVO.CZ* [online]. 2019 [cit. 22.03.2020]. Dostupné z: https://www.epravo.cz/top/clanky/soucasna-pravni-uprava-data-retention-je-dle-ustavniho-soudu-ustavne-konformni-a-tedy-pripustna-110069.html

RAZA, Ali. 10 Most Notorious Hacking Groups. *HackRead* [online]. 20. leden 2016 [vid. 2020-01-02]. Dostupné z: https://www.hackread.com/10-most-notorious-hacking-groups/

Rizikové e-shopy. *Česká obchodní inspekce* [online]. [vid. 2020-04-03]. Dostupné z: https://www.coi.cz/pro-spotrebitele/rizikove-e-shopy/

Section III – Criminal Procedure. *Revue internationale de droit pénal* [Cairn.info]. 2014, roč. 85, č. 3–4, s. 613–618. ISSN 9782749246499.

SCHARRE, Paul. Killer Apps. *Foreign Affairs* [online]. 2020 [cit. 29.08.2020]. ISSN 0015-7120. Dostupné z: https://www.foreignaffairs.com/articles/2019-04-16/killer-apps

Spoofing – what it is and how to defend against it. *Avast* [online]. [vid. 2019-09-15]. Dostupné z: https://www.avast.com/c-spoofing

TAMKIN, Emily. *10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?* [online] [cit. 20.08.2020]. Dostupné z: https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

TEEUW, Wouter B. a Anton VEDDER, ed. *Security Applications for Converging Technologies – Impact on the constitutional state and the legal order* [online]. B.m.: TELEMATICA INSTITUUT, ENSCHEDE. 2008 [vid. 2020-01-01]. Dostupné z: https://pure.uvt.nl/ws/portalfiles/portal/951064/Security_Applications_for_Converging_Technologies_WODC.pdf

TITLBACH, Filip. Česká státní správa je zabezpečená na 20 procent, říká kyberspecialista. *Deník N* [online]. 2019. Dostupné z: https://denikn.cz/224271/studio-n-ceska-statni-sprava-je-zabezpecena-na-20-procent-rika-kyberspecialista

Typosquatting. *UpCounsel* [online]. 2019 [vid. 2019-11-04]. Dostupné z: https://www.upcounsel.com/typosquatting

UN GENERAL ASSEMBLY. *Guidelines for the Regulation of Computerized Personal Data Files* [online]. 1990 [cit. 01.01.2020]. Dostupné z: https://www.refworld.org/docid/3ddcafaac.html

UN GENERAL ASSEMBLY. *Proposed outline and modalities for the further activities of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Background paper prepared by the Secretariat.* [online]. 15. 6 2020. Dostupné z: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Background_paper/A_AC.291_2_E.pdf

Varování před hrozbou kybernetických útoků na nemocnice a jiné významné cíle ČR [online]. Národní úřad pro kybernetickou bezpečnost, 2020. Dostupné z: https://www.nukib.cz/download/uredni_deska/Varovani_NUKIB_2020-04-16.pdf

VAVRA, Shannon. NATO cyber-operations center will be leaning on its members for offensive hacks. In: *Cyberscoop* [online]. 30. 8. 2019 [cit. 20.08.2020]. Dostupné z: https://www.cyberscoop.com/nato-cyber-operations-offensive-hacking-neal-dewar/

VRBÍK, Marek. Regulace open-source P2P platební sítě Bitcoin. *EPRAVO.CZ* [online]. 2014 [cit. 04.09.2020]. Dostupné z: https://www.epravo.cz/top/clanky/regulace-open-source-p2p-platebni-site-bitcoin-93971.html

WEIMANN, Gabriel. *Cyberterrorism. How Real Is the Threat?* [online]. United States Institute of Peace, Special Report 119, 2004. Dostupné z: https://www.usip.org/sites/default/files/sr119.pdf

What is a Botnet? | Preventing Botnet Attacks. In: *Kaspersky* [online] [cit. 28.09.2019]. Dostupné z: https://www.kaspersky.com/resource-center/threats/botnet-attacks

What is a man-in-the-middle attack? *NortonLifeLock* [online]. [vid. 2019-09-22]. Dostupné z: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

Whois Lookup & IP. *Whois.net* [online]. [vid. 2020-02-05]. Dostupné z: https://www.whois.net/

WORI, Okechukwu. Computer Crimes: Factors of Cybercriminal Activities. *International Journal of Advanced Computer Science and Information Technology; Vol 3, No 1 (2014)* [online]. 2014. Dostupné z: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-136

Seznam použitých právních předpisů

Evropská úmluva o ochraně lidských práv ve znění Protokolů č. 11 a 14 s Protokoly č. 1, 4, 6, 7, 12, 13 a 16.

Evropská úmluva o právní ochraně služeb s podmíněným přístupem a služeb tvořených podmíněným přístupem [ÚV L 336/2].

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

Nařízení Evropského parlamentu a Rady č. 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení č. 526/2013 („akt o kybernetické bezpečnosti“) [ÚV L 151/15].

Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti.

Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů.

Směrnice Evropského parlamentu a Rady 2009/110/ES ze dne 16. září 2009 o přístupu k činnosti institucí elektronických peněz, o jejím výkonu a o obezřetnostním dohledu nad touto činností, o změně směrnic 2005/60/ES a 2006/48/ES a o zrušení směrnice 2000/46/ES.

Směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV.

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.

Směrnice Evropského parlamentu a Rady (EU) 2017/541 ze dne 15. března 2017 o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady 2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV.

Směrnice Evropského parlamentu a Rady (EU) 2019/713 ze dne 17. dubna 2019 o potírání podvodů v oblasti bezhotovostních platebních prostředků a jejich padělání a o nahrazení rámcového rozhodnutí Rady 2001/413/SVV.

Úmluva o počítačové kriminalitě. In: *Sbírka mezinárodních smluv České republiky*. 2013, částka 56, s. 10785-10837.

Vyhláška č. 37/1967 Sb., k provedení zákona o znalcích a tlumočnících.

Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.

Zákon č. 141/1961 Sb., o trestním řízení soudním

Zákon č. 36/1967 Sb., o znalcích a tlumočnících

Zákon č. 121/2000 Sb., autorský zákon

Zákon č. 127/2005 Sb., o elektronických komunikacích

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti

Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu

Zákon č. 284/2009 Sb., o platebním styku

Zákon č. 40/2009 Sb., trestní zákoník

Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Zákon č. 370/2017 Sb., o platebním styku

Seznam použité judikatury

Nález ÚS ze dne 20. 8. 2013, sp. zn. I. ÚS 1428/13 (N 150/70 SbNU 389).

Nález ÚS ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17.

Rozsudek SDEU ze dne 8. 4. 2014, spojené věci C-293/12 a C-594/12 *Digital Rights Ireland a další*.

Rozsudek ze dne 13. 2. 2014, Nils Svensson a další, C-466/12.

Rozsudek ze dne 8. září 2016, GS Media BV, C-160/15.

Rozsudek ze dne 7. srpna 2018, Land Nordrhein-Westfalen, C-161/17.

Stanovisko Nejvyššího soudu ze dne 30. 1. 2013, sp. zn. Tpjn 300/2012, č. 3/2013 Sb. rozh. obč.

Stanovisko Nejvyššího státního zastupitelství ze dne 26. 1. 2015, sp. zn. 1 SL 760/2014, ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek.

Usnesení Evropského parlamentu ze dne 16. února 2017 obsahující doporučení Komisi o občanskoprávních pravidlech pro robotiku (2015/2103(INL)), [ÚV C 252/239].

Usnesení Krajského soudu v Praze ze dne 29. 6. 2017, sp. zn. 9To 227/2017-379.

Usnesení Nejvyššího soudu ze dne 21. 5. 2009, sp. zn. 11 Tdo 349/2009.

Usnesení Nejvyššího soudu ze dne 15. 12. 2010, sp. zn. 5 Tdo 1312/2010.

Usnesení Nejvyššího soudu ze dne 8. 9. 2011, sp. zn. 8 Tdo 1082/2011.

Usnesení Nejvyššího soudu ze dne 27. 2. 2013, sp. zn. 8 Tdo 137/2013.

Usnesení Nejvyššího soudu ze dne 29. 5. 2013, sp. zn. 5 Tdo 271/2013.

Usnesení Nejvyššího soudu ze dne 7. 3. 2019, sp. zn. 11 Tdo 1428/2018.

Usnesení Ústavního soudu ze dne 28. 3. 2002, sp. zn. IV. ÚS 2/02 (U 11/25 SbNU 385).

Usnesení Ústavního soudu ze dne 3. 10. 2013, sp. zn. III. ÚS 3812/2012 (U 10/71 SbNU 573).

Usnesení Ústavního soudu ze dne 15. 2. 2017, sp. zn. II. ÚS 4211/16.

Usnesení SDEU ze dne 21. října 2014, BestWater International GmbH, C-348/13.

Seznam ostatních zdrojů

Důvodová zpráva k zákonu č. 141/2014 Sb., č. 141/2014 Dz.

Důvodová zpráva k zákonu č. 253/2018 Sb., sněmovní tisk 752/0.

Důvodová zpráva k zákonu č. 287/2018 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony, č. 287/2018 Dz.

Návrh nařízení Evropského parlamentu a Rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech 2018/0108/COD.

Octopus 2019 „Cooperation against Cybercrime“, 20.–22. November 2019, Palais de l'Europe, Council of Europe, Strasbourg, France.

Salvadorská deklarace o komplexních strategiích pro globální výzvy: Prevence kriminality a systémy trestní justice a jejich vývoj v měnícím se světě.

Sdělení Ministerstva zahraničních věcí č. 104/2013 Sb.m.s., o sjednání Úmluvy o počítačové kriminalitě.

Společné sdělení Evropskému parlamentu a Radě ze dne 13. 9. 2017 „Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU“.

Technická norma ISO/IEC 27037:2012 (Informační technologie – Bezpečnostní techniky – Směrnice pro identifikaci, sběr, akvizici a uchovávání digitálních důkazů).

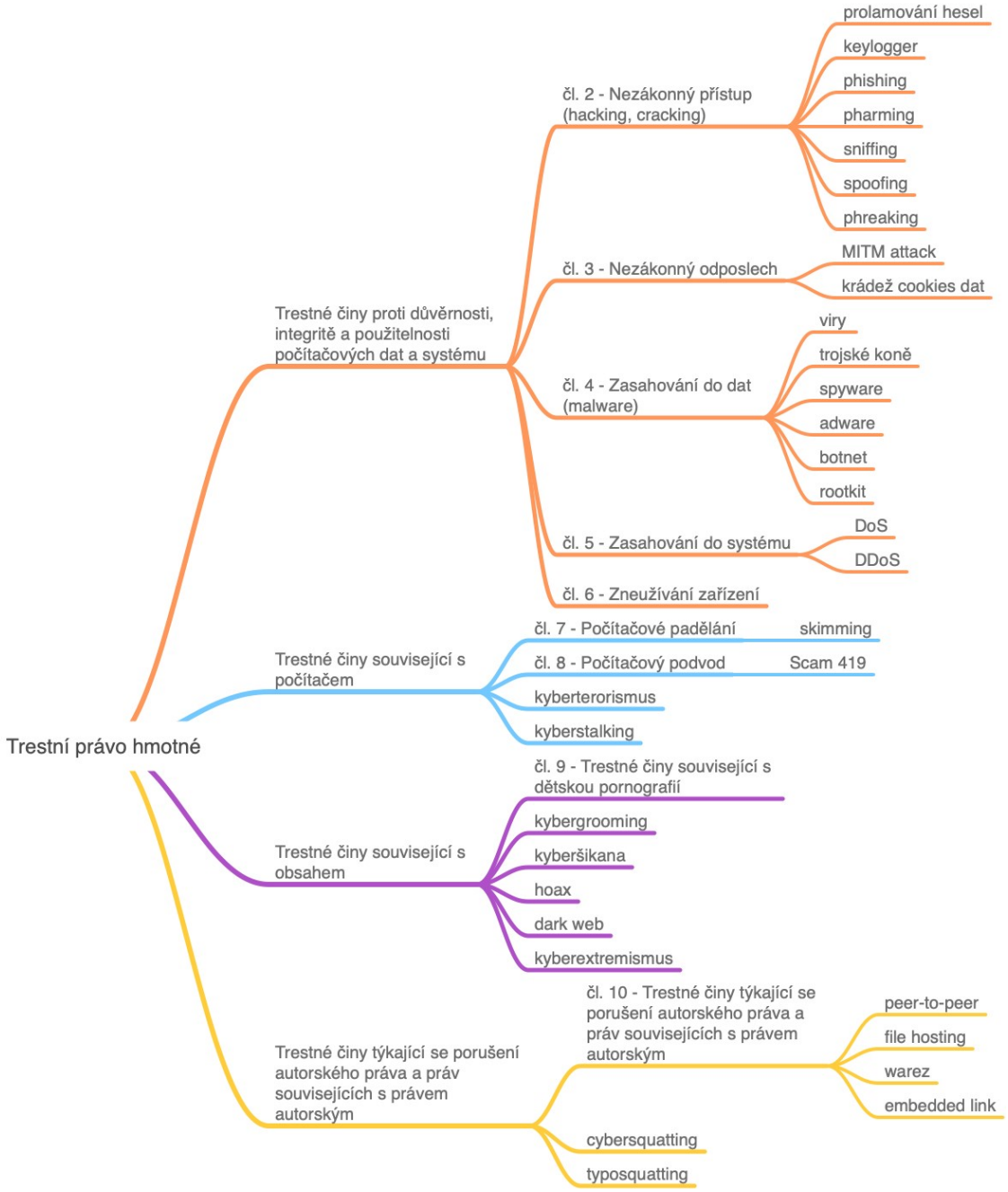
PŘÍLOHY

Seznam příloh

Příloha 1 Schéma kyberútoků I

Příloha 2 Kybernetické trestné činy v TZ II

Příloha 1 Schéma kyberútoků



Příloha 2 Kybernetické trestné činy v TZ

§	Trestný čin	Objekt	Objektivní stránka	Subjekt	Subjektivní stránka	Následek	Předmět útoku	Souběh	Úmluva o počítačové kriminalitě	Útoky
§ 182	porušení tajemství dopravovaných zpráv	ochrana tajemství dopravovaných zpráv	porušení tajemství datové, textové, (…) zprávy posílané prostřednictvím sítě elektronických komunikací, nebo neveřejného přenosu počítačových dat	obecný	úmysl	poruchový	datová zpráva, přenos počítačových dat	možný s § 329, § 330	Neoprávněné zachycení informací (čl. 3)	sniffing
§ 183	porušení tajemství listin a jiných dokumentů uchovávaných v soukromí	ochrana listovního tajemství a tajemství jiných písemností, záznamů a dokumentů uchovávaných v soukromí	porušení tajemství listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu, počítačových dat	obecný	úmysl	poruchový	listina nebo jiná písemnost uchovávaná v soukromí	možný s § 329, § 330	Neoprávněné zachycení informací (čl. 3)	sniffing
§ 192	výroba a jiné nakládání s dětskou pornografií	ochrana mravního vývoje dětí a ochrana před jejich sexuálním zneužíváním	přechovávání pornografického díla, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, získání přístupu k dětské pornografii, výroba, dovezení (…), kořistění	obecný	úmysl	poruchový	dítě (osoba mladší 18 let)	možný s § 201	Trestné činy související s dětskou pornografií (čl. 9)	šíření závadného obsahu, sexting
§ 193	zneužití dítěte k výrobě pornografie	ochrana zdravého mravního vývoje děti a ochrana před jejich zneužíváním k výrobě pornografických děl	přimění, zjednání, nájem, zlákání, svedení či zneužití dítěte k výrobě pornografického díla nebo kořistění z účasti dítěte na takovém pornografickém díle	obecný	úmysl	poruchový	dítě (osoba mladší 18 let)	možný s § 185, § 186, § 187	Trestné činy související s dětskou pornografií (čl. 9)	revenge porn
§ 193a	účast na pornografickém představení	ochrana zdravého mravního vývoje dětí a ochrana před jejich zneužíváním v podobě aktivní účasti na pornografickém představení	účast na pornografickém představení nebo jiném obdobném vystoupení, ve kterém účinkuje dítě	obecný	úmysl	poruchový	dítě (osoba mladší 18 let)	vyloučen s § 191, § 192 a § 193	Trestné činy související s dětskou pornografií (čl. 9)	šíření závadného obsahu

§ 193b	navazování nedovolených kontaktů s dítětem	ochrana mravního vývoje dětí a ochrana před jejich sexuálním zneužíváním	návrh setkání dítěti mladšímu patnácti let v úmyslu spáchat některý z uvedených trestných činů	obecný	úmysl	ohrožovací	dítě mladší patnácti let	vyloučen s § 191, § 192 a § 193	Trestné činy související s dětskou pornografií (čl. 9)	kybergrooming
§ 209	podvod	ochrana majetkových práv bez ohledu na formu vlastnictví	obohacení se tím, že pachatel uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti	obecný	úmysl	poruchový	majetkové právo	možný s § 233 odst. 2 alinea 2, s § 270	Podvod související s počítači (čl. 8)	phishing, pharming, spear phishing,
§ 230 (1)	neoprávněný přístup k počítačovému systému a nosiči informací	ochrana před neoprávněným vniknutím do počítačového systému	překonání bezpečnostního opatření a zároveň s tím získání neoprávněného přístupu k počítačovému systému	obecný	úmysl	poruchový	počítačový systém	vyloučen s § 181, § 207, § 228	Nezákonný přístup (čl. 2)	hacking (prolamování hesel, keylogger, phishing, pharming, sniffing, spoofing, phreaking)
§ 230 (2) (a)	neoprávněný přístup k počítačovému systému a nosiči informací	ochrana dat před neoprávněnou manipulací s nimi	získání neoprávněného přístupu k počítačovému systému a zároveň neoprávněné užití dat	obecný	úmysl	poruchový	počítačový systém, nosič informací, data	možný s § 230 (1), vyloučen s § 264 odst. 2, § 267 odst. 2	Zasahování do dat (čl. 4)	malware, hacking, DoS, DDoS
§ 230 (2) (b)	neoprávněný přístup k počítačovému systému a nosiči informací	ochrana dat před neoprávněnou manipulací s nimi	získání neoprávněného přístupu k počítačovému systému a zároveň vymazání či jiné poškození dat	obecný	úmysl	poruchový	počítačový systém, nosič informací, data	možný s § 230 (1), vyloučen s § 264 odst. 2, § 267 odst. 2	Neoprávněné zasahování do dat (čl. 4)	malware, hacking, DoS, DDoS
§ 230 (2) (c)	neoprávněný přístup k počítačovému systému a nosiči informací	ochrana dat před jejich falšováním	získání neoprávněného přístupu k počítačovému systému a zároveň padělání nebo pozměnění dat	obecný	úmysl	poruchový	data	možný s § 230 (1), vyloučen s § 264 odst. 2, § 267 odst. 2	Počítačové padělání (čl. 7)	malware, hacking
§ 230 (2) (d)	neoprávněný přístup k počítačovému systému a nosiči informací	ochrana počítačového systému před neoprávněnou manipulaci a zájem na jeho řádném fungování	získání neoprávněného přístupu k počítačovému systému a zároveň vložení dat do systému či jiný zásah do softwaru	obecný	úmysl	poruchový	počítačový systém, nosič informací, data	možný s § 230 (1), vyloučen s § 264 odst. 2, § 267 odst. 2	Zasahování do systému (čl. 5)	malware, DoS, DDoS

§ 231 (1) (a)	opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	ochrana společnosti a osob před možným ohrožením vyplývajícím z nekontrolovaného opatření a přechovávání zařízení, nástrojů a prostředků	vyrobení, uvedení do oběhu, dovoz, vývoz, průvoz, nabídka, zprostředkování, prodej nebo jiné zpřístupnění, sobě nebo jinému opatření nebo přechovávání zákonem specifikovaného přístupového zařízení a hesla, pomocí nichž lze získat neoprávněný přístup k počítačovému systému nebo jeho části	obecný	úmysl	poruchový	zařízení, nebo jeho součást, postup, nástroj nebo jakýkoli jin prostředek, včetně počítačového programu, počítačové heslo, kód, data, postup a jiný prostředek	souběh s § 182 (1 (b) (c) a § 230 (1) (2) možný pouze v případě, že je ohrožení způsobené přechováváním přístupových zařízení širší než samotná porucha způsobená trestným činem	Zneužívání zařízení (čl. 6)	password crackers, sniffing, MITM attack a další
§ 232	poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti	ochrana dat a technického či programového vybavení počítače (jiného technického zařízení pro zpracování dat) před nedbalostním poškozovacím jednáním	zničení, poškození, pozměnění dat nebo učinění dat neupotřebitelnými, či učinění zásahu do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat	obecný	hrubá nedbalost	poruchový	data nebo programové vybavení počítače	vyloučen s § 221	Zasahování do dat (čl. 4)	malware, hacking, DoS, DDoS
§ 234	neoprávněné opatření, padělání a pozměnění platebního prostředku	ochrana platebního prostředku a ochrana řádného fungování celého platebního styku	opatření, zpřístupnění, příjem nebo přechovávání platebního prostředku jiného	obecný	úmysl	poruchový	platební prostředek	možný s § 205	Počítačové padělání (čl. 7)	skimming
§ 270	porušení autorského práva a práv souvisejících s právem autorským a práv k databázi	ochrana duševní činnosti	neoprávněný zásah nikoli nepatrný do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi	obecný	úmysl	poruchový	autorské právo a právo související s právem autorským a právo k databázi	možný s § 248 odst. 1, § 251, § 261, dále i s § 209	Trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským (čl. 10)	peer-to-peer, file hosting, warez, embedded link, cybersquatting, typosquatting

§ 311 (1) (a) (e)	teroristický útok	ochrana ústavního zřízení a obranyschopnosti České republiky, demokratických principů, na nichž je republika založena, základní hospodářské struktury státu, života a zdraví obyvatel	(a) zničení nebo poškození ve větší míře telekomunikačního nebo počítačového systému, (e) provedení útoku proti počítačovému systému spočívající ve vložení dat do počítačového systému nebo na nosič informací anebo vymazání nebo jiné zničení, poškození, změnění nebo potlačení dat uložených v počítačovém systému nebo na nosiči informací, snížení jejich kvality nebo učinění jich neupotřebitelnými	obecný	úmysl	poruchový	počítačový nebo telekomunikační systém	možný s § 140, vyloučen s § 272, § 273. §290, § 291, § 292, § 309	Trestné činy související s počítačem	kyberterorismus
§ 354	nebezpečné pronásledování	ochrana nerušeného mezilidského soužití	dlouhodobé pronásledování jiného, které je prováděno v taxativně stanovených formách jednání, které jsou způsobilé v jiném vzbudit důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých	obecný	úmysl	poruchový	člověk	možný s § 171, § 178, § 184, § 228, § 358, § 302, § 353	Trestné činy související s počítačem	kyberstalking

NÁZEV DIPLOMOVÉ PRÁCE V ČESKÉM JAZYCE

Kriminalizace útoků na informační systémy

ABSTRAKT

Kyberkriminalita představuje stále větší nebezpečí pro lidskou společnost. Hlavním cílem této práce je zjistit, jaké útoky na informační systémy představují hrozbu pro stát a zda představují nové technologické trendy v oblasti útoků na informační systémy výzvu pro současnou českou právní úpravu v oblasti trestního práva. Metodologie se napříč touto prací různí. K naplnění cíle práce je použita především analytická metoda spolu se syntézou. V některých částech je pak užíván přístup empirický.

V úvodní části práce jsou vysvětleny klíčové instituty v oblasti kyberkriminality a mezinárodní instrumenty pro boj proti kyberkriminalitě. Nejvýznamnějším dokumentem je Úmluva Rady Evropy o počítačové kriminalitě. Stěžejní část práce je věnována úskalím současné české právní úpravy v souvislosti s kyberútoky. Závěrečná část práce se zabývá aktuálními technologickými trendy, jako je umělá inteligence, cloudová úložiště, virtuální měny a internet věcí, které hrají významnou roli v oblasti útoků na informační systémy.

Současná česká právní úprava zareagovala na stoupající tendence kyberkriminality, a proto byly zavedeny nové druhy trestných činů. Umělá inteligence představuje především problém z hlediska odpovědnosti za způsobený trestný čin. Cloudová úložiště vytvářejí výzvu v oblasti vyšetřování trestných činů, konkrétně zajišťování důkazů. Kryptoměny mohou velmi dobře posloužit k ukrytí peněz získaných z trestné činnosti. Propojení všech věcí v rámci internetu věcí vytváří zranitelné struktury, které se mohou stát terčem útoku. Přestože současná právní úprava dostačuje, je rozvoj technologií tak turbulentní, že bude v blízké době nutné přijmout nový právní rámec. Zároveň je na místě zvýšit zabezpečení počítačových systému, a to jak na úrovni státu, tak na úrovni samotných uživatelů.

KLÍČOVÁ SLOVA

kyberkriminalita, kyberprostor, kyberútok

NÁZEV DIPLOMOVÉ PRÁCE V ANGLICKÉM JAZYCE

The Criminalization of Cyberattacks on Information Systems

ABSTRACT

Cybercrime represents an increasing danger to human society. The main aim of this thesis is to find out which attacks on information systems pose a threat to the state and whether new technological trends represent a challenge for the current Czech legislation in the field of criminal law. The methodology varies across this thesis. The analytical method together with the synthesis is used to fulfil the aim. In some parts, an empirical approach is used.

The introductory part of the thesis explains the key institutes in the field of cybercrime and international instruments for combating cybercrime. The most important document is the Council of Europe Convention on Cybercrime. The main part of the thesis is devoted to the difficulties of current Czech legislation in connection with cyberattacks. The final part of the thesis deals with current technological trends, such as Artificial Intelligence, Cloud Computing, Cryptocurrencies and the Internet of Things, which play an important role in the field of attacks on information systems.

The current Czech legislation has responded to the growing tendency of cybercrime, and therefore new types of criminal offenses have been introduced. Artificial Intelligence is primarily a problem in terms of liability for the crime. Cloud Computing poses a challenge in criminal investigations, specifically in securing evidence. Cryptocurrencies can very well serve to hide money obtained from crime. The interconnection of all things within the Internet of Things creates vulnerable structures that can be attacked. Although the current legislation is sufficient, the development of technology is so turbulent that a new legal framework will need to be adopted in the near future. At the same time, it is appropriate to increase the security of computer systems, both at the state level and at the level of the users themselves.

KEYWORDS

cybercrime, cyberspace, cyberattack