Univerzita Karlova v Praze

Právnická fakulta

Jan Čikovský

INTERNETOVÁ A POČÍTAČOVÁ KRIMINALITA

Diplomová práce

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

Katedra: **Katedra trestního práva**

Datum vypracování práce (uzavření rukopisu): **21. října 2013**

Prohlášení

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, a to za použití zdrojů a literatury v práci uvedených.

Prohlašuji, že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze dne 21. října 2013

_____

Jan Čikovský

Poděkování

Děkuji doc. JUDr. Tomášovi Gřivnovi, Ph.D. za odborné vedení této práce, jeho cenné podněty, připomínky a rady.

Obsah

ÚVOD

Téma počítačové a internetové kriminality se v posledních desetiletích stává stále aktuálnějším. Rozšiřující se technické možnosti spočívající ve využití prvků moderních informačních technologií přinášejí obrovský užitek ve všech oborech lidské činnosti. Do velkého množství běžně rozšířených a dnes už i velice levných a dostupných předmětů jsou implementovány mikroprocesory provádějící početní operace s daty, čímž zařízení výpočetní techniky - nejen počítače, ale i další spotřební elektronika - prostupují do každodenního života jedinců.[1] Prudký rozvoj telekomunikačních technologií a jejich pozvolné splývání s přístroji výpočetní techniky umožňuje komunikaci uživatelů těchto přístrojů mezi sebou navzájem, což užitek pro společnost jen podtrhuje. Nejen prostředí Internetu nabízí uživatelsky poměrně jednoduchý způsob, jak i osoby s relativně nízkým povědomím o oboru informačních technologií mohou snadno získávat, využívat a šířit informace v míře, která ještě před několika lety byla nemyslitelná. Lze říci, že každým rokem se přibližujeme k naplnění vize o tzv. *informační dálnici* v podobě, v jaké ji celosvětově proslavil již v roce 1995 Bill Gates. Ve svém díle „Informační dálnice“ tímto pojmem Gates popisuje koncept, dle něhož propojením všech moderních technologií vznikne komukoliv, kdekoliv a kdykoliv dostupná masa informací, včetně zábavy a nových způsobů komunikace.[2]

Je možné polemizovat s tím, zdali dnes již informační dálnice existuje či nikoliv, je ale nesporné, že v digitálním věku přicházejí nová paradigmata a vzniká tzv. *informační společnost*, která na informační technologie klade takový důraz, až se na nich stává závislá, a do jisté míry právě z tohoto důvodu i zranitelná. Nepatrná škoda způsobená na některých elementech informační infrastruktury se může projevit jako závažná újma pro celou společnost. Některými způsoby je možné nepozorného uživatele výpočetní techniky velmi snadno poškodit. Proto je nutné, aby do informační svobody, kdysi bezbřehé, zasahovalo právo a bylo schopné účinně, tj. soukromoprávními i veřejnoprávními prostředky, chránit zájmy celé společnosti stejně jako soukromá práva jednotlivců. To vše samozřejmě při zachování úcty k základním lidským právům a svobodám a s ohledem na ochranu osobnosti jednotlivce.

---

[1] Význam mikroprocesoru v moderních technologiích a jeho rozšíření do domácností přehledně shrnuje článek TIŠNOVSKÝ, P. *Jak se zrodil procesor* [online]. [citováno dne 9. října 2013]. Dostupný z www: http://www.root.cz/clanky/jak-se-zrodil-procesor/

[2] Nutno podotknout, že Gates tehdejší Internet za informační dálnici nepovažoval, ale považoval jej za její „nejbližší aproximaci“. Blíže viz GATES, Bill. *The road ahead: completely revised and up-to-date*. Druhé vydání. London: Penguin Books, 1996.

Nutno ovšem podotknout, že právo je - a navzdory všem snahám i vždy bude - pro svůj obecně normativní charakter v tomto nelehkém poslání pozadu za realitou. Zejména v trestněprávní oblasti existuje tak velké množství stále se vyvíjejících způsobů páchání trestné činnosti, že je velmi těžké je všechny náležitě předem popsat tak, aby byla konkrétní společensky škodlivá jednání s ohledem na zásadu *nulla crimen sine lege* subsumovatelná pod danou obecnou právní normu. Není ovšem nutné pro nové způsoby páchání trestné činnosti vytvářet nové skutkové podstaty, pokud na ně lze aplikovat skutkové podstaty stávající. Počítačová a internetová kriminalita se tak může projevovat jako některý ze širokého spektra „klasických" trestných činů.[3] Speciálně pro postižení této oblasti kriminality byly při rekodifikaci trestního práva hmotného do TZ zahrnuty zcela nové tři skutkové podstaty.[4]

Internetová a počítačová kriminalita se dále vyznačuje specifiky i v procesně trestněprávní oblasti a též specifiky vyšetřování. Pachatele je obvykle obtížné identifikovat, je náročné legálními prostředky dokázat jeho zavinění, mnohdy může být pachatel zcela mimo místní působnost orgánů činných v trestním řízení a je nutné naplno využít všech možností mezinárodní spolupráce. Pro vyšetřování tohoto druhu kriminality je nutné využívat znalosti nejen z oboru trestního práva, ale i jiných právních disciplín, a též je nutné vycházet z poznatků specificky technických oborů.

V průběhu roku 2013 byly v České republice projednávány dvě významné právní normy související s internetovou a počítačovou kriminalitou. První ze zmíněných norem je Úmluva o počítačové kriminalitě,[5] což je mezinárodní smlouva Českou republikou podepsaná již v roce 2005, avšak k jejíž ratifikaci dochází až letos. Druhou normou

[3] Například porušení tajemství dopravovaných zpráv dle § 182 TZ, pomluva dle § 184 TZ, podvod dle § 209 TZ, trestné činy proti průmyslovým právům a proti autorskému právu dle § 268-271 TZ, nebezpečné vyhrožování dle § 353 TZ, šíření poplašné zprávy dle § 357 TZ a podobně. V některých případech může vzniknout otázka, zdali daná trestná činnost ještě spadá pod počítačovou či internetovou kriminalitu. Blíže se vysvětlení těchto pojmů a jejich kategorizaci budu věnovat v příští kapitole.

[4] Konkrétně se jedná o tři skutkové podstaty zařazené do hlavy páté, popisující trestné činy proti majetku. Jsou to trestné činy neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 TZ), opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ) a poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZ). Budou rozebrány v 5. kapitole.

[5] Úmluva Rady Evropy č. 185 ze dne 23. 11. 2001 o počítačové kriminalitě. Dostupná také z http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, český překlad srov. Sněmovní tisk č. 890, 6. volební období. Okolnosti ratifikace této smlouvy v České republice, stejně jako její jednotlivá ustanovení, budou rozebrány ve 4. kapitole této práce.

je připravovaný zákon o kybernetické bezpečnosti,[6] jehož paragrafové znění bylo dne 15. 4. 2013 Národním bezpečnostním úřadem rozesláno do mezirezortního připomínkového řízení a návrh tohoto zákona byl dne 8. 7. 2013 předložen vládě. Vzhledem k probíhajícímu legislativnímu (resp. nedávnému ratifikačnímu) procesu u těchto dvou norem bude má práce zaměřena zejména na *trestnou činnost ohrožující kybernetickou bezpečnost*, čímž rozumím především trestnou činnost odpovídající skutkovým podstatám popsaným v článcích 2 - 6 Úmluvy o počítačové kriminalitě. Cílem práce je charakterizovat zejména tuto skupinu internetové a počítačové kriminality, posoudit soulad její vnitrostátní úpravy s požadavky plynoucími z Úmluvy o počítačové kriminalitě a zhodnotit dopad chystaného zákona o kybernetické bezpečnosti na tuto oblast.

Diplomová práce začíná vymezením základních pojmů v první kapitole. Druhá kapitola naznačí některé složitější filosoficko-právní problémy, k nimž patří například oprávněnost a užitečnost zásahů státní moci do práv a svobod jednotlivců pro účely vymáhání a kontroly hmotněprávních povinností nebo problematika tzv. distančních deliktů. Zmíněné problémy, kterými se budu zabývat (aniž bych však měl ambici tyto pomyslné gordické uzle jednou provždy rozetnout a ohromit tak celosvětovou právní vědu), jsou pro počítačovou a zejména internetovou kriminalitu velice výstižné. Ve třetí kapitole bude popsána samotná trestná činnost ohrožující kybernetickou bezpečnost, avšak nemohu opomenout a alespoň letmo nezmínit i jinou trestnou činnost spadající pod pojmy internetová a počítačová kriminalita - té ale nebude s ohledem na snahu o dodržení standardního rozsahu diplomové práce věnována taková pozornost. Čtvrtá kapitola shrnuje zásadní evropské i mezinárodní instrumenty upravující internetovou a počítačovou kriminalitu. V páté kapitole čtenář nalezne hmotněprávní způsoby postihu trestné činnosti uvedené v kapitole třetí, a dále zhodnocení souladu českého práva s požadavky plynoucími z mezinárodních a evropských dokumentů uvedených v kapitole čtvrté. Zde se pokusím vyložit a utřídit jednotlivé trestné činy sem spadající a zkombinovat přitom vědomosti technické povahy s právními poznatky. V závěrečné kapitole se budu zabývat trestněprávními důsledky vyplývajícími z chystaného zákona o kybernetické bezpečnosti a shrnout vliv tohoto právního předpisu na boj s počítačovou a internetovou kriminalitou.

---

[6] *Návrh zákona o kybernetické bezpečnosti.* Národní bezpečnostní úřad, 2013. Dostupné také z www: http://www.nbu.cz/cs/aktuality/1398-navrh-zakona-o-kyberneticke-bezpecnosti-byl-predlozen-vlade-ceske-republiky/ [citováno dne 9. října 2013] Trestněprávní souvislosti tohoto zákona budou probrány v 6. kapitole této práce.

Jak jsem naznačil v této úvodní kapitole, budu mít vždy na zřeteli zejména trestnou činnost ohrožující kybernetickou bezpečnost. Právě toto téma totiž považuji v současnosti za aktuální.

1. VÝKLAD ZÁKLADNÍCH POJMŮ

Pro další výklad je nutné nejprve popsat základní pojmy související s počítačovou a internetovou kriminalitou a s kybernetickou bezpečností. Ačkoliv se jedná se o pojmy v běžné mluvě často používané, trvalo poměrně dlouhou dobu, než se právu podařilo definovat jejich obecně přijímané vymezení.[7] Nesprávným používáním pojmů hrozí jejich záměna. Často se zaměňují například výrazy informace a data, nebo počítačová, internetová a kybernetická kriminalita.

Definic je u některých pojmů nepřeberné množství, vybírám proto jen ty nejdůležitější z nich, pokouším se uvádět též i legální definice, tj. takové, které jsou obsaženy ve vnitrostátních nebo mezinárodních právních normách, resp. v technických normách.

1.1 Informace, data a počítačová data

Pojmy informace a data bývají často zaměňovány nebo slučovány. Jejich význam však není identický. *Informací* je dle technické normy ČSN ISO/IEC 2382-1[8] *„určitý poznatek, týkající se jakýchkoliv objektů, např. fakt, událostí, věcí, procesů nebo myšlenek, včetně pojmů, který má v daném kontextu specifický význam"*. Informace je subjektivně zabarvená, závislá na okolnostech, neboť její význam je patrný jen v kontextu a změní-li se kontext, může se změnit i význam informace. Naproti tomu *data* jsou objektivní a mohou, ale nemusí mít význam vůbec žádný. Pokud se ale data zpracují tak, že se zařadí data do kontextu a budou doplněna o význam pochopitelný lidem, stanou se data informacemi.[9] A naopak, zpětným procesem lze informaci formalizovat do podoby dat vhodných pro komunikaci, interpretaci nebo další zpracování. Všechny informace jsou tedy daty, ale data se nemusejí nutně stát informacemi.[10] Účelem informací je organizovat prvky do systematických celků a snižovat tak entropii - neurčitost, nejistotu, obecnou rozkladnou tendenci.[11] Lze tedy

[7] Ovšem ve srovnání s vývojem některých klasických právních pojmů a právních institutů, jejichž definice hledaly svou formulaci někdy i v řádech staletí, lze ustálení pojmosloví v oblasti práva informačních technologií za několik desetiletí hodnotit jako velmi rychlé.

[8] ČSN ISO/IEC 2382-1:1998. *Informační technologie - Slovník - Část 1: Základní termíny*. Praha, Český normalizační institut, 1998. Technické normy nejsou obecně závazné a mají povahu doporučení.

[9] NOVOTNÝ, O., VOKOUN, R., ŠÁMAL, P. a kol. *Trestní právo hmotné. Zvláštní část*. 6. vydání, Praha, Wolters Kluwer ČR, a. s., 2010, str. 211.

[10] POŽÁR, J. a kol. *Základy teorie informační bezpečnosti.* Praha, Vydavatelství Policejní akademie České republiky, 2007, str. 10 a násl.

[11] POLČÁK, R. Autoritativní regulace kyberprostoru a legitimita trestního práva. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

shrnout, že data jsou poznatky určené k dalšímu zpracování, čímž z nich lze extrahovat informace.

Závěr, že data je vhodné dále zpracovat, zatímco informace zpracované již jsou, dobře poslouží k definování pojmu *počítačová data*. Počítačová data jsou zpracovatelná pomocí počítačového systému. Obdobný závěr je uveden např. v čl. 1 Úmluvy o počítačové kriminalitě, dle kterého znamenají počítačová data *„jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.“*

1.2 Systém, informační systém a počítačový systém, počítačová síť

Systém je obecně vzato množina prvků a vazeb mezi nimi, přičemž prvky jsou spolu v systému spojeny logickými vazbami a interagují spolu navzájem. V *informačním systému* jsou tyto vazby definovány jako informace, a prvky jako místa, ve kterých jsou tyto informace zpracovávány. Prvky informačního systému jsou například lidé, hardware nebo software; vazby jsou přenosové cesty, kabely a podobně.[12] Účelem informačního systému je zpracování dat. Informační systém vůbec nemusí být napojen na moderní technická zařízení a může existovat v ryze papírové podobě. Jako příklad takového informačního systému lze uvést kartotéku či telefonní seznam.

V informačních systémech dochází ke zpracování dat. V případě, že informační systém bude data zpracovávat automaticky, bez přímého lidského zásahu, bude se jednat o *počítačový systém*. Obecně je počítačový systém zařízení určené k automatickému zpracování digitálních dat, pročež počítačový systém využívá technická a programová vybavení, tj. hardware a software. Klasická definice uvádí, že počítačový systém je *„jakékoli zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat.“*[13] Pojem počítačový systém je zvláště důležitý, protože se s ním operuje ve skutkových podstatách uvedených v § 230 - 232 TZ.

Počítačovým systémem se nerozumí jen to, co český jazyk označuje jako počítač, resp. osobní počítač (PC). Zmíněná definice pokrývá i širokou škálu rozličných zařízení moderní

---

[12] POŽÁR, J. a kol. *Základy teorie informační bezpečnosti.* Praha, Vydavatelství Policejní akademie České republiky, 2007, str. 16.

[13] NOVOTNÝ, O., VOKOUN, R., ŠÁMAL, P. a kol. *Trestní právo hmotné. Zvláštní část*. 6. vydání, Praha, Wolters Kluwer ČR, a. s., 2010, str. 211.

techniky, včetně notebooků, mobilních telefonů, GPS navigací, smartphonů, ale například i vozidel či některých hudebních nástrojů.[14] Všechna uvedená zařízení jsou počítačovými systémy a požívají tak specifické právní ochrany dle citovaných ustanovení.

Skupina navzájem propojených počítačových systémů tvoří *počítačovou síť*.[15] Počítačové systémy mohou být propojeny pomocí kabelů, ale též bezdrátově (tzv. Wi-Fi) či kombinovaně. Podle geografického rozsahu existují sítě lokální (tzv. LAN) či rozlehlé (WAN). Celosvětově rozšířenou sítí je Internet propojující množství sítí, které používají stejné protokoly (tj. protokol TCP/IP).[16]

1.3 Internet a kybeprostor

Internet lze s jistou výhradou chápat jako informační systém dle výše uvedené definice. Mezi prvky Internetu patří fyzické i právnické osoby (např. uživatelé, poskytovatelé služeb) a věci (technické a programové vybavení). Čím se ale Internet od běžných automatizovaných informačních systémů liší, je jistá omezená celistvost: jednotlivé prvky Internetu netvoří žádnou konkrétní instituci, která by mohla být subjektem práva.[17] To je dáno historickým vývojem Internetu.

Internet vznikal postupným propojováním jednotlivých počítačových systémů a počítačových sítí bez ohledu na právo. Rozvíjel se bez zásahů státní moci, svobodně, spontánně a nekontrolovatelně. Předchůdci Internetu, sítě ARPANET a MILNET, se sice vyvíjely (již od konce šedesátých let minulého století) právě z impulzu státní moci a měly být využívány mimo jiné i pro komunikaci mezi vládou a jinými subjekty; v dalším rozvoji ale již hrály značnou roli nestátní subjekty včetně např. hackerských komunit. Právě hackerská subkultura ovlivnila další vývoj zejména tím, že namísto tržní ekonomiky převládly na Internetu a v kyberprostoru ideje bezúplatně šířených dat a informací.[18] Až později, když

---

[14] Například na elektrických klávesových hudebních nástrojích typu digitální syntetizátor nebo workstation lze různě upravovat zvukové a tónové vlastnosti hudebníkem právě hraných tónů stejně jako již do paměti nástroje nahraných melodií. Jedná se tak o automatické zpracování dat na základě programu, a proto tento hudební nástroj počítačovým systémem bezesporu je.

[15] NOVOTNÝ, O., VOKOUN, R., ŠÁMAL, P. a kol. *Trestní právo hmotné. Zvláštní část*. 6. vydání, Praha, Wolters Kluwer ČR, a. s., 2010, str. 211.

[16] GŘIVNA, T. K ustanovením Úmluvy o počítačové kriminalitě. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

[17] SMEJKAL, V. Legislativa na rozcestí. In: *CHIP, 7/1999.* Dostupný také z www: http://www.jvproject.cz/Archiv_CHIP/1999/Chip_07_99.pdf [citováno dne 9. října 2013]

[18] ZAVRŠNIK, A. Definiční problémy a kriminologická specifika kyberzločinu. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

se prostřednictvím Internetu začaly realizovat ekonomické i další společenské vztahy, bylo nutné se s otázkou působnosti právních norem na Internetu a v kyberprostoru - a vůbec s „právní neexistencí“[19] Internetu - vyrovnat.

Právní vymezení Internetu je složité a jeho legální definice neexistuje. Český právní řád pojem Internet nedefinuje (ačkoliv jej někdy používá)[20] a prostředí Internetu reguluje pomocí obecnějších pojmů jako „veřejná komunikační síť“. Poměrně komplikovanou definici veřejné komunikační sítě obsahuje zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).[21] Domnívám se, že právě z důvodu komplikovanosti dané definice je tam, kde je operováno s pojmem „veřejná komunikační síť“, pro vyloučení pochybností někdy též uveden vysvětlující dodatek „například Internet“, jako je tomu v § 53 odst. 1 zákoně č. 40/1964 Sb., občanského zákoníku. Nový občanský zákoník, zákon č. 89/2012 Sb., občanský zákoník, už pojem „veřejná komunikační síť“ nepoužívá vůbec a zobecňuje jej do výrazu „prostředky komunikace na dálku“.[22]

Lze tedy uzavřít, že zákonodárce se užívání slova Internet spíše vyhýbá a nahrazuje jej obecnějšími výrazy. I já budu v této práci používat obecnější pojem „kyberprostor“, jehož součástí je i Internet. Termín *kyberprostor* se v právním řádu České republiky vůbec nevyskytuje, ale pro účely popsání kybernetické, internetové a počítačové kriminality je podstatně praktičtější. Navzdory jisté dávce poetičnosti, která je dána odvozením pojmu původně z beletristické vědecko-fantastické literatury, je pojem dnes již běžně používán odbornou veřejností i trestněprávní vědou. Není však, ostatně stejně jako pojem Internet, nijak ostře vymezen. Prapůvodní popis slova kyberprostor však základní kontury velmi dobře nastiňuje: „*Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat*

---

[19] Termín právní neexistence se v této souvislosti objevuje v odborné literatuře, viz SMEJKAL, V. *Internet a §§§*. Praha, Grada, 2001, str. 16 a násl.

[20] Např. pojem „internetové stránky“ v § 2 písm. f) zákona o některých službách informační bezpečnosti, nebo „funkční přístup k internetu“ v § 40 odst. 5 zákona o elektronických komunikacích.

[21] § 2 písm. j) zákona o elektronických komunikacích: *„Veřejnou komunikační sítí je síť elektronických komunikací, která slouží zcela nebo převážně k poskytování veřejně dostupných služeb elektronických komunikací, a která podporuje přenos informací mezi koncovými body sítě, nebo síť elektronických komunikací, jejímž prostřednictvím je poskytovaná služba šíření rozhlasového a televizního vysílání.“* Pojmy „síť elektronických komunikací“, „služby elektronických komunikací“ a „veřejně dostupné služby elektronických komunikací“ jsou definovány pod písmeny h), n) a o) téhož paragrafu.

[22] § 1820 zák. č. 89/2012 Sb., občanský zákoník. Pojem „Internet“ jako takový se v zákoně vyskytuje jen ojediněle - je zmíněn i v § 1830 a § 1840.

abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat." Těmito slovy popsal kyberprostor americký spisovatel William Gibson v roce 1984 - tedy více než desetiletí před masivním rozšířením Internetu - ve svém románu Neuromancer.[23] Záměrem autora jistě nebylo vytvořit definici bez dalšího použitelnou pro právní vědu, přesto ale velmi dobře naznačil některé relevantní trestněprávní aspekty kyberprostoru - ten je pouze zdánlivý a reálně neexistuje (Gibson píše o kyberprostoru jako o „halucinaci" a „neprostoru mysli"), intenzivní, rozšířený a globální, nezná hranic („halucinace každý den zakoušená miliardami oprávněných operátorů všech národů"), je jen odrazem dat uložených v počítačových systémech, obsahuje množství informací („grafická reprezentace dat abstrahovaných z bank všech počítačů") a „nedomyslitelně komplexní". O zmíněných aspektech budu pojednávat v následující kapitole.

Je tedy patrné, že precizní právní definice pojmů Internet i kyberprostor, které by byly všeobecně akceptovatelné, neexistují. Dle některých názorů to ovšem nemusí být na obtíž, neboť komplexní charakter těchto prostředí jakoukoliv snahu o výstižnou definici značně znesnadňuje, přičemž vynaložené úsilí na popsání pojmů ani nemusí být účelné - podobně jako například není účelné pokoušet se jednoznačně definovat pojmy jako právo nebo spravedlnost.[24] Názor, že není třeba definice zmíněných dvou pojmů, pokud jsou alespoň naznačeny, sdílím - avšak dodávám, že je nutné vymezit alespoň odlišnosti mezi těmito výrazy. Stručně řečeno, Internet je třeba chápat jako pouhou součást kyberprostoru, případně jako jednu z jeho forem. Dle komentáře k trestnímu zákoníku je kyberprostor tvořený velkým množstvím navzájem propojených počítačů, serverů, přepínačů, optických kabelů a podobně, přičemž prostřednictvím této infrastruktury kyberprostor umožňuje její funkci, a konkrétně je jím *„vše od Internetu až po imaginární prostor, který nemá hmotnou podstatu"*.[25] Vedle Internetu lze jako další součást kyberprostoru chápat například telekomunikační sítě, virtuální

[23] GIBSON, W. *Neuromancer*. Plzeň, Laser, 1992. Výraz „kyberprostor" autor zmínil a naznačil již v roce 1982 ve své dřívější práci, v kyberpunkové povídce Burning Chrome, která byla publikována o čtyři roky později ve sbírce povídek Burning Chrome (český překlad GIBSON, W. *Jak vypálit Chrome*. Brno, Návrat, 2004. Překlad Ondřej Neff.). V této povídce Gibson používá ve stejném významu též výrazu „matrix".

[24] POLČÁK, R. *Normativní regulace soutěže v prostředí informačních sítí.* Brno, 2006. Disertační práce. Právnická fakulta Masarykovy univerzity v Brně. Vedoucí práce prof. JUDr. Petr Hajn, DrSc.. Str. 8 a násl. Dostupné také z: http://is.muni.cz/th/21177/pravf_d/

[25] ŠÁMAL, P. a kol. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání, Praha, C. H. Beck, 2012.

realitu nebo počítačovou hru.[26] Jako tradiční příklad pojetí kyberprostoru se uvádí telefonní hovor. Komunikace při telefonním hovoru neprobíhá ani v okolí komunikujících, ani v žádném z telefonních sluchátek či v kabelech, ale právě v kyberprostoru.

1.4 Internetová, počítačová a kybernetická kriminalita

Máme-li základní představu o rozdílu mezi pojmy Internet, počítačový systém a kyberprostor, bude již snadné od sebe odlišit i jednotlivé formy kriminality s nimi spojené. Je nutné si uvědomit, že podobně jako nejsou synonyma výrazy Internet - počítačový systém - kyberprostor, nelze libovolně zaměňovat ani výrazy z nich odvozené: internetová - počítačová - kybernetická kriminalita. Bohužel k tomu ale neopatrným zacházením s cizojazyčnými pojmy dochází. V zahraničí se objevují termíny jako *computer crime, computer-related crime, high-tech crime, technological crime, Internet crime* nebo *cybercrime*. Uvedené termíny nejsou synonymní a označují jiný okruh kriminality. Navzdory tomu se při některých neopatrných překladech s těmito pojmy jako se synonymními zachází. Například přeložením mezinárodního dokumentu „Convention on Cybercrime" názvem „Úmluva o počítačové kriminalitě" dochází ke zbytečnému sbližování pojmů kybernetické a počítačové kriminality, ačkoliv se tyto reálně liší.[27] Osobně se domnívám, že k nepřesnému překladu dochází z důvodu nerespektování určitého posunu chápání obou termínů v zahraničí: s rozvojem informačních a komunikačních technologií koncem devadesátých let začal být výraz *computer crime* příliš úzký - nešlo pod něj podřadit nové formy kriminality. Proto se postupně začala užívat vhodnější a obecnější kategorie *cybercrime*, bohužel do českého jazyka stále překládaná jako počítačová kriminalita namísto kybernetická.

Pojem *kybernetická kriminalita* či kybernetický trestný čin (*cybercrime)* je odvozen od kyberprostoru. Zjednodušeně řečeno se jedná o kriminalitu páchanou v kyberprostoru. Protože součástí kyberprostoru je i Internet a též všechny počítačové systémy, proti kterým či s jejichž pomocí lze páchat internetovou a počítačovou kriminalitu, resp. v jejichž prostředí ji lze páchat (viz níže), jsou i internetová a počítačová kriminalita jen podmnožinami kybernetické kriminality. Není proto správné používat tyto výrazy jako synonyma.

---

[26] JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007. Str. 17.

[27] Navzdory pojmové nepřesnosti budu v dalším textu vždy používat oficiálního českého názvu Úmluva o počítačové kriminalitě, neboť právě s tímto názvem v roce 2013 proběhl ratifikační proces tohoto dokumentu.

Pro ilustraci uvádím definici uvedenou v monografii Václava Jirovského „Kybernetická kriminalita“, v níž lze nalézt popis kybernetické kriminality jako kriminality, která *„může být namířena proti počítačům, jejich hardwaru, softwaru, datům, sítím apod.; nebo v ní vystupuje počítač pouze jako nástroj pro páchání trestného činu; případně počítačová síť a k ní připojená zařízení jsou prostředím, v němž se taková činnost odehrává.“*[28] Zmíněným prostředím je nepochybně myšlen kyberprostor. Kybernetická kriminalita, nazývána též kybernalita, zahrnuje např. i politicky motivovanou špionáž, extremismus či kyberterorismus,[29] samozřejmě za předpokladu, že k těmto jevům dochází v kyberprostoru.

Úmluva o počítačové kriminalitě, která má v současnosti značný vliv na chápání kybernetické kriminality, rozděluje kybernetickou kriminalitu do tří kategorií: [30]

1. **trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů** (tj. trestné činy ohrožující informační a komunikační technologie, tedy ohrožující kybernetickou bezpečnost; dle výše uvedené definice se jedná o *„kriminalitu namířenou proti počítačům, jejich hardwaru, softwaru, datům, sítím apod.“*);
2. **trestné činy související s počítači** (tj. trestné činy využívající informační a komunikační technologie ke spáchání tradičních trestných činů. V zahraničí je tato skupina označována jako *computer-related crime*. Dle Jirovského definice se jedná o kriminalitu, v níž vystupuje *„počítač pouze jako nástroj pro páchání trestného činu.“*);
3. **trestné činy související s obsahem a s porušením autorského práva a práv příbuzných autorskému právu** (tj. pomocí informačních a komunikačních technologií se šíří obsah, který je sám o sobě ilegální. V zahraniční se tato skupina označuje jako *content-related crime*. Zmíněná definice ji popisuje jako činnost, kdy je *„počítačová síť a k ní připojená zařízení prostředím, v němž se trestná činnost odehrává“*).

---

[28] JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007. Str. 19.

[29] Tamtéž, str. 270.

[30] GŘIVNA, T. K ustanovením Úmluvy o počítačové kriminalitě. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008. Srov. ZAVRŠNIK, A. Definiční problémy a kriminologická specifika kyberzločinu. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

Pojmy *počítačová* a *internetová kriminalita* pouze zužují kriminalitu páchanou v kyberprostoru výhradně na počítačové systémy a na Internet. Někteří autoři ovšem tyto kategorie směšují. Oproti tomu považuji za účelné operovat s nejobecnější pojmovou kategorií obsahující všechny tři výše uvedené skupiny, tj. kybernetickou kriminalitou.

1.5 Kybernetická a informační bezpečnost

Informační bezpečnost je obor usilující o dosažení komplexního řešení problematiky ochrany informací ve všech fázích jejich „života" - během jejich vzniku, zpracování, ukládání, přenosu a likvidace. Cílem oboru je minimalizovat rizika související s ochranou informací navrhováním odpovídajících protiopatření.[31] Informační bezpečnost se pokouší dosáhnout stavu, kdy jsou relevantní informace dostupné všem oprávněným osobám v nezbytně nutném rozsahu a jen tehdy, je-li to potřebné.[32] Tento obor se snaží dosáhnout toho, aby informace splňovaly tři základní kritéria: důvěrnost, integritu a dostupnost. *Důvěrnost* je atribut, díky kterému informaci získá jen oprávněná, autorizovaná osoba, a nikdo jiný. *Integrita* znamená, že je zabezpečena přesnost a kompletnost informací včetně metod jejich zpracování, tj. že oprávněná osoba se může spolehnout, že získaná informace je celistvá, například nezměněná neautorizovanou osobou nebo nepoškozená jiným vnějším vlivem. *Dostupností* je myšlena možnost získat informaci autorizovanou osobou v předpokládaném čase jeho potřeby.[33]

Informační bezpečnost lze chápat na úrovni osobní či organizační (např. snaha dosáhnout důvěrnosti, integrity a dostupnosti jednoho informačního systému), národní (např. ochrana osobních údajů všech občanů či některých zvlášť utajovaných informací v rámci celého státu) či nadnárodní (jednotlivé státy spolupracují s cílem dosáhnout vyššího stavu informační bezpečnosti). Informační bezpečnost není pouhým zabezpečením informačních systémů či informačních a komunikačních technologií - je to pojem komplexní, zahrnující

---

[31] JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007. Str. 270.

[32] POŽÁR, J. a kol. *Základy teorie informační bezpečnosti.* Praha, Vydavatelství Policejní akademie České republiky, 2007, str. 17 a násl.

[33] Tamtéž. Namísto pojmů důvěrnost, integrita a dostupnost se v literatuře objevuje též důvěryhodnost, neporušenost a použitelnost. V této práci ale nebudu tyto pojmy synonymní pojmy s ohledem na zachování jednotného pojmosloví používat. Nutno podotknout, že jednotný pojmový aparát nepoužívá ani oficiální český překlad Úmluvy o počítačové kriminalitě, který např. v čl. 16 odst. 2 pracuje s výrazem „neporušenost", ale v preambuli či v kapitole II. operuje s termínem „integrita". Obdobné platí i u pojmů dostupnost a použitelnost, a to navzdory tomu, že v původním znění se jedná o jeden a týž pojem. Důvodová zpráva k Úmluvě o počítačové kriminalitě též trpí nejednotou pojmů.

mimo jiné i organizační procedury a chování jednotlivců.[34] Na národní úrovni je informační bezpečnost řešena právními předpisy.

Jedním z odvětví informační bezpečnosti je *kybernetická bezpečnost*, což je informační bezpečnost zaměřená na ochranu určité části kyberprostoru před bezpečnostními hrozbami.[35] Pojem byl definován na půdě Organizace společných národů v doporučení Mezinárodní telekomunikační unie ITU-T X.1205 ze dne 18. 4.2008, čl. 3.2.5, přičemž tuto definici s drobnými úpravami překládám jako *„soubor nástrojů, strategií, bezpečnostních konceptů a záruk, zásad, doporučených postupů atd., které mohou být použity k ochraně kyberprostoru, organizací a aktiv uživatele, včetně veškeré síťově připojené výpočetní techniky, zaměstnanců, infrastruktury, aplikací, služeb, telekomunikačních systémů a též souhrnu přenesených anebo uložených informací v kyberprostoru.“*[36] Cílem kybernetické bezpečnosti je podobně jako u informační bezpečnosti dosáhnout důvěrnosti, integrity a dostupnosti informací. Kybernetická bezpečnost se dosažením těchto vlastností snaží ochránit organizaci a uživatelská aktiva před bezpečnostními riziky v kyberprostoru.

I kybernetickou bezpečnost lze chápat na osobní (resp. organizační), národní a nadnárodní úrovni. Na osobní, resp. organizační úrovni, je kybernetická bezpečnost právně relevantní jen v případech, kdy by bezpečnostní incident mohl mít negativní dopad v národním měřítku, např. kdyby hrozil výpadek páteřní sítě.[37] Na národní úrovni tento pojem vystihuje chystaný zákon o kybernetické bezpečnosti, který ji v § 2 písm. b) popisuje jako *„souhrn právních, organizačních, technických a vzdělávacích prostředků k zajištění ochrany kybernetického prostoru“,* čímž odpovídá definici Mezinárodní telekomunikační unie. Nadnárodní úroveň kybernetické bezpečnosti popisuje například dokument Evropské unie „Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor“

---

[34] POŽÁR, J. a kol. *Základy teorie informační bezpečnosti.* Praha, Vydavatelství Policejní akademie České republiky, 2007, str. 17 a násl.

[35] *„Bezpečnostní hrozbou je skutečnost, událost, síla nebo osoby, jejichž působení může způsobit poškození, zničení, ztrátu důvěry nebo hodnoty aktiva.“* Aktivy se rozumí *„všechny hmotné i nehmotné statky, které mají pro uživatele informačního systému jistou hodnotu, například peníze, majetek, data a informace.“* Bezpečnostní hrozba není totéž co útok (resp. bezpečnostní incident), neboť útok musí být zaviněný: *„Útokem rozumíme buďto úmyslné využitkování zranitelného místa, nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech. (…) Útočit lze přerušením, odposlechem, změnou či přidáním hodnoty k datu.“* POŽÁR, J. a kol. *Základy teorie informační bezpečnosti.* Praha, Vydavatelství Policejní akademie České republiky, 2007, str. 18.

[36] *Recommandation ITU-T X.1205 Overview of Cybersecurity.* Organizace spojených národů, Mezinárodní telekomunikační unie, 2008. Dostupné také z: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.1205 [citováno dne 9. října 2013]. Překlad autor. Termín „cyber environment“ překládám do českého jazyka jako „kyberprostor".

[37] POLČÁK, R. *Legislativa v České republice* [online].[citováno dne 9. října 2013]. Dostupné z www: http://www.cybersecurity.cz/law.html

z února 2013. Kybernetická bezpečnost se dle tohoto dokumentu *„vztahuje na záruky a opatření, jež mohou být použity k ochraně kyberprostoru v civilní i vojenské oblasti před hrozbami, které mají spojitost se vzájemně závislými sítěmi a informační infrastrukturou nebo které je mohou poškodit. Kybernetická bezpečnost má zachovat dostupnost a integritu sítí a infrastruktury, jakož i důvěrnost informací, jež jsou v nich obsaženy.“*[38] Cílem nadnárodní úrovně kybernetické bezpečnosti je spolupráce za účelem dosažení ochrany národních kyberprostorů před bezpečnostními hrozbami. Zmíněný dokument Evropské unie, a ostatně i chystaný zákon o kybernetické bezpečnosti, vychází z předpokladu, že nedostatečná kybernetická bezpečnost na úrovni organizace či jednotlivce může mít za následek nedostatečnou kybernetickou bezpečnost i na vyšší úrovni, což může vést až k narušení základních služeb.[39]

Kybernetické bezpečnosti a jejím trestněprávním důsledkům bude věnována závěrečná kapitola této práce.

[38] JOIN/2013/0001. Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů. Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor. Brusel, Vysoká představitelka Evropské unie pro zahraniční věci a bezpečnostní politiku, 2013. Str. 3. Dostupné také z www: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:CS:PDF [citováno dne 9. října 2013]

[39] Tamtéž.

2. LEGITIMITA A PŮSOBNOST TRESTNÍHO PRÁVA V KYBERPROSTORU

Ještě než se začneme zabývat samotnou kybernetickou kriminalitou, považuji za vhodné se krátce zamyslet nad otázkou oprávněnosti práva v kyberprostoru. Má vůbec být kyberprostor jakkoliv právem upravován, nebo k ochraně subjektivních práv uživatelů postačí jeho samoregulační mechanismy? Jsou hrozby mající původ v kyberprostoru pro společnost natolik škodlivé, že opravňují aplikaci trestního práva, které by mělo s ohledem na zásadu subsidiarity trestní represe reagovat na protiprávní jednání až v krajních případech, kdy nepostačují prostředky jiných právních odvětví?[40]

Samozřejmě na obě otázky v následujícím textu odpovím kladně - jinak bych ostatně popřel celou svou práci. Nabízejí se ale i další otázky legitimity z těchto vyplývající - v jaké intenzitě je regulace kyberprostoru trestním právem odůvodnitelná? S jakými zvláštnostmi kyberprostoru se právní regulace musí vyrovnat, aby byly právní normy vymahatelné? Nastíněnou oblastí se budu zabývat v první a druhé části kapitoly. Následně se zaměřím na specifikum teritoriální neohraničenosti kyberprostoru a s tím související problematiku místní působnosti trestněprávních norem.

2.1 Právně relevantní specifika kyberprostoru

2.1.1 Definiční normy a definiční autority v kyberprostoru

První specifikum kyberprostoru je dáno významem tzv. *definičních norem* a *definičních autorit*[41] v něm působících. Důležitým normativním systémem v kyberprostoru totiž není právo samotné, ale i jiné regulativy lidského chování. Mezi tyto regulativy patří podle amerického ústavního právníka Lawrence Lessiga[42] kromě práva i normy ve smyslu

[40] Zásada subsidiarity trestní represe a povaha trestního práva jako *ultima ratio* je zakotvena v § 12 odst. 2 TZ. Komentář k trestnímu zákoníku k těmto zásadám uvádí: *„Zásada subsidiarity trestní represe, jako jedna ze základních zásad trestního práva, vyžaduje, aby stát uplatňoval prostředky trestního práva zdrženlivě, to znamená především tam, kde jiné právní prostředky selhávají nebo nejsou efektivní, neboť trestní právo a trestněprávní kvalifikaci určitého jednání jako trestného činu je třeba považovat za ultima ratio, tedy za krajní prostředek, který má význam především celospolečenský, tj. z hlediska ochrany základních celospolečenských hodnot.“* ŠÁMAL, P. a kol. Trestní zákoník I. § 1 až 138. Komentář. 2. vydání, Praha, C. H. Beck, 2012. Str. 115 a násl.

[41] K pojmům definiční normy a definiční autority a jejich význam v kyberprostoru blíže viz např. POLČÁK, R. *Internet a proměny práva*. Praha, Auditorium, 2012. Str. 166 - 201.

[42] Lawrence Lessig je mimo jiné též specialistou na autorské právo a širší veřejnosti je znám jako zakladatel neziskové organizace Creative Commons, jejímž cílem je šíření autorských děl k legálnímu využívání a sdílení veřejností při současném zachování některých práv autora.

sociálním (k nimž patří i individuální etické regulativy a samoorganizační sociální mechanismy), pravidla ekonomiky a normy v podobě tzv. *kódu*,[43] který je v kyberprostoru právě zmíněnými definičními normami. Právě díky tomuto kódu kyberprostor funguje. Jeho uživatelé se až na výjimky tomuto kódu musí podřídit, protože obvykle nedisponují dostatečnými technickými znalostmi ke změně kódu. Chování uživatelů utvářejí definiční autority přesnou formulací kódu.

Definiční normou - kódem - není v tomto smyslu jen počítačový program nebo zdrojový kód webové stránky, ale je jím skutečně vše, co technicky ovlivňuje chování jednotlivých složek informační infrastruktury - tedy i technická pravidla jako například přenosové protokoly a podobně.[44] Kód se oproti systému práva vyznačuje **třemi zásadními rozdíly**. Za prvé: původcem pravidel (definičními autoritami) jsou nejčastěji osoby odlišné od státu, nejčastěji soukromoprávní subjekty. Jejich oprávnění k normotvorbě je dáno faktickou a technickou kompetencí - jsou to přeci právě tyto definiční autority, které kyberprostor formují. Za druhé: adresáti norem kódu (uživatelé) nemají možnost volby, zda se normě podřídí - podobně jako například lidé nemají možnost volby podřídit se zákonu gravitace v reálném světě. Ze skutečnosti, že se adresáti norem podřizují bez ohledu na svou vůli, vyplývá třetí rozdíl: ve struktuře kódu zcela chybí sankce, neboť tato není potřeba k vynucení kódu.[45] Někteří z adresátů norem ale mohou kód obejít nebo jej dokonce změnit (obvykle využitím nedokonalosti kódu), čímž nejsou normou vázáni a sami se stávají definiční autoritou.

Osobně se domnívám, že Lessigovým kódem mohou být i některé fyzikální zákony, které mají svůj dosah jak v reálném světě, tak v kyberprostoru. Uživatel je totiž v pohybu kyberprostorem omezen fyzickými parametry a stavem svého počítače, resp. jiného zařízení. Například pro telefonování prostřednictvím Internetu (technologie VoIP) je nutné disponovat dostatečně kvalitním připojením k Internetu. Soubor technických požadavků na kvalitu připojení k Internetu, jimiž je podmíněno užití technologie VoIP, tak lze chápat jako definiční normu. Lessigův kód je jediným regulativem lidského chování v kyberprostoru, který uživateli zakazuje využít této technologie i v případě nesplnění požadavků na kvalitu

[43] Lessigovým kódem se v české literatuře blíže zabývá zejména Radim Polčák, např. POLČÁK, R. *Internet a proměny práva*. Praha, Auditorium, 2012. Str. 188.

[44] Tamtéž.

[45] Tamtéž, str. 190-193.

připojení. Pokud uživatel tuto normu nerespektuje, stejně nebude moci technologii VoIP plnohodnotně využít, dokud definiční normě nevyhoví.

Definiční autorita vytváří kód. Autoritou v tomto smyslu tak může být například vývojář programu (kód programu je definiční normou), provozovatel webové stránky nebo uživatel e-mailové schránky (v těchto případech je definiční normou zdrojový kód stránky nebo některá uživatelská nastavení e-mailové schránky), poskytovatel služeb Internetu nebo telekomunikační operátor (zde spatřuji definiční normy v technických pravidlech, která umožní uživateli připojit se k jinému uzlu telekomunikační sítě).

V první kapitole této práce bylo naznačeno, že vývoj Internetu a ostatně i celého kyberprostoru nebyl ve svých počátcích ovlivňován vůbec žádnými právními normami. Bylo tomu tak proto, že zákonná úprava nebyla potřebná: kyberprostor byl formován Lessigovým kódem a sám o sobě zpočátku neumožňoval žádné rozsáhlé zásahy do cizích subjektivních práv. Případné konflikty byly řešeny samoregulačními mechanismy kyberprostoru, tj. definičními autoritami, a to ke všeobecnému užitku. Tento stav, který Radim Polčák přirovnává ke zlatému věku lidstva v pojetí antických bájí,[46] však netrval dlouho. Ještě dlouho před nástupem Internetu se rozmohl fenomén tzv. *phreakingu* - technik k manipulaci se službami telefonních společností. Phreakeři[47] tak byli první uživatelé kyberprostoru,[48] kteří se ve velkém rozsahu naučili přizpůsobovat si kód dle svých představ. S rozšířením počítačů i do domácností v letech osmdesátých a s celosvětovou expanzí Internetu v letech devadesátých se začaly objevovat nové možnosti dalšího zneužívání kódu. Zásadně se změnila komunita tzv. *hackerů* - až dosud totiž aktivity hackerů nepřesahovaly rámec univerzity a neškodily širšímu okruhu osob, a proto byly obvykle tolerovány.[49] S objevem dalších možností ale někteří hackeři začali vyrábět a šířit škodlivý software, stále častěji docházelo k bankovním podvodům, útokům na webové stránky významných institucí a k dalším formám kybernetické kriminality.

---

[46] POLČÁK, R. Autoritativní regulace kyberprostoru a legitimita trestního práva. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

[47] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Druhé vydání, Praha, 2013. Str. 72.

[48] Phreaking se rozmohl v USA již v sedmdesátých letech, tedy ještě před prvním výskytem pojmu kyberprostor. Protože však v této práci chápu jako součást kyberprostoru i telekomunikační kanály, lze za uživatele kyberprostoru považovat i uživatele telefonních služeb.

[49] JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007. Str. 49. Subkultura hackerů bude více popsána v kapitole 3.1.1.

Z uvedeného je patrné, že samotný normativní systém kódu není v kyberprostoru účinný. Existuje totiž skupina uživatelů (jako příklad výše uvedení hackeři a phreakeři), kteří jsou z jeho působnosti díky svým technickým schopnostem vyňati,[50] čímž mohou ohrozit zájmy jiných uživatelů kyberprostoru.

2.1.2 Omezenost státní moci v kyberprostoru

I pokud prozatím připustíme všeobecnou vázanost kyberprostoru právem, což bude ještě předmětem zkoumání v následující podkapitole, stále existuje problém s vykonatelností práva v kyberprostoru. Nejvyšší moc v kyberprostoru mají již zmíněné definiční autority, mezi nimiž mají výsadní postavení *poskytovatelé služeb informační společnosti* (dále jen „**ISP“** - *Information Service Provider*, někdy se používá i jako *Internet Service Provider*), kteří uživatelům poskytují část své informační infrastruktury. Ve vztahu k uživatelům mohou ISP svým zásahem omezit nebo zastavit poskytování služby, čímž může dojít například k nedostupnosti konkrétní webové stránky ostatním uživatelům nebo naopak k nemožnosti uživatele se k Internetu připojit. Jinou vlivnou skupinou definičních autorit jsou tzv. *doménové autority*, pod jejichž kontrolou probíhá registrace doménových jmen. Tyto autority spravují databáze, pomocí kterých je jednoznačný, ale složitý číselný identifikátor serveru (IP adresa)[51] převáděn na též jednoznačné, ale lépe zapamatovatelné alfanumerické doménové jméno, které si zájemce o registraci doménového jména sám zvolí. Doménové autority mohou rozhodnout o neregistrování doménového jména nebo provoz již registrované domény přerušit.

Na rozdíl od zmíněných definičních autorit nemá stát v rámci kyberprostoru žádnou moc, kterou by mohl vůči konkrétním uživatelům plošně uplatňovat. Nemůže sám zajistit, aby byl přerušen provoz konkrétního serveru z důvodu porušování právních norem. Stát může toliko o takovém přerušení provozu za určitých podmínek rozhodnout vydáním individuálního právního aktu. Pro jeho výkon je ovšem nutné jej provést zprostředkovaně, za pomoci příslušné definiční autority, která k takovému výkonu má potřebnou technickou kompetenci.[52] Pro účely vymahatelnosti práva je tedy nutné, aby stát spolupracoval

---

[50] Srov. POLČÁK, R. Autoritativní regulace kyberprostoru a legitimita trestního práva. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

[51] *„Číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, kterou používá internetový protokol. Slouží k rozlišení síťových rozhraní připojených k počítačové síti.* JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.“* Druhé vydání, Praha, 2013. Str. 52.

[52] POLČÁK, R. *Internet a proměny práva*. Praha, Auditorium, 2012. Str. 195.

s definičními autoritami. To je možné jen s těmi, které jsou zákonnými prostředky identifikovatelné v reálném světě mimo kyberprostor a které spadají pod působnost práva daného státu.

Spolupráce státu s definičními autoritami je realizována více právními instituty. Jednak se jedná o *obecnou povinnost vyhovět* dožádáním orgánů činných v trestním řízení při plnění jejich úkolů dle § 8 odst. 1 TŘ.[53] Tato povinnost je blíže konkretizována jako *povinnost poskytnout požadovanou pomoc* v případě vyšetřování prováděném Policií České republiky dle § 18 zákona č. 273/2008 Sb., o Policii České republiky.[54] Na základě tohoto ustanovení může Policie České republiky požadovat od ISP poskytnutí informací o jeho klientech. Informace o uživatelích jsou oprávněni od ISP dále požadovat i soudy v rámci civilního, správního a samozřejmě i trestního řízení, a v mezích autorského práva dokonce i osoby, do jejichž autorských práv bylo prostřednictvím hostingových služeb zasaženo.[55] Tyto povinnosti jsou obvykle jen dílčími postupy vedoucími k vyšší vymahatelnosti práva a v podstatě ISP při jejich plnění nijak nezasahuje do kyberprostoru, neboť jen poskytuje informace - výjimkou je povinnost poskytnout požadovanou pomoc Policii České republiky. Dle některých doktrinálních výkladů § 47 zákona č. 283/1991 Sb., o Policii České republiky, který v minulosti odpovídal citovanému ustanovení § 18 zák. č. 273/2008 Sb., totiž může Policie České republiky k zajištění veřejného pořádku v některých případech nařídit českým ISP blokovat příslušné IP adresy.[56]

Jiným institutem, kterým stát spolupracuje s definičními autoritami pro vyšší vymahatelnost práva, je *odpovědnost ISP za obsah*, která je konstruována objektivně. V případě závadného obsahu (může jít o zásah do autorských práv, ale i o obsah s tematikou extremismu, dětské pornografie nebo např. o obsah způsobilý poškodit záznam v počítačovém systému pomocí škodlivého software) tak odpovědnost ISP nezakládá až zavinění ISP, ale již samotný fakt, že ISP o protiprávnosti obsahu prokazatelně věděl. České právo v zákoně

---

[53] § 8 odst. 1 věta první TŘ: *„Státní orgány, právnické a fyzické osoby jsou povinny bez zbytečného odkladu, a nestanoví-li zvláštní předpis jinak, i bez úplaty vyhovovat dožádáním orgánů činných v trestním řízení při plnění jejich úkolů.“*

[54] § 18 zákona č. 273/2008 Sb., o Policii České republiky: *„Policista je v rozsahu potřebném pro splnění konkrétního úkolu policie oprávněn požadovat od orgánů a osob uvedených v § 14 věcnou a osobní pomoc, zejména potřebné podklady a informace včetně osobních údajů. Tyto orgány a osoby jsou povinny požadovanou pomoc poskytnout; nemusí tak učinit, brání-li jim v tom zákonná nebo státem uznaná povinnost mlčenlivosti anebo plnění jiné zákonné povinnosti. Fyzická osoba tak nemusí dále učinit, pokud by poskytnutím pomoci vystavila vážnému ohrožení sebe nebo osobu blízkou.“*

[55] POLČÁK, R. *Právo na internetu: Spam a odpovědnost ISP.* Brno, Computer Press, 2007. Str. 84 a násl.

[56] Tamtéž, str. 79 a násl.

č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů,[57] rozděluje ISP dle režimů odpovědnosti za obsah do tří kategorií: na poskytovatele služeb spočívající v přenosu informací poskytnutých uživatelem (běžně je používán anglický termín *access provider*; tento režim je upraven v § 3), poskytovatele služeb spočívajících v automatickém meziukládání informací poskytnutých uživatelem (tito poskytují tzv. *caching*; jejich režim je upraven v § 4) a poskytovatele služeb spočívajících v ukládání informací poskytnutých uživatelem na žádost uživatele (poskytují tzv. *hostingové služby* dle režimu v § 5). Každý z odpovědnostních režimů se mírně liší a tak jednotlivé typy poskytovatelů služeb odpovídají různými způsoby.

Lze tedy uzavřít, že spolupráce státu a definičních autorit v kyberprostoru (v současnosti realizována jednak jako povinnost poskytnout požadovanou pomoc Policii ČR, jednak jako odpovědnost ISP za obsah) je pro vymahatelnost práva naprosto nepostradatelná.

2.1.3 Teritoriální neomezenost kyberprostoru

Zatímco kyberprostor nezná hranic, lze právo státu realizovat jen a pouze na státním území. Za hranicí státu může v některých případech nalézt právo svou působnost (viz níže), ale stát nemůže ukládat povinnosti definičním autoritám působícím v kyberprostoru, které se nacházejí na území jiného státu. V kyberprostoru lze ale protiprávní jednání provádět z libovolného místa světa a jeho následek se může projevit na jakémkoliv jiném místě v kyberprostoru, mnohdy i na velkém množství míst naráz. S tímto faktem se musí právo vyrovnat.

Převážná většina počítačové kriminality má přeshraniční charakter.[58] Situace v praxi ale bývá často ještě komplikovanější. Pachatel nacházející se na území Číny může získat neoprávněný přístup k počítačovému systému umístěnému na území Rumunska k získání neoprávněného přístupu k počítačovému systému v České republice, a počítačová data takto získaná odeslat do Ruska. Česká trestněprávní doktrína mluví o tzv. *distančních deliktech*, pro které je charakteristické, že *„nejsou spáchány na území České republiky ve všech svých znacích. Postačí, aby tu bylo provedeno jednání, i když následek (zpravidla půjde o účinek)*

[57] Tento zákon provádí směrnici č. 98/34/ES ve znění směrnice č. 98/48/ES, o postupu při poskytování informací v oblasti technických norem a předpisů a pravidel pro služby informační společnosti, a dále směrnici č. 2000/31/ES, o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu. K tzv. směrnici o elektronickém obchodu viz kapitola 4.2 této práce.

[58] ŠIMOVČEK, I. a kol. *Kriminalistika.* Plzeň, Aleš Čeněk, 2011. Str. 378.

nastal v cizině, nebo naopak."[59] V zahraniční literatuře se v souvislosti s trestnými činy páchanými v kyberprostoru vedle distančních deliktů mluví i o tzv. *multiteritoriálních deliktech*. Tento pojem označuje trestné činy, které sice jsou spáchány fyzicky z jediného místa jednoho státu, ale škodlivý následek nastal nebo může nastat ve větším množství dalších států.[60] Typickým příkladem multiteritoriálního deliktu jsou trestné činy související s obsahem. Škodlivý obsah (např. obsahující dětskou pornografii), který je součástí webové stránky na Internetu, je sice nahrán na server fyzicky umístěný v jednom státě, ale je dostupný uživatelům Internetu z většiny států světa. Pokud je šíření tohoto obsahu v těchto státech trestným činem, spadá pod národní jurisdikce více států. Případy konfliktů jurisdikcí se budu zabývat v poslední části této kapitoly.

Závěrem k tomuto tématu podotýkám, že neomezenost kyberprostoru nepůsobí obtíže jen při stanovení, podle kterého práva se bude posuzovat trestnost společensky nebezpečného jednání v kyberprostoru. Možnost pachatelů kybernetické kriminality volně přecházet mezi jednotlivými jurisdikcemi a užít ke spáchání trestného činu počítač fyzicky umístěný na druhé straně světa zásadně komplikuje i odhalování trestné činnosti a práci orgánů činných v trestním řízení. Na rozdíl od pachatele jsou totiž osoby činné v trestním řízení omezeny svou místní působností. Proto je nutná spolupráce na mezinárodní úrovni.

2.1.4 Anonymita kyberprostoru

Vysoká anonymita uživatelů kyberprostoru je dána tím, že „tváří" uživatele je IP adresa, kterou mu pro přístup k síti přidělil ISP poskytující uživateli připojení k Internetu. Identifikace uživatelů Internetu s konkrétními fyzickými osobami je nesnadná, nicméně v součinnosti s ISP je možná. Anonymita tedy může být prolomena, ale zkušenější uživatele je složité odhalit i s využitím všech (legálních) prostředků. Uživatel totiž může využít služeb různých anonymizérů. Například pomocí systému *cibulového směrování* (onion routing) lze docílit toho, že datové pakety[61] jsou zašifrovány a vedeny přes síť anonymizujících směrovačů (routerů), které si vzájemně předávají jen některé informace.

---

[59] ŠÁMAL, P. a kol. *Trestní zákoník*. 2. vydání, Praha, C. H. Beck, 2012. Str. 70.

[60] VALERIUS, B. Zum Anwendungsbereich nationaler Rechtsordnungen im Zeitalter des Internets. In: HERCZEG, J. HILGENDORF, E. GŘIVNA, T. (Hrsg). *Internetkriminalität und die neuen Herausforderungen der Informationsgesellschaft des 21. Jahrhunderts*. Praha, Wolters Kluwer, 2010.

[61] Pomocí paketů probíhá veškerá komunikace na Internetu a v počítačových sítích. Paket je blok informací, který je přenášen v kyberprostoru. Každý paket je opatřen informacemi o jeho odesílateli a příjemci (resp. o jejich IP adresách). Než se paket dostane od odesílatele k příjemci, obvykle si několikrát tyto informace vymění s jinými pakety. Pro ISP, který zná IP adresy svých uživatelů, tak nemusí být složité zjistit například to, jaké stránky uživatelé navštěvují.

Zatímco v běžných směrovačích si pakety vymění s ostatními pakety informace o svých odesílatelích a příjemcích (resp. o jejich IP adresách), při cibulovém směrování jsou tyto informace zašifrované a směrovač zjistí jen to, od jakého směrovače paket přijal a ke kterému směrovači jej má poslat dál. Směrovač tedy nezjistí, jaké jiné směrovače paket během své cesty kyberprostorem navštívil, protože data o nich jsou zašifrovaná různými klíči. Po odeslání paketu má další směrovač jiný klíč, kterým opět zjistí jen informaci o předchozím a následujícím směrovači. Pokud tedy kdokoliv, včetně osob činných v trestním řízení, bude zkoumat, kdo je odesílatelem paketu, namísto IP adresy odesílatele zjistí IP adresu některého ze zařízení v síti anonymizujících směrovačů.[62] To může nejen znemožnit identifikaci skutečného pachatele, ale dokonce vést k podezření, že pachatelem je někdo zcela jiný.

2.1.5 Efektivnost kybernetické kriminality

Z vysoké anonymity popsané výše vyplývá pro uživatele - pachatele kybernetické trestné činnosti poměrně oprávněný pocit neodhalitelnosti. S minimálním nebezpečím odhalení a při vynaložení relativně malého úsilí i finančních prostředků[63] lze v kyberprostoru napáchat rozsáhlé škody anebo získat majetkový prospěch. Z těchto důvodů je kybernetická kriminalita velmi efektivní.

2.2 Legitimita trestního práva v kyberprostoru

Od okamžiku, kdy v kyberprostoru začaly probíhat první ekonomické a jiné vztahy, jejichž realizace byla v zájmu jednotlivců i celé společnosti, začala být aktuální otázka, zdali jsou tyto vztahy chráněné právem. Protože v kyberprostoru osmdesátých let patřily mezi nejvýznamnější definiční autority jednotlivci sdružující se do undergroundových hackerských komunit vzývajících hodnoty kyberpunku,[64] převládající názor znějící kyberprostorem byl

---

[62] ČÍŽEK, J. *TOR: Skutečně anonymní internet* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://www.zive.cz/clanky/tor-skutecne-anonymni-internet/sc-3-a-149055/default.aspx

[63] Například útok typu DDoS (viz kapitola 3.1.1) je pro byť jen minimálně zkušeného programátora velmi jednoduché připravit. Takový útok není ani nijak drahé či pro kohokoliv složité koupit. NÝVLT, V. *Internet mimo provoz? DDoS útok lze koupit za pár korun* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://technet.idnes.cz/ddos-hrozba-cxk-/sw_internet.aspx?c=A130305_072420_sw_internet_nyv. Srov. též HOUSER, P. *Kolik lze vydělat počítačovou kriminalitou* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://computerworld.cz/securityworld/kolik-lze-vydelat-pocitacovou-kriminalitou-47816

[64] *„Kořeny kyberkultury lze najít v revolučním, protikulturním období, které charakterizovalo sedmdesátá léta. Byla to éra široce definovaná bojem proti vědeckému - či přeučenému - chápání reality a technologie. K transformaci došlo později v devadesátých letech, kdy se protikultura spojila s formami technologie, které zdánlivě nabízely určité prostředky úniku od extenzivních společenských regulací. Za těchto podmínek kyberkultura zahrnuje úsilí o osvobození jednotlivce, které bylo postupně převzato a omezeno velkými mezinárodními technologickými systémy. (...) Tato kultura byla primárně založena na principu ekonomiky daru,*

právo do něj pokud možno nevpustit. Tyto myšlenky svobodného kyberprostoru prosazovala organizace *Electronic Frontier Foundation* (EFF), která se již od svého založení v roce 1990 veřejně angažuje podporou boje proti (z pohledu organice reálně hrozícímu) omezování svobody jedince na Internetu, například formou právní pomoci v soudních sporech.[65]

Argumenty právně neregulovaného kyberprostoru organizace shrnula do ***Deklarace nezávislosti kyberprostoru***,[66] kde je prezentována idea autonomního kyberprostoru s fungujícími samoregulačními mechanismy odlišnými od práva. Nulová působnost práva je požadována na základě *argumentu neexistence společenské smlouvy* mezi původcem právních norem a jejich adresáty, dále na základě *argumentu nepotřebnosti* právní regulace a *argumentu neschopnosti* státu efektivně právo v kyberprostoru vynucovat.[67]

2.2.1 Argument neexistence společenské smlouvy v kyberprostoru

Deklarace doslova uvádí, že uživatelé kyberprostoru mají *„novou společenskou smlouvu.“*[68] To je zřejmý odkaz na myšlenky raně novověkých myslitelů (počínaje Thomasem Hobbesem), dle kterých se všichni lidé ve společnosti dobrovolně vzdávají části svých práv ve prospěch suveréna, tj. státu, kterému tímto dávají svolení ochraňovat zájmy společnosti i jednotlivců právem a toto právo vůči všem vynucovat. Tento souhlas ovládaných je nazýván společenskou smlouvou a právě z ní pramení legitimita práva.

Deklarace nezávislosti kyberprostoru se domnívá, že v kyberprostoru platí jiná společenská smlouva, k níž musí uživatelé kyberprostoru dát svůj souhlas. To ovšem není úplně pravda - společenská smlouva totiž nevznikla konkrétním projevem vůle jednotlivců, kteří se dovolávali ochrany ze strany státu, ale už objektivní potřebou takové ochrany.[69] Společenské vztahy vznikající v kyberprostoru jsou založeny na stejné podstatě jako

---

včetně volného přístupu a sdílení znalostí.“ ZAVRŠNIK, A. Definiční problémy a kriminologická specifika kyberzločinu. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

[65] POLČÁK, R. Autoritativní regulace kyberprostoru a legitimita trestního práva. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

[66] Deklarace pochází z roku 1996 a je přímou reakcí na americký zákon deregulující trh s telekomunikacemi (*Telecommunications Act of 1996)*, v němž EFF spatřovala zásadní omezení svobody na Internetu. Text v anglickém originále *A Declaration of the Independence of Cyberspace* dostupný z www: https://projects.eff.org/~barlow/Declaration-Final.html

[67] POLČÁK, R. Autoritativní regulace kyberprostoru a legitimita trestního práva. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

[68] *„You have no sovereignty where we gather. (…) We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.“* Celý text deklarace je dostupný z www, viz reference uvedená v poznámce č. 66.

[69] POLČÁK, R. *Internet a proměny práva*. Praha, Auditorium, 2012. Str. 97.

společenské vztahy mimo kyberprostor, nová je toliko forma jejich realizace. Objektivní potřeba právní ochrany je tedy stejná v kyberprostoru jako mimo něj, kde již byla historicky prověřena.[70] Proto je nejen právem, ale dokonce povinností státu zajistit, aby kyberprostor byl regulován právními normami za účelem ochrany společenských vztahů.

Jinak je tomu ovšem u vztahů, které se v kyberprostoru objevují nově a historickou legitimitou ještě nedisponují. Zde bude zcela na místě společenská debata o tom, zda je dobré zmíněné vztahy pevně regulovat právem. Dle některých názorů[71] je nutné znovu hledat legitimitu například k některým institutům autorského práva, které nejsou vhodné pro současné technologie umožňující hromadné kopírování a právně téměř nepostižitelné sdílení obsahu. Obecně ale legitimita práva v kyberprostoru založená platnou společenskou smlouvou existuje.

2.2.2 Argument nepotřebnosti právní regulace v kyberprostoru

Argument nepotřebnosti práva odvíjející se od tvrzení, že s případnými konflikty je kyberprostor sám připraven se vypořádat vlastními prostředky a jakékoliv snahy řešit tyto konflikty ze strany státu jsou jen záminkou k státním zásahům do kyberprostoru,[72] též neobstojí. Při pohledu na prudce stoupající křivky kybernetické kriminality skutečně nelze mluvit o úspěšnosti samoregulace kyberprostoru. Jak vyplývá z kapitoly 2.1.1, samotný normativní systém kódu není schopen oprávněné zájmy jednotlivců i společnosti efektivně chránit, neboť existuje široký okruh uživatelů, kteří se díky svým technickým schopnostem stávají nepostižitelnými.

Je proto nutné, aby v kyberprostoru vedle kódu působil i normativní systém práva. Stav a dynamika kybernetické kriminality jsou dokonce natolik závažné, že je nutné a vhodné chránit některé společenské vztahy v kyberprostoru trestním právem. Například proti fenoménu dětské pornografie je soukromé právo naprosto bezbranné.

---

[70] POLČÁK, R. *Internet a proměny práva*. Praha, Auditorium, 2012. Str. 98.

[71] Významnou postavou volající po reformě autorského práva je již zmíněný Lawrence Lessig. Blíže viz LESSIG, L. *Free Culture*. New York, The Penguin Press, 2004. Pod licencí Creative Commons k volnému stažení z www: http://www.free-culture.cc/freeculture.pdf [citováno dne 9. října 2013]

[72] *„You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means.“* Celý text deklarace je dostupný z www, viz reference uvedená v poznámce č. 66.

2.2.3 Argument neschopnosti státu efektivně právo vymáhat v kyberprostoru

Argument neschopnosti státu vymáhat své právní normy v kyberprostoru[73] je ze tří argumentů uvedených v Deklaraci nezávislosti kyberprostoru nejzávažnější. Nelze ale resignovat na normotvorbu jen z toho důvodu, že domněle není vymahatelná. Naopak je nutné hledat řešení problematiky vymahatelnosti. V kyberprostoru působí různé definiční autority a je vhodné se ptát, zdali by právní regulaci nevymáhala některá z nich k všeobecnému prospěchu všech uživatelů kyberprostoru lépe než stát, nebo zdali by nebyla vhodná nějaká forma spolupráce mezi nimi. Právě spoluprací byl v posledních desetiletích problém nevymahatelnosti právních norem v kyberprostoru do značné míry překlenout. Regulace celého kyberprostoru státem je nemožná a s ohledem na značné ohrožení svobody jednotlivce v kyberprostoru, k němuž by pokus o takovou regulaci pravděpodobně vedl, i nežádaná.[74] Mnohem přijatelnější cestou pro stát je kooperace s definičními autoritami a s jinými státy.

Součinnost státu se soukromoprávními osobami, nezbytná například i pro výkon rozhodnutí, je v první řadě zajištěna ***společnými zájmy státu a těchto osob***. Například provozovatel služeb e-mailu může svou aplikaci vybavit filtrem na zachytávání spamu nebo škodlivého software, který se šíří elektronickou poštou. Nečiní tak proto, že šíření takových e-mailů může být samo o sobě protiprávní,[75] ale z důvodu tlaku konkurence, která nutí poskytovatele k vyšší kvalitě služeb za účelem uspokojení svých zákazníků. Stejně tak ISP budou mít zájem na tom, aby se na jejich serverech nešířil škodlivý obsah v podobě extremismu nebo dětské pornografie. Tento obsah by jistě část uživatelů odradil. Jeho odstranění proto obsahu vede ke zvýšení kvality informační sítě, jejímu dalšímu rozvoji a případnému finančnímu zisku.[76]

V mnohých případech ovšem k dobrovolné spolupráci soukromé subjekty nemají vůli. Ani tehdy se ovšem stát nemusí uchylovat k přímému vynucování norem, postačí zaručení

---

[73] *„Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.(...) Our identities may be distributed across many of your jurisdictions.(...) We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts."* Celý text deklarace je dostupný z www, viz reference uvedená v poznámce č. 66.

[74] Značná oprávnění státu mívají zejména režimy známé svou nižší demokratičností. Zde lze mluvit o skutečné cenzuře Internetu, kdy jsou některé jinde běžně rozšířené služby Internetu z území daného státu zcela nedostupné. Události tzv. arabského jara, při kterém sehrál značnou roli i Internet jako svobodné médium, ukázaly, že některé režimy na podobných omezeních Internetu skutečně stojí, a zejména padají.

[75] K trestněprávním důsledkům viz 5. kapitola.

[76] POLČÁK, R. *Internet a proměny práva*. Praha, Auditorium, 2012. Str. 110.

právní ochrany státem.[77] ***Institut odpovědnosti ISP***, stručně popsaný v minulé podkapitole, doplňuje dobrovolné chování v zájmu státu. Stát přímo ukládá některým definičním autoritám povinnosti postihovat některá protiprávní jednání v té části kyberprostoru, nad kterou mají ISP nadvládu. Pokud o protiprávním jednání ISP ví a nezakročí proti němu, může to v závislosti na typu ISP založit jeho odpovědnost vůči třetím subjektům nebo státu. ISP navíc může na rozdíl od státu využít svého postavení silné definiční autority v kyberprostoru, který může ovlivňovat kódem. Další výhodou je soukromoprávní charakter ISP a z něj plynoucí princip legální licence, díky kterému si ISP může řadu podmínek ujednat se svými klienty individuálně, s výjimkou takových ujednání, která jsou zakázána.[78] V takovém režimu postačí státu jen kontrolovat, že ISP dbá na ochranu soukromí svých klientů, nezneužívá svého postavení k omezení hospodářské soutěže a podobně.

Samozřejmě, realita není ve vymahatelnosti práva tak jásavá, jak by se mohlo zdát po přečtení předchozího textu. Z důvodu neomezenosti hranic kyberprostoru je často obtížně zjistitelné, kdo vlastně je ISP ve světě mimo kyberprostor, resp. pod jurisdikci jakého státu patří. Stát nemůže ISP nespadající pod svou jurisdikci přímo ukládat žádné povinnosti. Tento problém se pokouší řešit ***mezinárodní spolupráce***. Podobně jako v případě spolupráce se soukromoprávními subjekty se i zde stát vzdává části své suverenity - tentokrát ve prospěch třetích států, na které umožňuje v některých případech přenést jurisdikci. Mezinárodní spolupráce z velké části řeší kompetenční konflikty jurisdikcí (které blíže představím v podkapitole 2.3), dále též některé mezinárodní smlouvy umožňují přímou spolupráci mezi osobami činnými v trestním řízení. Nejvýznamnější takovou smlouvou je Úmluva o počítačové kriminalitě, která bude rozebrána v kapitole 4.

2.2.4 Intenzita státní regulace kyberprostoru

Regulaci kyberprostoru ze strany státu, včetně tvorby a vymáhání trestněprávních norem, považuji na základě výše uvedených argumentů za legitimní. Proti jakékoliv regulaci brojí Deklarace nezávislosti kyberprostoru. Je třeba si ale uvědomit, že tento text pochází z roku 1996, kdy si až na několik vizionářů nikdo nedovedl představit technické možnosti nového tisíciletí. Domnívám se, že ani EFF si při tvorbě svého stěžejního dokumentu neuvědomovalo stinné stránky tohoto rozvoje. Na druhou stranou od vzniku Deklarace

[77] Tendence přechodu chápání státu od státu jako subjektu přímo provádějící regulaci ke státu pouze zaručujícímu fungující volný trh s minimálními přímými zásahy je patrná nejen v České republice a nejen v oblasti kyberprostoru.

[78] POLČÁK, R. *Internet a proměny práva*. Praha, Auditorium, 2012. Str. 109.

nezávislosti kyberprostoru prošlo právo rychlým vývojem zejména v oblasti vymahatelnosti v kyberprostoru. Dnešní kyberprostor je značně odlišný od toho, kterého měla deklarace udržet nezávislým. Dnešní EFF již také nemá za cíl pokračovat ve svém boji za nezávislost, ale bránit svobodu slova, soukromí, inovace a zákaznická práva v kyberprostoru.[79] Lze říci, že samotnou existenci práva v kyberprostoru tak nikdo z řad odborné veřejnosti nezpochybňuje. Sporná ovšem nadále zůstává míra regulace.

Současný režim založený na spolupráci definičních autorit se státem a na spolupráci států mezi sebou osobně považuji za dostatečně silný k efektivní ochraně práv jednotlivců i celé společnosti na jedné straně, a zároveň respektující práva uživatelů kyberprostoru a nezvyšující odpovědnostní či jinou zátěž definičních autorit na straně druhé. Nutno ovšem podotknout, že nesprávným nastavením parametrů tohoto režimu lze vytvořit systém selhávající v obou těchto kritériích.

2.3 Působnost norem trestního práva v kyberprostoru

2.3.1 Zásady určující působnost trestního práva

Ze specifika neohraničenosti kyberprostoru vyplývá požadavek, aby trestní právo u kybernetické kriminality rozlišovalo mezi místem jednání a místem následku. Například u šíření obsahu, kterým lze naplnit skutkovou podstatu trestného činu popírání, zpochybňování, schvalování a ospravedlňování genocidia,[80] jsou místem následku všechny státy světa, z jejichž území je tento obsah dostupný a dle jejichž práva je obsah způsobilý porušit nebo ohrozit zájem chráněný trestním právem. Princip rozlišování mezi místem jednání a místem následku není v právu nijak nový a není uplatňován jen u kybernetické kriminality. Například v případu *Lotus*, který byl řešen Stálým dvorem mezinárodní spravedlnosti před více než osmdesáti lety, si dva státy nárokovaly jurisdikci nad posádkou parníku, která v cizích teritoriálních vodách zavinila srážku s jinou lodí. Dle rozhodnutí soudu je třeba trestné činy, jejichž pachatelé se v době spáchání nacházejí na území jiného státu,

[79] K těmto cílům se Electronic Frontier Foundation hlásí na své webové stránce www.eff.org [citováno dne 9. října 2013]

[80] § 405 TZ: *„Kdo veřejně popírá, zpochybňuje, schvaluje nebo se snaží ospravedlnit nacistické, komunistické nebo jiné genocidium nebo jiné zločiny nacistů a komunistů proti lidskosti, bude potrestán odnětím svobody na šest měsíců až tři léta."*

považovat za spáchané na území tohoto státu, pokud se zde objevil jeden ze základních prvků trestného činu, zejména jeho následek.[81]

Působnost trestního práva stojí na zásadě teritoriality zakotvené v § 4 TZ, dle jehož prvního odstavce se podle zákona České republiky posuzuje trestnost činu, který byl spáchán na jejím území. Případy, kdy místa jednání a následku jsou odlišná, upravuje druhý odstavec, podle kterého zakládá působnost českého trestního práva i pokud je území České republiky jen místem jednání nebo naopak jen místem následku. V takovém případě bude možné uplatňovat trestní právo i proti pachatelům trestných činů spáchaných alespoň zčásti v cizině. K obdobné aplikaci může dojít i v případě splnění podmínek pro uplatnění dalších principů upravujících působnost trestněprávních norem, k nimž patří zásada registrace (§ 5 TZ), zásada personality (§ 6 TZ), zásada ochrany a zásada univerzality (§ 7 TZ) nebo subsidiární zásada univerzality (§ 8 TZ).[82] Působnost může být stanovena i mezinárodní smlouvou (§ 9 TZ).

Zmíněné zásady, jejichž hlubší analýza by byla nad rámec této práce, mají ve vztahu ke kybernetické kriminalitě za následek minimalizaci rizika nevyšetření trestného činu a nepotrestání pachatele. K takové situaci by mohlo dojít např. v případě, kdy by se pachatel mimo území České republiky dopustil jednání, jehož škodlivý následek porušující nebo ohrožující zájem chráněný trestním zákonem by nastal (nebo by alespoň zčásti mohl nastat) právě na území České republiky. Takové jednání je v kyberprostoru velmi časté - příkladem budiž neoprávněný přístup k počítačovému systému (který bude způsobilý naplnit skutkovou podstatu trestného činu uvedeného v § 230 odst. 1 TZ) umístěnému na území České republiky, během kterého je pachatel fyzicky přítomen na území Číny. Nebýt odpovídajících zásad působnosti trestních zákonů, nebylo by takové jednání vůbec postižitelné českým trestním právem.

Z výše uvedených zásad rozhodných pro nalezení jurisdikce, které mají svou obdobu v právních řádech většiny vyspělých států, vyplývá, že u multiteritoriálních nebo distančních deliktů[83] mohou v zásadě nastat dvě sporné situace: buď se stát snaží svou jurisdikci rozšířit na úkor jiných a posuzovat konkrétní čin dle svého práva (pak se jedná o *pozitivní konflikt*),

---

[81] Rozsudek Stálého dvora mezinárodní spravedlnosti ze dne 7. 9. 1927, publikovaný v: *Publications of the Permanent Court of International Justice, Series A - No. 10; Collection of Judgments*. Leyden, A. W. Sijthoff's Publishing Company, 1927. Dostupné také z www: http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm [citováno dne 9. října 2013]

[82] ŠÁMAL, P. a kol. *Trestní zákoník*. 2. vydání, Praha, C. H. Beck, 2012. Str. 68 a násl.

[83] Viz kapitola 2.1.3.

nebo naopak svou působnost popírá a nechce své právo uplatnit vůbec (tehdy nastane *negativní konflikt).*

2.3.2 Negativní konflikty

K negativním konfliktům dojde zpravidla tehdy, pokud škodlivý následek nastane na území státu, ale osoby činné v trestním řízení odmítnou právo aplikovat. K tomu může dojít i u běžných deliktů bez jakéhokoliv mezinárodního prvku. Samozřejmě se v tomto případě nejedná o mezinárodní konflikt jurisdikcí, ale o situaci, kdy stát vyjádří vůli se věcí nezabývat pro domnělou neexistenci působnosti práva v daném případě. Příkladem je odložení případu trestného činu pomluvy Policií České republiky s odkazem na jeho uskutečnění na diskusním fóru na Internetu, pročež údajně nešlo prokázat spáchání trestného činu. V následném řízení o stížnosti pro porušení zákona Nejvyšší soud rozsudkem[84] shledal porušení zákona a konstatoval, že vyšetřovatel nezjistil řádně skutkový stav věci a neprovedl všechny dostupné důkazy.[85]

Negativní konflikty jurisdikcí vytváří zejména snaha vyhovět mezinárodněprávní *zásadě nevměšování se do záležitostí cizích států*. Stát totiž nemůže vykonávat svou moc na území jiného státu, neboť by narušil cizí suverenitu. Typicky pokud na území státu A není pachatel fyzicky přítomen a ani není možné zajistit jeho technické prostředky včetně telekomunikační infrastruktury, je v praxi téměř nemožné jej efektivně stíhat pouze orgány státu A.[86] Stát A proto raději svou jurisdikci na daný případ nevztáhne, čímž nechá prostor pro jurisdikci státu B, kde nejen že nastal škodlivý následek, ale i kde bylo jednáno. Pokud ale ve státě B není dané jednání trestné, pravděpodobně nebude pachatel nikdy potrestán.

V zájmu mezinárodního společenství je zrušení tzv. *bezpečných přístavů kybernetické kriminality*. Nástrojem k jejich omezení jsou mezinárodní smlouvy, jejichž smluvní státy se zavazují prohlásit daná jednání za trestná a zajistit jejich efektivní stíhání a spolupráci ohledně těchto trestných činů s jinými smluvními státy. Nejvýznamnější takovou smlouvou je Úmluva o počítačové kriminalitě, o níž bude pojednáno v kapitole 4.

---

[84] Rozhodnutí č. 4 Tz 265/2000, dostupné z www.nsoud.cz.

[85] POLČÁK, R. *Právo na internetu: Spam a odpovědnost ISP.* Brno, Computer Press, 2007. Str. 1-2.

[86] POLČÁK, R. *Internet a proměny práva*. Praha, Auditorium, 2012. Str. 117.

2.3.3 Pozitivní konflikty

Zatímco negativní konflikty narážejí na zásadu nevměšování se, pozitivní konflikty jsou ohraničeny zásadou *nevydávání vlastních státních příslušníků* k trestnímu stíhání či k výkonu trestu. Ta je v českém právním řádu[87] zakotvena v § 10 odst. 1 TZ.[88] Pokud tedy český občan spáchá na území České republiky distanční delikt, jehož škodlivý následek nastane i v jiných státech, nebude tento občan vydán k zahraničnímu stíhání, ale bude stíhán dle českého práva. Problematičtější by byla situace, kdy by dané jednání nebylo trestné dle českého právního řádu, ale podle právních řádů, kde nastal škodlivý následek, ano. Trestní stíhání pachatele by v České republice nebylo vůbec zahájeno. To ale nevylučuje zahájení trestního stíhání pachatele v jiném státě.

Obdobným problémem se zabývaly německé soudy v případu Geralda Fredricka Töbena,[89] který vyvolal v Německu diskuze o mezích svobody projevu. Tento australský občan německého původu zveřejnil na své webové stránce (umístěné na australském serveru) texty bagatelizující holocaust. Právní řád Austrálie chápe svobodu slova poměrně široce a toto jednání nepovažuje za trestné. Jinak je tomu ovšem z pohledu německého práva, podle kterého byla naplněna skutková podstata německého trestného činu podněcování.[90] Zveřejnění daných textů na Internetu bylo podle německého Spolkového soudního dvora způsobilé narušit veřejný pořádek v Německu, neboť webová stránka obsahující tyto texty byla přístupná i z území Německa. To samotné ale pro založení působnosti cizího trestního práva nestačí, protože v takovém případě by tento případ podléhal jurisdikci libovolného jiného státu, v němž byly Töbenovy webové stránky dostupné. Soud tak vyžadoval jako další podmínku i prokázání tzv. mezinárodním právem odůvodnitelného hraničního určovatele (*völkerrechtlich legitimierenden Anknüpfungspunkt)*. Tento určovatel soud spatřoval v tom,

---

[87] Zatímco ale zásada nevměšování se je univerzální zásadou mezinárodního práva, zásada nevydávání vlastních státních příslušníků je zcela v kompetenci národního práva.

[88] § 10 odst. 1 TZ: *„Občan České republiky nemůže být vydán cizímu státu k trestnímu stíhání ani k výkonu trestu."*

[89] Rozsudek Bundesgerichtshof (Spolkový soudní dvůr, nejvyšší instance v trestních věcech Spolkové republiky Německo) 1 StR 184/00 ze dne 12. 12. 2000, publikovaný v BGHSt 46, 212. Dostupné také z www: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=20678&pos=0&anz=1

[90] Trestný čin *Volksverhetzung* je popsán v § 130 německého trestního zákoníku (*Strafgesetzbuch*). Součástí této skutkové podstaty, kterou překládám jako „podněcování", je i (překlad autor): *„veřejné schvalování, popírání nebo zlehčování jakéhokoliv trestného činu spáchaného pod vládou národního socialismu popsaného v § 6 odst. 1 zákona „Völkerstrafgesetzbuch" způsobem způsobilým narušit veřejný pořádek,"* za což může být pachatel potrestán trestem odnětí svobody až na pět let nebo peněžitou pokutou.

že daný text - ač byl psán v anglickém jazyce - měl výhradní vztah pouze k Německu, což vyplývalo z proklamací textu adresovaných německému obyvatelstvu.[91]

Nutno podotknout, že citovaný rozsudek sklidil značnou kritiku z řad odborné veřejnosti, a to nejen kvůli výše uvedenému. Zejména bylo často vytýkáno, že požadavek mezinárodním právem odůvodnitelného hraničního určovatele nezabrání rozsáhlému pronikání jurisdikce i do států, v nichž jsou dotčená jednání nejen beztrestná, ale případně i ústavně zaručena - což je ve zřejmém rozporu s výše uvedenou zásadou nevměšování.[92] Příliš horlivé hledání hraničních určovatelů by mohlo vést například k situaci, kdy bude při vstupu do Saúdské Arábie zadržen a pro mravnostní trestný čin odsouzen výrobce dámského prádla, který se na Internetu prezentuje katalogem obsahujícím fotografie žen ohrožující mravnost saúdských Arabů.[93] Z pohledu evropské kultury lze takový důsledek hodnotit jako nepříliš akceptovatelný.

Na druhou stranu je jistě nežádaná situace, kdy skupina hackerů provádí z území státu A kybernetické útoky vůči státu B. Pokud by toto jednání bylo trestné jen ve státě B, při aplikaci postupu podobného jako v případě Töben by tento stát mohl založit svou jurisdikci. Přesto kritici rozhodnutí Töben požadují, aby jurisdikce u multiteritoriálních deliktů byla založena primárně místem jednání, zatímco jurisdikce dle místa následku by byla možná jen v případech, kdy je jednání trestné i podle práva státu místa jednání, popřípadě pokud místo jednání nepodléhá žádné státní moci.[94] Zjevná nevýhoda takového přístupu je vznik dalších bezpečných přístavů (viz výše). Dokud pachatel nevstoupí na území státu B (stát místa účinku), bez odpovídajících diplomatických a smluvních mechanismů upravujících spolupráci v trestních věcech a vydávání osob nemůže stát B své trestní právo nijak vynucovat. Spolupráce je ale často zdlouhavá, komplikovaná a formalizovaná,[95] na globální úrovni navíc i nejednotná.

---

[91] Čl. 6 písm. c) části D rozsudku citovaného v referenci č. 89.

[92] VALERIUS, B. *Zum Anwendungsbereich nationaler Rechtsordnungen im Zeitalter des Internets.* In: HERCZEG, J. HILGENDORF, E. GŘIVNA, T. (Hrsg). *Internetkriminalität und die neuen Herausforderungen der Informationsgesellschaft des 21. Jahrhunderts*. Praha, Wolters Kluwer, 2010.

[93] MALEK, K. *Strafsachen im Internet*. Heidelberg, Müller, 2005. Str. 20.

[94] VALERIUS, B. *Zum Anwendungsbereich nationaler Rechtsordnungen im Zeitalter des Internets.* In: HERCZEG, J. HILGENDORF, E. GŘIVNA, T. (Hrsg). *Internetkriminalität und die neuen Herausforderungen der Informationsgesellschaft des 21. Jahrhunderts*. Praha, Wolters Kluwer, 2010.

[95] POLČÁK, R. *Internet a proměny práva*. Praha, Auditorium, 2012. Str. 115 - 116

Mé stanovisko je na straně kritiků přístupu německého soudu. Pro řešení pozitivních konfliktů vidím východisko spíše než v hledání hraničních určovatelů v primární jurisdikci dle místa jednání, kdy bude jednání stíhatelné státem místa následku jen v případě oboustranné trestnosti. Ačkoliv by takový princip vedl ke vzniku dalších bezpečných přístavů, více by odpovídal požadavkům na právní jistotu. Zejména u kontroverzních a jednotlivými státy i kulturami různě vykládaných otázek jako svoboda projevu, mravnost nebo autorská práva může být právní jistota jednotlivce zasažena právními řády povyšujícími jednotlivce na pachatele, aniž by dotyčný o těchto právních řádech ve svém životě kdy slyšel.

Pro omezení počtu bezpečných přístavů lze využít rozsáhlých diplomatických metod, jak přesvědčit tyto státy k zavedení trestnosti daného činu na jejich území. Momentálně nejnadějnějším počinem je již několikrát zmíněná Úmluva o počítačové kriminalitě, vedle této mezinárodní smlouvy ale mají státy možnost uzavírat i bilaterální dohody upravující trestnost některých jednání.

3. FORMY PÁCHÁNÍ TRESTNÉ ČINNOSTI V KYBERPROSTORU

Kyberprostor je s ohledem na svá specifika[96] živnou půdou pro rozsáhlou skupinu protiprávních jednání. Zaměříme-li se jen na jednání poškozující nebo ohrožují zájmy chráněné trestním zákonem, stále bude tato skupina značně nestejnorodá. Kybernetickou kriminalitu lze rozčlenit dle různých hledisek, ale žádná z možných kategorizací není jednoznačná a vždy se některé skupiny budou vzájemně prolínat. Pro účely této práce si vybírám klasifikaci kybernetické kriminality dle role, jakou hraje výpočetní technika při páchání trestné činnosti.[97] Právě podle tohoto kritéria rozlišuje Úmluva o počítačové kriminalitě jednotlivé skutkové podstaty.

Výpočetní technika může při páchání trestné činnosti figurovat jako:

- **předmět trestné činnosti**, tj. výpočetní technika je cílem útoku. Tyto aktivity jsou často nazývány jako útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů. Do této kategorie řadím vedle různých druhů hackingu i sociální inženýrství.
- **nástroj trestné činnosti v rukou zločince**. Může se jednat o některý z trestných činů souvisejících s počítačem, např. o rozličné varianty počítačových podvodů.
- **prostředí, v němž se tato činnost odehrává.** Do této skupiny spadají trestné činy související s obsahem a trestné činy související s porušením autorského práva a práv příbuzných autorskému právu.

Cílem této kapitoly je popsat uvedené aktivity. Místy bude nezbytné v textu rozebírat i zevrubná technická specifika těchto aktivit. Ta mají podstatný význam pro trestněprávní kvalifikaci, o níž bude pojednáno v kapitole 5. Protože je však množství popisovaných aktivit skutečně vysoké, bude nutné uchýlit se ke značné stručnosti až zkratkovitosti. Více prostoru bude věnováno jen první skupině, protože právě hacking nejvíce souvisí s tématem kybernetické bezpečnosti, na které se v diplomové práci pokouším zaměřit.

3.1 Útoky proti počítačovým systémům a počítačovým datům

K těmto útokům patří zejména situace, kdy jsou počítačová data pod útokem osob, které k těmto útokům využívají jiných počítačových systémů. Rizikem pro důvěrnost,

[96] Viz kapitola 2.1.

[97] JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007. Str. 19 - 20.

integritu a dostupnost předmětu útoku je ale velmi často i možnost získávání a zneužívání dat, k nimž dochází využitím nikoliv jiného počítačového systému, ale toliko osob oprávněných s napadenými systémy nakládat. K takovým případům řadím i metody sociálního inženýrství. Všemi naznačenými příklady se bude zabývat tato podkapitola.

Bezpečnostní hrozby[98] pro počítačová data mohou být objektivního rázu, kdy takové hrozby nemají původ v lidském faktoru. Může se jednat o přírodní katastrofy nebo výpadek napětí. Hrozby subjektivního charakteru jsou naproti tomu zaviněné lidmi, ať už úmyslně či nedbalostně.[99] Všemi druhy hrozeb se musí zabývat obor kybernetické bezpečnosti, neboť všechny představují významná nebezpečí pro počítačové systémy. Kybernetickou kriminalitou jsou ale jen subjektivní hrozby, pročež další text bude uvažovat jen tyto.

Z důvodu proměnlivosti kyberprostoru a jeho nepřetržitého vývoje je zřejmé, že se neustále objevují nové hrozby. Konečná taxonomie hrozeb je sice nesnadná, ale například dle charakteru hrozby lze hrozby rozdělit do tří velkých skupin: hrozby základní, aktivační a podkladové.[100] Působení některé ze *základních hrozeb* bezprostředně směřuje k porušení důvěrnosti, integrity nebo dostupnosti předmětu útoku. Základní hrozby jsou právě čtyři, konkrétně únik informací, narušení integrity, nelegitimní užití a potlačení služby. Podstatou prvních tří jmenovaných hrozeb je umožnění neautorizovanému subjektu jednat způsobem, který je jinak umožněn jen určitému okruhu subjektů. Může tak dojít k zachycení informací a dat neautorizovaným subjektem (*únik*), nebo ke změně, smazání nebo vytvoření nových počítačových dat neautorizovaným uživatelem (*narušení integrity*), nebo k neomezenému použití předmětu útoku neautorizovaným subjektem, přičemž na rozdíl od hrozby narušení integrity zde nemusí dojít k vytváření, změně či smazání stávajících dat (*nelegitimní užití)*. Zbývající hrozba *potlačení služby* je způsobilá zabránit přístupu autorizovaného subjektu k informacím či datům.

Pro vznik rizika základní hrozby je obvykle potřeba součinnosti několika různých faktorů - někdy zcela náhodných skutečností, někdy naopak úmyslných jednání využívajících jiných hrozeb. Může jít jednak o využití *aktivačních hrozeb*, které se pokoušejí základní

---

[98] Základní pojmy kybernetické bezpečnosti, jako bezpečnostní hrozba, aktiva nebo útok, byly vysvětleny v referenci č. 35.

[99] POŽÁR, J. a kol. *Základy teorie informační bezpečnosti.* Praha, Vydavatelství Policejní akademie České republiky, 2007, str. 23 a násl.

[100] K této taxonomii hrozeb a bližšímu vysvětlení jednotlivých druhů hrozeb viz JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007. Str. 21 - 24.

hrozbu cíleně aktivovat, a jednak o využití *podkladových hrozeb*, které se nesnaží aktivovat základní hrozbu přímo, ale představují potenciální hrozbu využitelnou pro realizaci až několika základních hrozeb. Zároveň platí, že jedna a tatáž hrozba může být kvalifikována jako základní, ale v jiné souvislosti může být hrozbou podkladovou nebo aktivační. Vztah všech tří skupin hrozeb považuji za vhodné ilustrovat na následujícím příkladu.

Osoba autorizovaná k práci se zabezpečeným počítačovým systémem si heslo k němu zapíše na list papíru. Už jen tím se pro počítačový systém zvýší riziko základní hrozby úniku informace, neboť informaci o přístupovém heslu mohou poměrně snadno získat neautorizované subjekty. Tato hrozba bude ve vztahu k neautorizovanému subjektu, který se listu papíru s heslem skutečně zmocní, hrozbou podkladovou. Neautorizovaný subjekt totiž může kdykoliv sám přístupového hesla využít a vydávat se tak za jiného uživatele, využívaje všech jeho přístupových práv k počítačovému systému, včetně práv k vytváření, změně nebo smazání dat. Proto se okamžikem zisku informace o přístupovém heslu rapidně zvýší riziko základní hrozby narušení integrity. Ovšem znalost přístupového hesla poskytne zkušenému uživateli mimo jiné možnost přihlásit se k zabezpečenému počítačovému systému a úpravou jeho nastavení vytvořit vzdálený přístup, díky čemuž získá nerušený a utajený přístup k údajně zabezpečenému systému například ze svého osobního počítače. Z toho plyne, že hrozba narušení integrity je nyní hrozbou aplikační, jejíž realizací se přímo zvýší riziko hrozby nelegitimního použití. Tento příklad demonstruje mimo jiné i skutečnost, že ochrana počítačových systémů a počítačových dat by měla být skutečně komplexní, protože riziko hrozeb mohou zvyšovat i skutečnosti nezávislé na technickém zabezpečení počítačového systému.

Z uvedené taxonomie vyplývá zejména poměrně jasné vymezení čtyř základních hrozeb, jejichž význam je pro počítačové systémy zásadní. Riziko aplikačních či podkladových hrozeb není proto z pohledu počítačových systémů tak fatální, neboť jejich uskutečněním samo o sobě nevznikne přímá škoda, ale „pouze“ se zvýší riziko základních hrozeb. Proto pachatelé kybernetické kriminality zaměřují své nástroje zejména na realizaci těchto čtyř základních hrozeb.

3.1.1 Hacking a jeho formy

Význam slova ***hack*** v posledních desetiletích prošel značným vývojem. Pro první generaci hackerů, tvořenou zejména studenty univerzity MIT (Massachusetts Institute of Technology) počátkem osmdesátých let, hack obecně představoval důmyslné a inovativní hardwarové nebo softwarové řešení programátorského problému, které nepůsobí nikomu nové

komplikace, ale naopak překonává ty stávající. Pokud hacker v tomto významu někomu obtíže způsobil, jednalo se obvykle jen o neškodné žertíky, jejichž realizace představovala pro hackera určitou intelektuální výzvu i zábavu.[101] Hackeři první generace byli skutečnými odborníky v oblasti výpočetních technologií, kteří se sdružovali do komunit za účelem bezplatného sdílení svých znalostí. Princip všeobecné dostupnosti veškerých informací se stal základem hackerské etiky. Díky technologickému rozvoji se hackerské praktiky stávaly dostupnějšími stále širšímu okruhu osob, dokonce i znalostně značně méně vybaveným jedincům. Hackerská etika kázající o svobodě v kyberprostoru se pro mnohé stala svůdným ospravedlněním kriminálních praktik, které ale ve skutečnosti stály v přímém rozporu s morálními hodnotami hackerské subkultury. Protože pravověrní hackeři vždy jednají jen z nemateriálních, nezištných důvodů, kriminálními praktikami v kyberprostoru opovrhují a distancují se od nich. Přesto se pojetí hackera tak, jak jej chápe dnešní společnost, blíží spíše nebezpečnému zločinci než eticky jednajícímu odborníku v oblasti výpočetních technologií.[102]

V hackerských komunitách se pohybují různé typy osobností. Lze je zařadit do dvou skupin dle již naznačeného kritéria motivace pro jejich působení v kyberprostoru. Vede-li k motivaci pro prolamování ochranných prvků samotná touha po dobrodružství či zábavě, snaha prokázat vlastní intelektuální převahu nebo vyniknout v rámci komunity, to vše bez potřeby získaná data jakkoliv využít či poškodit, lze mluvit o *hackingu*. Pokud je ale hlavní motivací pro uvedené jednání v kyberprostoru finanční zisk nebo jiné uspokojení plynoucí z využití či poškození získaných dat, jedná se o *cracking*. Jako matoucí se může jevit skutečnost, že jako cracking je ale též označována specifická metoda, kdy jsou z počítačového programu neoprávněně odstraněny prvky technicky zajišťující ochranu programu autorským právem. Proto je vhodnější namísto rozdělování na hackery a crackery používat tzv. kloboukové dělení. Zde je kritériem též motivace - skupině hackerů popsaných výše odpovídá označení „white hats“, skupině crackerů „black hats“, a jako neutrální skupina se označuje „grey hats“.[103]

---

[101] MCQUADE, S. C. *Encyclopedia of cybercrime.* Westport, Conn, Greenwood Press, 2009. Str. 87 - 89.

[102] JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007. Str. 47 - 58.

[103] Blíže k těmto skupinám hackerů srov. POŽÁR, J. a kol. *Základy teorie informační bezpečnosti.* Praha, Vydavatelství Policejní akademie České republiky, 2007, str. 112 a násl, nebo též srov. JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007. Str. 54 - 56.

White hats bývají zaměstnáni u obchodních společností zaměřených na vývoj počítačových systémů, které hackeři chrání před útoky black hats. Jednak odhalují již skutečně provedené útoky, jednak vyhledávají nové slabiny počítačového systému a pronikají do něj obdobným způsobem, jakým by do něj pronikal skutečný útočník - ovšem se svolením majitele počítačového systému. Motivem jejich útoků je napomáhat k optimalizaci bezpečnostních řešení. White hats zásadně ctí výše naznačenou hackerskou etiku. White hats mohou nabízet své služby i veřejnosti. Klienti si je mohou najmout například k provedení analýzy svého počítačového systému nebo sítě.

Jako *grey hats* se označují hackeři, kteří se do počítačových systémů prolamují bez vědomí jejich majitelů, ale nepůsobí v nich žádné závažné škody. Motivací jim může být pouhá zábava či recese, ale často po provedení útoku kontaktují administrátora napadeného počítačového systému, uvědomí jej o existující chybě a nabídnou její opravu, obvykle za drobnou úplatu. Zvláštní motivací je i snaha o kariérní růst, kdy si hackera díky provedenému neškodnému, ale sofistikovanému útoku mohou všimnout prestižní softwarové společnosti a zaměstnat jej pro jeho odborné schopnosti.

Black hats prolamují ochranné prvky s cílem získat výhodu pro sebe nebo pro své zaměstnavatele. Tím často bývá nelegální organizace, která může například získaná data a důvěrné informace dále prodávat. V souvislosti se stále častěji v médii zmiňované tzv. „informační válce“ může být zaměstnavatelem hackera i stát. Součástí pracovní náplně některých týmů hackerů ve službách státu mohou být i útočné praktiky,[104] čímž lze tyto hackery zařadit do skupiny black hats. K black hats lze řadit i hackery - aktivisty neboli hacktivisty, kteří se pokoušejí vnutit zbytku společnosti své politické přesvědčení využitím hackerských metod, v současnosti zejména úpravou webových stránek nebo DoS útokem.[105]

---

[104] Od roku 2013 jsou útočné praktiky v kyberprostoru součástí doktríny americké armády. Dle US Cyber Command disponuje armáda specializovanými (překlad autor) *„útočnými týmy, které budou použity k obraně národa, pokud tento bude napaden v kyberprostoru.“* HRUSKA, J. *US Cyber Command Admits Offensive Cyberwarfare Capabilities, Fundamental Shift In US Doctrine* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://hothardware.com/News/US-Cyber-Command-Admits-Offensive-Cyberwarfare-Capabilities-Fundamental-Shift-In-US-Doctrine/

[105] Dnešní hacktivisté jsou za využívání těchto metod kritizováni dokonce i představiteli zakladatelů hacktivismu. Původní myšlenkou hacktivismu byla totiž podpora lidských práv za využití technologických prostředků. Dle kritiků lze těžko spatřovat podporu lidských práv tím, že někdo změní text na webové stránce nebo omezí přístup k ní, neboť tyto prostředky prakticky brání svobodě projevu. Blíže viz MILLS, E. *Old-time hacktivists: Anonymous, you've crossed the line* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://news.cnet.com/8301-27080_3-57406793-245/old-time-hacktivists-anonymous-youve-crossed-the-line/

Zvláštní skupinu hackerů tvoří *script kiddies.* Jedná se o amatéry nedisponující dostatečnými schopnostmi, kteří neumí vytvářet vlastní hackerské nástroje. Pouze bez znalosti širších souvislostí používají programy vytvořené skutečným hackerem. Protože často ani samotné script kiddie neví, jaké následky může program způsobit, jsou hrozby představované touto skupinou velmi nevyzpytatelné. Ačkoliv příslušníci této skupiny mohou například provést DoS útok a užít si krátkodobé pomíjivé slávy, v hackerské komunitě obvykle nejsou za hackery ani považováni.[106] Hacking by měl přinášet nové řešení - tento novátorský prvek však v počínání script kiddies zcela chybí, a pro nedostatek teoretických i praktických technických znalostí je vhodnější označit script kiddies spíše za jakési kvazihackery.

V počátcích hackingu byly k provedení útoku používány zejména *hardwarové nástroje.*[107] Dnes naopak zcela převažují *softwarové nástroje*, neboť tyto je pro hackera mnohem jednodušší a snazší vyrobit či modifikovat. Nadto jsou softwarové nástroje v různých verzích v kyberprostoru široce dostupné. Hackeři pro svou činnost mnohdy podpůrně využívají i *metod sociálního inženýrství.*

Se vzrůstající úrovní zabezpečení počítačových systémů se zvyšují požadavky na kvalitu hackerských nástrojů. Přípravě zcela nových nástrojů se věnuje jen malá část hackerů, ostatní hackeři se zabývají modifikováním stávajících nástrojů. Například zkušení hackeři objeví slabinu v zabezpečení konkrétního internetového prohlížeče a pro její využití vyvinou jednoúčelový nástroj, tzv. ***exploit***, který se následně rozšíří i mimo hackerskou komunitu. Než se o existenci slabiny dozví výrobce internetového prohlížeče a slabinu odstraní, exploit je různými hackery modifikován a vylepšován, aby více odpovídal cílům konkrétního hackera. Exploit je na konci tohoto procesu plně automatizován, takže jej začínají ve velké míře nasazovat i script kiddies. Protože je ale s postupem času slabina výrobcem odstraněna, daný exploit i většina jeho modifikací je aplikovatelný jen na stále zmenšující se skupinu uživatelů, kteří svůj internetový prohlížeč stále ještě neaktualizovali.[108] Exploity ale používají i zodpovědní hackeři ve smyslu white nebo grey hats, kterým usnadní testovat zabezpečení jejich počítačových systémů.

---

[106] JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007. Str. 56.

[107] Jednalo se např. o používání tzv. blue-boxů pro účely phreakingu.

[108] JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007. Str. 60 - 61.

V následujícím textu se pokusím popsat aktuálně nejčastěji používané hackerské nástroje. Není ale mou ambicí popsat veškeré možnosti hackerů. Namísto toho se pokusím vymezit jejich nejobvyklejší nástroje, které pro přehlednost rozděluji dle základních hrozeb, které se v konečném důsledku tyto nástroje pokoušejí realizovat.

1. Nástroje směřující k potlačení služby

Hacker se v tomto případě pokouší vyřadit cíl svého útoku z provozu. Nejčastěji se jedná o útoky typu *Denial of Service* (v překladu potlačení služby; běžně je používáno jen zkratky DoS). Data v napadeném počítačovém systému nejsou trvale zničena a ani nemusí být ohrožena jejich důvěrnost, tj. tento útok není cílen na získání počítačových dat. Útok je totiž veden s cílem zahltit zařízení, na které je útok veden, nebo jeho síťovou infrastrukturu, přičemž se útok pokouší vyčerpat jejich systémové zdroje. V důsledku zahlcení napadený systém přestane být pro své uživatele dostupný. O tom, zda se útočníku podaří systémové zdroje vyčerpat, rozhoduje množství systémových zdrojů, které se mu k útoku podaří mobilizovat. Útoky typu DoS jsou nejčastěji realizovány ve třech variantách.[109]

Varianta *Distributed Denial of Service* (DDoS) počítá s využitím velkého množství zařízení, které v jeden okamžik zahltí přístupovou cestu k cíli útoku nesmyslnými požadavky, v důsledku čehož se cíl útoku stane nedostupným. Tento postup předpokládá dřívější kompromitování velkého množství zařízení škodlivým softwarem, díky kterému útočník bude schopen z každého kompromitovaného zařízení odeslat datové pakety.[110] Útočník se tedy snaží převýšit systémové zdroje cíle útoku součtem systémových zdrojů kompromitovaných zařízení.

Jinou variantou je *zahlcení příkazem ping do sítě cíle útoku*. Obecně příkaz ping umožňuje zjistit existenci spojení mezi zařízeními v rámci jedné sítě. Jedno zařízení odešle na IP adresu druhého skupinu datových paketů, na kterou druhé zařízení připojené v síti odpoví. Příkaz ping odeslaný na adresu sítě a nikoliv konkrétního zařízení vede k tomu, že na něj odpoví všechna zařízení připojená k dané síti. Této možnosti hacker využije. Změní si navenek svou IP adresu na IP adresu cíle svého útoku a odešle příkaz ping na adresu sítě.

[109] Blíže k útoku typu DoS a jeho jednotlivým variantám viz JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007. Str. 66.

[110] Tímto vznikají rozsáhlé sítě (*botnets*) ovládaných zařízení (*zombies*), kterým může útočník naráz zadat jednoduchý příkaz a zombie jej splní. Kromě DDoS útoků lze botnet využít například pro odesílání spamu.

Všechna zařízení v síti poté odpoví na podvrženou adresu, čímž může dojít k zahlcení cíle útoku.

Třetí variantou je útok typu *SYN-flood*, který využívá mechanismu třícestného navázání přenosu[111] v Internetu. Útočníkův klient odešle na server požadavek na navázání přenosu (paket SYN) a server požadavek potvrdí, přičemž očekává závěrečné potvrzení přenosu klientem (paket ACK). Zásadní rozdíl oproti normální komunikaci je v tom, že hacker očekávané potvrzení přenosu již neodešle - toho může docílit například podvržením své IP adresy, v důsledku čehož server odešle datové pakety potvrzující požadavek na zcela jinou IP adresu. Nyní server očekává brzké zahájení přenosu, pro které si již rezervoval systémové prostředky. Své systémové prostředky server znovu uvolní během několika minut. Pokud v této době útočník zašle velké množství paketů typu SYN a současně žádný typu ACK, může vyčerpat volné systémové prostředky cíle útoku, který se tak stane pro všechny uživatele nedostupným.

Všechny uvedené útoky cílené na hrozbu potlačení služby mají společné to, že se jedná o poměrně zastaralé praktiky. Protože proti nim ale neexistuje levná a zároveň účinná preventivní obrana, mohou se projevit jako účinné. Ačkoliv cíle DoS útoků lze obvykle v jednotkách hodin opět zprovoznit, jsou mediálně velmi zajímavé. Proto jsou tyto praktiky užívány zejména hacktivisty. O mediální vděčnosti tématu svědčí případ DoS útoků z března roku 2013, kdy v České republice byly během jednoho týdne napadeny nejznámější české servery - od zpravodajských serverů přes servery bank a mobilních operátorů až po největší český vyhledávač a portál Seznam.cz. I když byly všechny následky útoku velmi rychle odstraněny, mediálním tématem zůstaly po několik týdnů.[112]

---

[111] Třícestné navázání spojení mezi klientem a serverem (tzv. *three-way handshake*) je základem komunikace přes protokol TCP/IP, který je jedním z nejrozšířenějších v Internetu. Za normálních okolností v prvním kroku komunikace klient odešle na server paket s příznakem SYN (značící zahájení synchronizace), na který v druhém kroku server odpoví paketem s příznaky SYN a ACK (*acknowledge* - potvrzená synchronizace) a ve třetím kroku klient ukončí zahajování spojení tím, že odešle paket s příznakem ACK zpět serveru. Server na tento paket čeká obvykle několik minut, během kterých si vyhradí systémové prostředky na očekávané spojení. Blíže viz *CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://www.cert.org/advisories/CA-1996-21.html

[112] Útok byl veden metodou SYN-flood s využitím podvržené IP adresy. Napadené servery vracely datové pakety na podvrženou adresu, což byla adresa skutečného serveru, který byl tímto též napaden a vyřazen z provozu. Dle osobního sdělení jednoho z výše postavených programátorů Seznam.cz bylo otázkou jen několika minut identifikovat útočníka v kyberprostoru a následně zastavit probíhající útok.

2. Nástroje směřující k úniku informací

Pomocí této skupiny nástrojů se hacker pokouší analyzovat konkrétní počítačový systém, aby na základě takto získaných dat zvolil další postup svého útoku, který může směřovat až k narušení integrity nebo k nelegitimnímu užití počítačového systému. Někdy je ale získání dat cílem samo o sobě, zejména pokud útočník získá přístupová hesla.

Časté útoky hackerů začínají analýzou otevřených portů[113] cílového počítačového systému. Útočník použije program typu *port scanner,* kterým se zkusí připojit ke všem otevřeným portům cílového zařízení. Pokud porty odpoví, znamená to, že jsou otevřené. Hacker z otevřených portů zjistí, jaké služby na nich běží, a získá základní představu o operačním systému zařízení, jaké aplikace a v jakých verzích jsou zrovna spuštěné nebo jaká je konkrétní konfigurace zabezpečení systému. Touto metodou tak lze zjistit místa zranitelnosti a na základě toho vybrat konkrétní exploit, který bude použit v další fázi útoku.[114]

Další analytickou metodou je *sniffing,* který je zaměřený na odposlouchání síťového provozu. Program provádějící tuto činnost - sniffer - zachytává datové pakety (buď veškeré, nebo cíleně vybírá jen ty, které jsou pro hackera zajímavé), zasílá je útočníkovi a ten rekonstrukcí získaných dat získá podklad pro zvolení vhodné metody dalšího útoku. Sniffingem lze zjistit mimo jiné též přístupová hesla.[115]

Účinnou metodou je sniffing v kombinaci s *IP spoofingem*. Útočník si nejprve v síti vytipuje dvojici zařízení, která se vzájemně považují za důvěryhodná, a zjistí si jejich IP adresy. Následně hacker zajistí, aby se jeho systém navenek zdál být jedním z dvojice vytipovaných zařízení, tj. podvrhne svou IP adresu, a druhému z dvojice zařízení zašle požadavek na zaslání některých dat. Napadený systém datové pakety sice zašle na IP adresu, kde se skutečně nachází důvěryhodné zařízení, ale útočník je zachytí cestou snifferem. Aby byl útok úspěšný, je vhodné zařízení nacházející se na podvržené IP adrese správně

---

[113] Porty umožňují komunikaci počítače v Internetu. Možných portů je velké množství (až 65 535), jen u části z nich (1 023) je ale pevně definována jejich funkce a jsou přiděleny ke konkrétním službám, jako například ke službám FTP, HTTP, HTTPS, Telnet, SSH, POP3 nebo DNS. JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Druhé vydání, Praha, 2013. Str. 77.

[114] JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007. Str. 64.

[115] Tamtéž, str. 64 - 65.

načasovaným DoS útokem vyřadit z provozu, jinak se napadený počítačový systém dozví, že podvržený počítačový systém žádná data nevyžadoval.[116]

K dalším metodám odposlechu patří technika *man-in-the-middle*, kdy se útočník pomyslně usadí do komunikačního kanálu mezi dvě strany a bez jejich vědomí zachycuje a modifikuje komunikaci.[117] Zákeřné je na této metodě to, že útočník je do jisté míry schopen číst i šifrovanou komunikaci, neboť může zasáhnout do procesu výměny šifrovacích klíčů a nahradit šifrovací klíče svými, přičemž komunikující zařízení budou klíč útočníka považovat za bezpečný klíč protistrany.

Jednoduchým nástrojem, jak zachytit mimo jiné i přihlašovací hesla, je *keylogger* - zařízení, které zachycuje všechny stisky kláves. Lze tak bez vědomí uživatele rekonstruovat veškerý jím zapsaný text.[118] Kromě softwarové verze tohoto nástroje, která získaná data obvykle hned či v pravidelných intervalech odesílá útočníku, existuje i hardwarová varianta. Takový keylogger je drobné zařízení, které zachytává stisky kláves na cestě mezi klávesnicí a skříní počítače.

3. Nástroje směřující k narušení integrity

Jedná se o nástroje, které se útočník pokouší podsunout do napadeného počítačového systému, a s jejich pomocí následně vytvářet, měnit nebo mazat počítačová data. Hackeři mohou těmito programy napadat konkrétní počítačové systémy, které hodlají infiltrovat, nebo se pokoušejí infikovat co největší množství nespecifikovaných počítačových systémů.

Nejproslulejšími a mediálně nejoblíbenějšími škodlivými programy jsou bezesporu *viry a červi*, což jsou programy s autoreprodukční schopností. Napadají konkrétní programy tím, že část jejich kódu nahradí svým. Kód viru se provede po spuštění programu, čímž se virus nainstaluje do počítačového systému, a zároveň se šíří i napadáním dalších souborů počítače. Červi jsou síťovou obdobou virů, šíří se prostřednictvím komunikačních linek mezi zařízeními v síti. Účinky virů i červů jsou různé, nejnebezpečnějším projevem bývá poškození či zničení někdy i všech souborů na pevném disku.[119]

---

[116] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Druhé vydání, Praha, 2013. Str. 76 a 105.

[117] Tamtéž, str. 31.

[118] Tamtéž, str. 53.

[119] POŽÁR, J. a kol. *Základy teorie informační bezpečnosti.* Praha, Vydavatelství Policejní akademie České republiky, 2007, str. 47.

Přístup k počítačovému systému mohou zajistit tzv. *trójské koně*. Jejich kódy jsou součástí jiného nosného programu, který má mít pro uživatele lákavou funkci. Uživatel si nosný program - často nepotřebný software dostupný zdarma na Internetu - vědomě nainstaluje do svého počítače, ale již neví o škodlivém programu v něm působícím. Trójský kůň může poté monitorovat činnost počítače (pak se jedná se o tzv. spyware, který své uplatnění může najít mimo jiné i pro analýzu trhu - program zaznamenává, o jaké webové stránky či produkty se uživatel zajímá, a následně mu zasílá cílenou reklamu), ale existují i podstatně škodlivější varianty, které mohou vést až k ovládnutí počítačového systému hackerem.[120]

Přístup k počítačovému systému umožňují též *backdoors*, což jsou skryté součásti programů využitelné pro obcházení bezpečnostních mechanismů počítačového systému. Backdoors do programu vkládají programátoři při vývoji software například pro účely programátorského testování nebo umožnění pozdějšího auditu systému. Opomenutím odstranění tohoto nástroje jej můžou využít cizí útočníci, a v případě úmyslného ponechání backdoors programátorem jej často využívá též i samotný autor pro narušení integrity počítačového systému.[121]

4. Nástroje směřující k nelegitimnímu užití

Hackeři mohou provádět útoky zaměřené na nelegitimní užití napadeného systému z více důvodů. Mohou se spokojit s tím, že ovládnutý systém používají, aniž by byli autorizovaní či řádně platící uživatelé. Často ale ovládnutý systém využívají pro páchání dalších forem kybernetické kriminality. Ovládnutý systém se může stát například součástí útočníkovy sítě (tzv. botnet) a na jeho pokyn provést DoS útok nebo rozesílat spam. Ovládnutý systém se pak může jevit jako útočník. To jednak snižuje šanci na vystopování skutečného útočníka, jednak komplikuje život majiteli napadeného systému, který může být později stíhán jako pachatel.

K získání úplného přístupu k počítačovému systému mohou vést i některé metody a nástroje, resp. jejich kombinace, popsané výše. Nejpřímočařejším nástrojem k získání přístupu je *prolamovač hesel*, který jako heslo do zabezpečeného systému zkouší zadat různé

---

[120] JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007. Str. 67.

[121] POŽÁR, J. a kol. *Základy teorie informační bezpečnosti.* Praha, Vydavatelství Policejní akademie České republiky, 2007, str. 45.

kombinace znaků, dokud nenarazí na správnou kombinaci. Nalezené heslo program odešle hackerovi. Program v první fázi zkouší tzv. slovníkový útok, kdy postupně zadává všechna známá slova ze své databáze, která jako heslo přicházejí v úvahu (například všechna česká slova). Následně program znovu zkouší všechna slova ze své databáze, ale mírně je obmění, například kombinuje malá a velká písmena. Pokud ani tehdy nenalezne heslo, zkouší útok hrubou silou, kdy postupně zadává všechny možné kombinace znaků. Prolamovač hesel je nepoužitelný u silných hesel, u kterých prolomení může trvat několik tisíc let, a dále tam, kde zabezpečení systému umožní zadat jen několik hesel za sebou, a pokud žádné z nich nebude správné, tak se zablokuje.[122]

Zvláštní metodou vedoucí k nelegitimnímu užití systému je *phreaking*, kdy se útočník - phreaker - napojí na cizí telefonní linku a díky tomu je schopen bezplatně telefonovat nebo používat služeb Internetu, případně odposlouchávat telefonní hovory.[123] Phreaking je velice stará metoda, na jejímž počátku - podobně jako u metody hackingu obecně - převažovala touha samostudiem poznat zákonitosti telekomunikačních linek nad snahou o vlastní peněžité obohacení. Phreakeři mohli pomocí tónu o specifické frekvenci, pro jejichž přehrávání používali speciální zařízení (tzv. bluebox) nebo i méně sofistikované způsoby (hvizd ústy, dětská píšťalka), ovládat telekomunikační systém a spojit se s jakoukoliv jinou telefonní stanicí v síti. Dnešní telekomunikační sítě využití těchto více než čtyřicet let starých „exploitů“ neumožňují, ale stále jsou cílem útoků moderních phreakerů a phreaking jako takový zatím nevymizel.

3.1.2 Metody sociálního inženýrství

Postupy popsané v kapitole 3.1.1 jsou používány buď samostatně nebo v kombinaci, ještě lepších výsledků však útočník může dosáhnout při jejich současném použití s metodami sociálního inženýrství. Tyto tzv. sociotechniky se pokouší podvodným způsobem zneužít lidský element - manipulovat s uživateli kyberprostoru za účelem získání informace nebo jiné významné výhody pro útočníka.[124] Ani nejzabezpečenější počítačové systémy neobstojí při selhání lidského faktoru.

---

[122] Blíže viz www: http://www.viry.cz/hesla-hesla-hesla/ [citováno dne 9. října 2013]

[123] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Druhé vydání, Praha, 2013. Str. 72.

[124] Tamtéž, str. 95.

Ve vztahu k metodám hackingu může mít sociální inženýrství podpůrné postavení, kdy útočník zneužívá lidský element, aby následně mohl provést nebo si výrazně usnadnit hacking. Útočník typicky sbírá co největší množství i na pohled bezvýznamných informací, na základě kterých může například zaměstnance organizace přimět ke sdělení hesla k počítačovému systému. Zaměstnanec přitom vůbec nemusí vědět, že heslo vyzradil útočníkovi. Může ale s útočníkem i vědomě spolupracovat, ať už za úplatu nebo proto, že mu útočník učinil nabídku, kterou zaměstnanec nemohl odmítnout.[125] Z informací o životě zaměstnance, které by mohly být potencionálními hesly (jako je jméno či množství dětí, domácího zvířectva, manželek a podobně), může sestavit seznam slov vhodný pro slovníkový útok a v případě úspěchu získat přístup k počítačovému systému.[126]

Naopak ale může být ve vztahu k sociotechnickým metodám v podpůrném postavení hacking, který je v takové situaci jen nutným nástrojem umožňujícím následný podvod. Typickou ukázkou je *ransomware*. Hacker napadne systém škodlivým softwarem a požaduje zaplacení „výkupného“ za jeho odstranění, a to buď ihned, nebo do několika hodin.[127] Snaha vyděsit či šokovat uživatele a přesvědčit jej, aby co nejdříve zaplatil, je typickou ukázkou sociotechických metod.[128]

Velmi rozšířená je též metoda *phishingu*, kdy se útočník pokouší o krádež identity (v tomto případě je jeho cílem získat a následně zneužít přihlašovací údaje či čísla bankovních karet a účtů) vytvořením podvodné e-mailové zprávy, kterou se tyto údaje snaží vylákat.[129]

---

[125] Různou motivaci pro páchání kybernetické kriminality může mít zaměstnanec organizace - může být nespokojený s pracovními podmínkami, může mu hrozit propuštění, může být vydíraný či podplacený útočníkem pracujícím pro konkurenci, který si jej sociotechnickými metodami vytipoval.

[126] BRECHLEROVÁ, D. Sociální inženýrství. In: *IT Systems, 3/2007*. Dostupný také z www: http://www.systemonline.cz/it-security/socialni-inzenyrstvi.htm [citováno dne 9. října 2013].

[127] V České republice se velmi rozšířeným ransomware roku 2012 stala česká varianta programu, který po spuštění počítače nahradí úvodní obrazovku operačního systému sdělením informujícím o údajném trestním stíhání uživatele pro podezření z kybernetické kriminality. Sdělení je opatřené logem Policie České republiky a výzvou, že systém bude odblokován až po zaplacení peněžité pokuty ve výši několik tisíc korun. Uživateli je citováno několik smyšlených ustanovení, jejichž znění může pro člověka znalého trestního práva působit velice zábavně. Objevily se i varianty s menším množstvím pravopisných chyb a dokonce i IP adresou, lokalitou a fotografií uživatele (získanou ovládnutím webové kamery programem), pročež zpráva dokázala vyděsit množství uživatelů a přesvědčit je k zaplacení „pokuty“. Samozřejmě není jisté, že program po zaplacení počítač odblokuje, resp. že pokutu nebude s odstupem času vymáhat opakovaně, nebo zda program dokonce později nezneužije získané platební údaje oběti.

[128] Blíže viz *Symantec Internet Security Threat Report - 2013* [online]. [citováno dne 9. října 2013]. Str. 50. Dostupné z www: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

[129] Velké uplatnění nachází phishing zejména tam, kde se autor phishingového e-mailu vydává za bankovní ústav. Taková zpráva může vyzývat adresáta (klienta banky), aby pod záminkou změn v oblasti bezpečnostní politiky znovu sdělil své přihlašovací údaje k aplikaci internetového bankovnictví, číslo a heslo ke svému účtu

Příbuznou technikou je *pharming*, která se obejde bez rozesílání e-mailu. Hacker přímo napadne webové stránky např. bankovní instituce a zajistí, aby všichni návštěvníci této webové stránky byli přesměrováni na webovou stránku útočníka, která se vzhledem snaží být přesnou kopií podvržené stránky. Na neobezřetné uživatele, kteří se pokusí přihlásit ke svým účtům, zde ale čekají nástrahy v podobě programů, které si zapamatují jejich uživatelská jména a hesla a odešlou je hackerovi.[130]

3.2 Trestná činnost, při níž je počítačový systém prostředkem jejího páchání

Veškeré činnosti uvedené v kapitole 3.1 popisují případy, kdy útočník musí překonat bezpečností opatření (a tím neoprávněně získat přístup k počítačovému systému), a to pomocí jeho specifických schopností - ať už technických či sociotechnických. Tato podkapitola se zabývá případy, kdy útočník bezpečnostní opatření překonat nemusí, neboť již oprávněný přístup k (jakémukoliv) počítačovému systému má. V počítačovém systému ale buď provede činnost, k níž není fakticky oprávněn, nebo která je z určitého důvodu trestná.

Pachatel této trestné činnosti si vystačí jen s uživatelskými znalostmi počítačových systémů. Jeho jednání v kyberprostoru, z něhož lze vyvodit trestní odpovědnost, má velmi různorodé formy. Může jít o počítačové padělání, jehož pachatel může například změnit údaje v databázi, k níž má legální přístup, ale tato změna údajů je již protiprávní. Může jít o případy pomluvy, kdy pachatel e-mailem rozesílá pomlouvačná nepravdivá sdělení o jiných osobách. Může jít o libovolný případ podvodu - pachatel si zařídí elektronických obchod a zákazníkům po obdržení peněžitého plnění nepošle objednané zboží. Téhož jednání se lze dopustit i v elektronických aukcích.

Podrobný popis veškeré trestné činnosti, pro jejíž páchání lze zneužít prostředků výpočetní techniky, by sám o sobě překročil rozsah této práce. Z pohledu trestního práva je jednání v této kapitole uvedené postižitelné dle klasických skutkových podstat, jejichž popisováním by taktéž tato práce neúnosně narostla. Z těchto důvodů se této skupině nebudu dále věnovat. Jedinou výjimku učiním u spamu, neboť jeho problematika si pro specifičnost technického provádění i pro specifičnost právní regulace zaslouží alespoň stručnou pozornost.

---

apod. E-mail dokonce obsahuje odkaz na podvržené webové stránky, které na první pohled vypadají přesně jako webové stránky podvržené instituce. Blíže viz MCQUADE, S. C. *Encyclopedia of cybercrime.* Westport, Conn, Greenwood Press, 2009. Str. 139 - 142.

[130] Blíže viz MCQUADE, S. C. *Encyclopedia of cybercrime.* Westport, Conn, Greenwood Press, 2009. Str. 140.

3.2.1 Spam

Spam je nevyžádané obchodní sdělení, obvykle rozesílané elektronickou formou hromadně velkému množství adresátů naráz.[131] Rozesílatelé spamu pomocí tzv. spambotů procházejí webové stránky a veškeré e-mailové adresy zaznamenávají do seznamů, který pak využívají jako seznam adresátů spamu. K odesílání spamu je častou používán botnet (viz kapitola 3.1.1), takže skutečný odesílatel spamu o jeho odeslání ani nemusí vědět. Vedle faktu, že neustálé odmazávání spamu obtěžuje adresáta, může vzniknout i trestní odpovědnost - zejména v případech, kdy se prostřednictvím spamu přenáší škodlivý software či jinak protiprávní obsah. Problémem pro rozesílatele spamu může být i uveřejňování e-mailových adres jednotlivých „obětí", protože ty mohou za určitých okolností být osobním údajem.[132] Autoři některých spamů se pokoušejí působit na adresáty sociotechnickými metodami s cílem vylákat z adresátů finanční prostředky. Tato skupina spamů se označuje jako s*cam,* a lze sem zařadit mimo výše popsané metody phishingu nebo ransomware i tzv. *scam nigerijského typu,* jehož adresát je podvodně příslibem obrovského zisku nalákán k zaplacení určité finanční částky.

Jak vyplývá z analýz každoročně prováděných firmou Symantec, v posledních letech celkový objem spamu klesá a jeho podíl ze všech e-mailových zpráv se v roce 2012 ustálil na 69 %. Pokles spamu je ale zčásti způsoben jeho pouhým přesunem na sociální sítě.[133]

3.3 Trestná činnost související s obsahem a s porušením práv duševního vlastnictví

Specifickou kategorií trestné činnosti jsou případy, kdy uživatelé kyberprostoru rozšiřují obsah, jehož samotná existence je nebezpečná, protože *již při jeho vytvoření byl porušen zájem chráněný trestním zákonem*. Typicky se jedná o obsah zobrazující dětskou pornografii nebo obsah, jehož vznik neoprávněně zasáhl do zákonem chráněných práv k autorskému dílu, například vytvoření neoprávněné kopie počítačového programu. Vysoké

---

[131] MCQUADE, S. C. *Encyclopedia of cybercrime.* Westport, Conn, Greenwood Press, 2009. Str. 169 - 171.

[132] Podle § 4 písm. a) zák. č. 101/2000 Sb., o ochraně osobních údajů, se osobním údajem rozumí *„jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat."* Pokud tedy e-mailová adresa obsahuje jméno a příjmení, podle kterého lze adresáta identifikovat, je osobním údajem a pro nakládání s osobními údaji platí zvláštní režim.

[133] Blíže viz *Symantec Internet Security Threat Report - 2013* [online]. [citováno dne 9. října 2013]. Str. 42. Dostupné z www: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

intenzity ale může nabývat i nebezpečnost obsahu vyplývající nikoliv ze samotné jeho existence, ale jen z *potenciálního zneužití*. Proto existuje oprávněná potřeba jeho trestněprávní regulace. Šíření obsahu tedy naplňuje některou ze skutkových podstat uvedených v trestním zákoníku, přičemž výpočetní technologie vytvářejí prostředí, které šíření umožňuje či usnadňuje.[134]

K šíření škodlivého obsahu může jednoduše posloužit i prosté vytváření webových stránek obsahující texty či audiovizuální objekty porušující nebo ohrožující zájem chráněný trestním zákonem. Tím mohou být různé dehonestující webové prezentace, stránky obsahující návody k trestné činnosti[135] nebo stránky vybízející k extremismu.[136]

Další formou šíření škodlivého obsahu je využití diskusních serverů nebo sociálních sítí, jejichž uživatelé díky pocitu anonymity ventilují své myšlenky a výrazivo způsobem mnohdy překračujícím morální, ale též i trestněprávní meze. Nejčastěji se lze setkat se zásahy do osobnostních práv, šíření poplašných zpráv (tzv. hoax), výzvy k rasové či jiné nesnášenlivosti, propagace extrémistického hnutí, návody k trestné činnosti, nekalosoutěžních jednání nebo porušování autorských práv a jiných práv duševního vlastnictví.[137]

Specifickým prostředím umožňujícím účinně porušovat autorská práva jsou tzv. warez fóra, diskusní servery založené za účelem sdílení autorsky chráněných děl. Příslušníci komunit tato fóra provozujících jsou jednak crackeři pracující na prolamování ochranných prvků programových produktů, jednak osoby zajišťující funkci warez fóra - od jeho technické správy přes propagaci fóra na Internetu až po zajišťování agresivní reklamy na obskurní webové stránky, která provoz warez fóra živí.[138] Dnes jsou warez fóra používána zejména na šíření cracků (programů, které po nainstalování automaticky odstraní ochranné prvky softwarových produktů) a hyperlinků. Umístěním hyperlinku (internetového odkazu), který

---

[134] ŠIMOVČEK, I. a kol. *Kriminalistika.* Plzeň, Aleš Čeněk, 2011. Str. 370.

[135] V České republice například webová stránka Zdeňka Adamce, která se zabývala phreakingem a dále informacemi užitečnými pro tzv. darkery, kteří se bavili „zhasínáním" velkých podniků či vesnic zkratováním elektrického vedení. Adamec na své stránce poskytoval podrobné návody, jak vyvolat „zatemnění" v co největším rozsahu, pročež byl Adamec následně trestně stíhán. Adamec do širšího povědomí veřejnosti pronikl svým sebeupálením na Václavském náměstí v roce 2003. TOLAR, O. *Lze dospět k sebevraždě díky Internetu?* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://www.lupa.cz/clanky/lze-dospet-k-sebevrazde-diky-internetu/

[136] Viz případ G. F. Töbena popsaný v kapitole 2.3.3.

[137] POLČÁK, R. *Právo na internetu: Spam a odpovědnost ISP.* Brno, Computer Press, 2007. Str. 94 a násl.

[138] JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007. Str. 68 - 74 a str. 105 - 106.

přímo vede ke stažení souboru se škodlivým obsahem, dochází též k šíření tohoto škodlivého obsahu.[139]

Velmi oblíbenou metodou k šíření souborů se staly peer-to-peer sítě a z nich odvozené torrenty. Uživatelé těchto sítí nestahují soubor z jednoho serveru, ale od ostatních uživatelů sítě daný soubor sdílejících. Obvykle uživatel stahuje soubor, který zároveň dále sdílí, čímž může šířit škodlivý obsah.[140]

[139] POLČÁK, R. *Právo na internetu: Spam a odpovědnost ISP.* Brno, Computer Press, 2007. Str. 102 a násl.

[140] JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha, Grada Publishing, 2007. Str. 106.

4. EVROPSKÉ A MEZINÁRODNÍ PŘEDPISY VZTAHUJÍCÍ SE KE KYBERNETICKÉ KRIMINALITĚ A KYBERNETICKÉ BEZPEČNOSTI

Pro účinné potírání kybernetické kriminality, která má výrazný specifický přeshraniční charakter,[141] je potřeba spolupráce na úrovni států. Jako nejvýznamnější oblasti této mezinárodní spolupráce spatřuji následující:

- sjednocení pojmosloví. Jak bylo naznačeno v první kapitole této práce, stále panují určité nepřesnosti v legislativním chápání některých pojmů.
- upravení odpovědnosti poskytovatelů služeb. Ta je nezbytná pro vymahatelnost práva v kyberprostoru.[142]
- harmonizace skutkových podstat. Samotná hrozba trestněprávní sankce za určité jednání v kyberprostoru spáchané z území jednoho státu nemůže spolehlivě uchránit před tím samým jednáním provedeným z místa spadajícího pod jurisdikci státu, kde toto jednání postižitelné není.
- harmonizace procesních oprávnění. Má-li být jednání popsané v harmonizovaných skutkových podstatách stíháno jako trestné činy, je třeba osobám činným v trestním řízení stanovit pravomoc k jejich účinnému potírání a zároveň minimalizovat zásahy do soukromí uživatelů kyberprostoru při vynucování práva.
- efektivní spolupráce ve vyšetřování. Osoby činné v trestním řízení často potřebují k úspěšnému vyšetření kybernetické kriminality rychlou spolupráci se zahraničními subjekty.
- zajištění společného bezpečného kyberprostoru. Obava z kyberteroristických útoků cílených na kritickou infrastrukturu vede řadu států k přijímání legislativy zaměřené na kybernetickou bezpečnost. Protože snaha zajistit bezpečnost jakékoliv části kyberprostoru je do určité míry ovlivněna bezpečností jeho jakékoliv jiné části, je v zájmu států na bezpečném kyberprostoru stále spolupracovat.

Mezinárodněprávním dokumentem, který upravuje všechny výše uvedené oblasti s výjimkou otázek upravení odpovědnosti poskytovatelů služeb, je Úmluva Rady Evropy

[141] K problému teritoriální neomezenosti kyberprostoru viz kapitola 2.1.3.

[142] K problému vymahatelnosti práva v kyberprostoru viz kapitola 2.1.2.

o počítačové kriminalitě, kterou představím v kapitole 4.1. Velké množství dokumentů dále vzniklo na půdě Evropské unie. Těmi nejvýznamnějšími se budu zabývat v kapitole 4.2.

Záměrně se v této kapitole budu více zabývat jen nejvýznamnějšími a nejaktuálnějšími prameny práva, které souvisejí s otázkou kybernetické bezpečnosti tak, jak ji chápe zákon o kybernetické bezpečnosti[143] a evropský dokument Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor.[144] Při zajištění kybernetické bezpečnosti jde tedy zejména o snahu minimalizovat útoky proti důvěrnosti, integritě a dostupnosti počítačových systémů. Proto například záměrně nevěnuji pozornost jistě významné, ale s kybernetickou bezpečností nesouvisející, Obchodní dohodě proti padělání, široce medializované pod zkratkou ACTA.

4.1 Úmluva o počítačové kriminalitě[145]

Prvním a nejvýznamnějším dokumentem na mezinárodním poli, který se komplexně zabývá počítačovou kriminalitou, je Úmluva Rady Evropy o počítačové kriminalitě (dále jen „**Úmluva**“). Cílem Úmluvy, jak vyplývá z její preambule, je harmonizace trestní politiky zaměřené na ochranu společnosti před počítačovou kriminalitou, a to při zachování rovnováhy mezi zájmy vynucováním práva a ohledem na základní lidská práva, mimo jiné též práva na ochranu osobních údajů. Úmluva respektuje stávající mezinárodní dokumenty jak v oblasti lidsko-právní, tak úmluvy o spolupráci v trestní oblasti, přičemž Úmluva si klade za cíl tyto dokumenty doplňovat a zajistit tak efektivnější trestní vyšetřování a trestní řízení.

---

[143] § 2 písm. b) návrhu zákona: *„Kybernetická bezpečnost je souhrn právních, organizačních, technických a vzdělávacích prostředků k zajištění ochrany kybernetického prostoru.“* V důvodové zprávě k návrhu zákona je předmět právní úpravy negativně vymezen principem technologické neutrality: *„Navrhovaná právní úprava důsledně odděluje bezpečnost fungování služeb informační společnosti od informačního obsahu a předmětem regulace tak zde není obsah přenášených informací. Předmětem navrhované právní úpravy tedy nejsou například projevy obsahové informační či počítačové kriminality, jako např. šíření dětské pornografie, stalking nebo porušování práv duševního vlastnictví.“ Důvodová zpráva k návrhu zákona o kybernetické bezpečnosti*. Národní bezpečnostní úřad, 2013. Dostupné také z www: http://www.nbu.cz/cs/aktuality/1398-navrh-zakona-o-kyberneticke-bezpecnosti-byl-predlozen-vlade-ceske-republiky/ [citováno dne 9. října 2013]

[144] *„Kybernetická bezpečnost má zachovat dostupnost a integritu sítí a infrastruktury, jakož i důvěrnost informací, jež jsou v nich obsaženy."* Viz reference č. 38 na str. 20.

[145] Úmluva Rady Evropy č. 185 ze dne 23. 11. 2001 o počítačové kriminalitě. Dostupná také z www: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, český překlad srov. Sněmovní tisk č. 890, 6. volební období. Ač překlad uvedený ve sněmovním tisku vykazuje určité nedostatky (viz kapitoly 1.4 a 1.5 této práce), pro jeho oficialitu budu nadále používat termíny jemu odpovídající.

4.1.1 Vznik Úmluvy a její ratifikace ve světě a v České republice

Na přípravě Úmluvy se kromě některých států Rady Evropy podílely i USA či Japonsko. Úmluvy byla otevřena k podpisu dne 23. 11. 2001 v Budapešti, proto je někdy nazývána i jako Budapešťská úmluva. Ode dne otevření podpisu ji podepsalo celkem 49 států. K signatářským státům patří všechny členské státy Rady Evropy s výjimkou Ruska a San Marina, a dále čtyři nečlenské státy, které se na přípravě Úmluvy podílely - USA, Japonsko, Jihoafrická republika a Kanada. Pro nabytí účinnosti Úmluvy bylo třeba, aby byly u generálního tajemníka Rady Evropy uloženy ratifikační listiny (resp. listiny o přijetí nebo schválení) od pěti států včetně alespoň tří členských států Rady Evropy. Tato podmínka byla splněna v průběhu roku 2004 a tak Úmluva vstoupila v platnost dne 1. 7. 2004. Do září roku 2013 ratifikačním procesem Úmluva prošla ve 40 státech. Česká republika Úmluvu podepsala již v roce 2005, ale k ratifikaci došlo z důvodu letitého nesouladu české legislativy s některými požadavky plynoucími z Úmluvy až 22. 8. 2013. Česká republika již tak nepatří k signatářským zemím, které stále ještě dokument neratifikovaly.[146]

Teprve po nabytí účinnosti nového trestního zákoníku a po několikeré novelizaci trestního řádu byly odstraněny rozpory s Úmluvou a proto byl vládou dne 3. 1. 2013 předložen Parlamentu České republiky návrh k vyslovení souhlasu s ratifikací Úmluvy.[147] Vláda v tomto dokumentu navrhuje, aby při uložení ratifikačních listin byla k některým ustanovením Úmluvy učiněna tzv. výhrada či prohlášení. Tyto budou rozebrány níže. Zahraniční výbor Poslanecké sněmovny Úmluvu projednal a ve svém usnesení ze dne 28. 2. 2013 doporučil dát souhlas s ratifikací. Totéž učinil i Senát České republiky. Druhé čtení proběhlo 9. května 2013, souhlas s mezinárodní smlouvou byl doručen prezidentu republiky dne 28. 5. 2013. Úmluva o počítačové kriminalitě byla vcelku nekonfliktně ratifikována a ode dne 1. 12. 2013 bude účinná.[148]

Úmluvu rozšiřuje Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových

---

[146] K těmto státům patří Monako, Řecko, Irsko, Lichtenštejnsko, Lucembursko, Polsko, Švédsko, Turecko, Kanada, Jihoafrická republika a Andorra. Naopak Austrálie a Dominikánská republika nejsou signatářskými státy, ale přesto Úmluvu ratifikovaly. Úmluva takový postup umožňuje v čl. 37. Tyto údaje jsou platné k datu psaní této kapitoly, tj. září 2013. Aktuální informace dostupné z http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

[147] Vládní návrh č. 890/0 ze dne 19. 12. 2012, sněmovní tisk č. 890, 6. volební období.

[148] Tyto údaje jsou platné k datu psaní této kapitoly, tj. září 2013. Aktuální informace dostupné z http://www.psp.cz/sqw/text/tiskt.sqw?o=6&ct=890&ct1=0 [citováno dne 9. října 2013]

systémů (dále jen „**Dodatkový protokol**“). Dodatkový protokol vymezuje skutkové podstaty týkající se rasismu a xenofobie, jejichž vymáhání může být národní legislativou některých států bráno jako přílišné zásahy do svobody projevu. Aby se dosáhlo co nejvyššího počtu ratifikací Úmluvy, nebyly tyto kontroverzní skutkové podstaty z tohoto důvodu zahrnuty v Úmluvě, ale samostatně v Dodatkovém protokolu.[149] Tyto úvahy mohou být dnes, s odstupem času, považovány za oprávněné, což potvrzuje mimo jiné i fakt, že Dodatkový protokol podepsalo i ratifikovalo podstatně méně států než Úmluvu. Protože Dodatkový protokol neobsahuje žádná ustanovení týkající se bezpečnosti počítačových systémů, a dále též s ohledem na jeho nepodepsání Českou republikou, nebudu se jím blíže v této práci zabývat.

4.1.2 Struktura Úmluvy, její nejvýznamnější ustanovení a základní principy

Úmluva sestává z preambule a 48 článků rozdělených do čtyř kapitol. V první kapitole (čl. 1) jsou vymezeny základní pojmy a definice, s nimiž Úmluva dále operuje, tj. počítačový systém, počítačová data, poskytovatel služby a provozní data. Tímto Úmluva sehrává zásadní roli v mezinárodním právu, neboť sjednocuje právní pojmy. Ostatně i v úvodní kapitole této práce jsem pro výklad pojmů použil příslušná ustanovení Úmluvy.

Druhá kapitola má název Opatření, která mají být přijata na vnitrostátní úrovni. V první části, zaměřená na trestní právo hmotné, se smluvní státy zavazují přijmout takovou legislativu na národní úrovni, která bude nezbytná k tomu, aby dle vnitrostátního práva daného státu byly trestnými činy skutkové podstaty uvedené v článcích 2 až 11. Články 11 až 12 upravují některé ze základů trestní odpovědnosti, konkrétně pokus trestného činu a účastenství (což je v Úmluvě bráno jako samostatná skutková podstata), a dále pojem pro české právo relativně nový, a to trestní odpovědnost právnických osob. Článek 13 se stanovuje požadavky na tresty uložené za trestné činy uvedené v předchozích článcích. Tresty mají být účinné, přiměřené a dostatečně odrazující, včetně trestu odnětí svobody a peněžitých sankcí.

Druhá část druhé kapitoly (čl. 14 - 21) je věnována procesně-právním opatřením, jejichž úkolem je zlepšit možnosti osob činných v trestním řízení vedoucí k odhalení a usvědčení pachatele. Smluvní strany se zavázaly přijmout tato opatření nejen v řízeních o trestných činech explicitně stanovených Úmluvou, tj. o trestných činech dle článků 2 až 11,

[149] GŘIVNA, T. K ustanovením Úmluvy o počítačové kriminalitě. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

ale též i v dalších trestních řízeních za předpokladu, že trestný čin (libovolný) byl spáchán prostřednictvím počítačového systému nebo jsou v řízení zajišťovány důkazy o trestném činu, které jsou v elektronické formě. Ke konkrétním opatřením patří urychlené uchování uložených dat, příkaz k předložení, prohlídka a zajištění uložených počítačových dat a shromažďování počítačových dat v reálném čase. Třetí část druhé kapitoly (čl. 22) ukládá smluvním státům povinnost stanovit svou soudní pravomoc ve vztahu k trestným činům stanoveným Úmluvou.[150]

Kapitola třetí se zaobírá ustanoveními o mezinárodní spolupráci, a to nejprve obecnými zásadami (čl. 23 – 28) a následně konkrétními ustanoveními (čl. 29 – 35). Na poli mezinárodní spolupráce již existuje několik dokumentů týkajících se právní pomoci ve věcech trestních,[151] které Úmluva ale neníní nahrazovat a vytvářet tak nový režim odlišný od stávajícího. Tím by mohly snadno vzniknout pochybnosti, kdy aplikovat jaká ustanovení. Namísto nahrazení stávajících nástrojů jsou ustanovení kapitoly třetí pojata jako doplňující ke zmíněným dokumentům. Konkrétní ustanovení v sobě zahrnují povinnost smluvních států vyhovět v případech stanovených Úmluvou žádosti jiného smluvního státu, pokud by tento hodlal využít některého z procesně-právních opatření dle článků 16 až 21 vůči počítačovému systému nebo poskytovateli služeb na území prvého smluvního státu; dále poskytovat vzájemnou pomoc týkající se shromažďování či odposlechu počítačových dat; a zřídit tzv. síť 24/7, tj. kontaktní místo schopné obratem poskytnout jinému smluvnímu státu v jakoukoliv denní dobu informace specifikované Úmluvou.

Čtvrtá kapitola (čl. 36 – 48) obsahuje závěrečná ustanovení upravující například podmínky pro vstup Úmluvy v platnost, možnost přistoupení třetích států, možnost vypovědět Úmluvu a podobně. Klíčové jsou zejména články 40 a 42, v nichž je zakotvena možnost smluvního státu při podpisu Úmluvy nebo při uložení ratifikační listiny (resp. listiny o přijetí, schválení nebo přístupu) prohlásit, že strana využívá tzv. dodatečných prvků[152] nebo výhrad.

---

[150] Problematika soudní pravomoci, působnosti distančních deliktů spáchaných v kyberprostoru byla již zmíněna v kapitole 2.1.3.

[151] Zejména Evropská úmluva o vydávání (Paříž, 13. 12. 1957, sdělení FMZV č. 549/1992 Sb.), Evropská úmluva o vzájemné pomoci ve věcech trestních (Štrasburk, 20. 4. 1959, sdělení FMZV č. 550/1992 Sb.) a Dodatkový protokol k Evropské úmluvě o vzájemné pomoci ve věcech trestních (Štrasburk, 17. 3. 1978, sdělení FMZV č. 31/1997 Sb.).

[152] V anglickém znění Úmluva používá termínu „*additional elements*". V literatuře je používán též pojem „dodatečné náležitosti", ve znění Úmluvy dle vládního návrhu č. 890/0 ze dne 19. 12. 2012 je však uveden pojem „dodatečné prvky". Jak již bylo uvedeno, pro účely této práce budu nadále používat pojmy dle vládního návrhu.

Dodatečné prvky dle čl. 40 mohou zúžit trestnost jen na nejzávažnější případy tím, že pro naplnění skutkové podstaty trestného činu, u kterého Úmluva dovoluje stanovit dodatečný prvek, bude vyžadováno splnění další kvalifikační okolnosti. Touto okolností může být například specifický úmysl či spáchání trestného činu ve vztahu k počítačovému systému, který je spojen s jiným počítačovým systémem. Výhrady mají - stejně jako dodatečné prvky - za cíl umožnit smluvním stranám vybrat si z pohledu jejich národního práva příznivější variantu ustanovení dle Úmluvy, avšak v čl. 43 je předpokládáno, že strana výhradu odvolá, jakmile to okolnosti dovolí. Aby se dosáhlo co nejvyšší harmonizace národních legislativ, lze dodatečné prvky i výhradu učinit jen a pouze u ustanovení, u kterých to Úmluva výslovně dovoluje.

4.1.3 Specifická úprava trestní odpovědnosti a sankcí dle Úmluvy

Smluvní strany se v Úmluvě zavázaly přijmout taková legislativní a jiná opatření, která budou nezbytná k tomu, aby dle vnitrostátních předpisů byla jednání popsaná v článcích 2 až 11 posuzována jako trestné činy. Kriminalizováno je vždy pouze úmyslné jednání, přičemž pro vznik trestní odpovědnosti u některých popsaných jednání musí úmysl zahrnovat i dosažení konkrétního cíle sledovaného tímto jednáním, tj. pachatel musí jednat ve specifickém úmyslu. Například u trestného činu počítačového podvodu dle čl. 8 Úmluvy je jako specifický úmysl vyžadován *„podvodný nebo nečestný úmysl získat majetkový prospěch pro sebe nebo pro jiného.“* Při absenci tohoto specifického úmyslu trestní odpovědnost za trestný čin počítačového podvodu vůbec nevznikne.

Každý trestný čin popsaný Úmluvou explicitně vyžaduje pro jeho kriminalizaci protiprávnost jednání, kterou obvykle vyjadřuje slovy „protiprávně“ či „neoprávněně“. Úmluva tím vylučuje aplikaci norem trestního práva jak na případy okolností vylučujících protiprávnost činu,[153] tak na oprávněné a obvyklé aktivity. Proto nemůže být trestně odpovědný např. administrátor počítačové sítě testující její zabezpečení, ačkoliv by svým jednáním mohl naplnit skutkovou podstatu popsanou v čl. 2 Úmluvy. V českém právním řádu je však protiprávnost znakem trestného činu vždy. Tento závěr lze učinit z dikce § 13 TZ, dle kterého je trestným činem protiprávní čin, který zákon označuje za trestný a který vykazuje znaky uvedené v zákoně. Není tedy pro nutné dosažení souladu českého právního řádu s Úmluvou u každé skutkové podstaty v trestním zákoníku zmiňovat i protiprávnost, ačkoliv u některých skutkových podstat trestných činů je znak protiprávnosti zdůrazněn.

[153] V českém trestním právu zakotveny v § 28 - 32 TZ.

Článek 11 Úmluvy ukládá státům přijmout opatření ke kriminalizaci účastenství (odst. 1) a pokusu (odst. 2). Dle prvního odstavce má být trestným činem jakákoliv úmyslná forma účastenství na spáchání každého trestného činu popsaného Úmluvou, pokud k účastenství došlo s úmyslem daný trestný čin spáchat. Z textu Úmluvy není zcela jasné, zda je pomoc trestná i v případě nedokonání trestného činu hlavním pachatelem. Dle důvodové zprávy ale trestní odpovědnost vznikne jen tam, kde hlavní pachatel trestný čin spáchal.[154] Tomu zcela odpovídá ustanovení § 24 odst. 2 TZ, podle něhož nevznikne trestní odpovědnost účastníka bez vzniku trestní odpovědnosti pachatele, tj. je nutné trestný čin dokonat anebo se o to alespoň pokusit. Jedná se o tzv. zásadu akcesority účastenství.[155]

Důvodová zpráva k Úmluvě v souvislosti s problematikou kriminalizace účastenství výslovně uvádí případ přenášení škodlivého obsahu nebo kódu, s nímž je spojena trestněprávní odpovědnost. Účastníkem v podobě pomocníka je zde poskytovatel telekomunikačních služeb, bez kterého by škodlivý obsah nebo kód nemohl být přenášen. Pokud ale poskytovatel telekomunikačních služeb nejednal v úmyslu spáchat trestný čin, nemůže za něj být jako účastník trestně odpovědný, pokud o trestním jednání pachatele nevěděl. Úmluva tedy nezavazuje poskytovatele telekomunikačních služeb aktivně sledovat obsah pro zbavení se trestní odpovědnosti.[156] Odpovědnost poskytovatele telekomunikačních služeb v tomto případě navíc v rámci evropského prostoru stanoví jiná norma.[157]

Co se týče vývojových stádií trestné činnosti, Úmluva vyžaduje trestnost úmyslného a neoprávněného pokusu spáchat trestný čin popsaný Úmluvou. U některých trestných činů ale byla realizace pokusu považována za nemožnou či obtížnou, proto čl. 11 odst. 2 taxativně vyjmenovává, v jakých případech je pokus trestný. K ustanovení o pokusu byla smluvním

---

[154] *The Explanatory Report of the Convention on Cybercrime.* Budapešť, Výbor ministrů Rady Evropy, 2001. Čl. 49. Dostupné z: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm. K tomu srov. GŘIVNA, T., POLČÁK, R. (eds.). K ustanovením Úmluvy o počítačové kriminalitě. In: *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

[155] GŘIVNA, T., POLČÁK, R. (eds.). K ustanovením Úmluvy o počítačové kriminalitě. In: *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

[156] *The Explanatory Report of the Convention on Cybercrime.* Budapešť, Výbor ministrů Rady Evropy, 2001. Čl. 49. Dostupné z: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

[157] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu"). Viz kapitola 4.2.

státům ponechána možnost vznést výhradu. Česká republika výhradu vznést nepotřebuje, neboť požadavky ohledně trestnosti pokusu odpovídají § 21 TZ.[158]

4.1.4 Požadavky Úmluvy na odpovědnost právnických osob a česká právní úprava

Článek 12 Úmluvy vyžaduje, aby za trestné činy stanovené Úmluvou byly odpovědné i právnické osoby. Ačkoliv Úmluva nutně nevyžaduje odpovědnost trestní, ale za jistých okolností i občanskoprávní či správní, Česká republika požadavkům Úmluvy naplno vyhověla až dne 1. 1. 2012, kdy nabyl účinnosti zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim (dále jen „**Zákon o trestní odpovědnosti právnických osob**"). Pro odpovědnost právnické osoby musí být trestný čin stanovený Úmluvou spáchán ve prospěch právnické osoby a musí jej spáchat fyzická osoba zastávající vedoucí funkci. Tato osoba musí na základě pravomoci buď jednat navenek jménem právnické osoby, nebo přijímat rozhodnutí jménem právnické osoby, nebo vykonávat kontrolu v rámci právnické osoby. Též je právnická osoba odpovědná v případě, že spáchání trestného činu stanoveného Úmluvou umožnil nedostatek dohledu nebo kontroly fyzické osoby zastávající vedoucí funkci, pokud právnické osobě z tohoto jednání vznikl prospěch a fyzická osoba jednala v rámci své pravomoci. Odpovědnost právnických osob nevylučuje trestní odpovědnost skutečných pachatelů, tj. fyzických osob.

Zákon o trestní odpovědnosti právnických osob v § 7 taxativně vyjmenovává trestné činy, u kterých může trestní odpovědnost právnické osoby vzniknout. Všechny trestné činy stanovené Úmluvou jsou v tomto výčtu zahrnuty. Trestní odpovědnosti podléhají všechny právnické osoby s výjimkou České republiky a územně samosprávných celků při výkonu veřejné moci (odpovědnost těchto entit je vyloučena v § 6 odst. 1). Trestně odpovědný je i právní nástupce právnické osoby (§ 10), čímž se zabraňuje tomu, aby se právnická osoba vyhnula trestní odpovědnosti svou přeměnou. Podmínky trestní odpovědnosti jsou definovány v § 8. Právnická osoba je trestně odpovědná, jestliže je trestný čin spáchán jménem právnické osoby, v jejím zájmu nebo v rámci její činnosti, jedná-li tak osoba určitého postavení (viz dále), a jestliže lze právnické osobě toto jednání přičítat podle § 8 odst. 2. Výše uvedený pojem „osoba určitého postavení", použitý jen pro účely zjednodušení tohoto textu, je v § 8 odst. 1 písm. a) až d) vyjádřen jako *„a) statutární orgán nebo člen statutárního orgánu, anebo jiná osoba, která je oprávněna jménem nebo za právnickou osobu jednat, b) ten, kdo*

[158] § 21 TZ: *„Jednání, které bezprostředně směřuje k dokonání trestného činu a jehož se pachatel dopustil v úmyslu trestný čin spáchat, je pokusem trestného činu, jestliže k dokonání trestného činu nedošlo."*

u této právnické osoby vykonává řídící nebo kontrolní činnost, i když není osobou uvedenou v písmenu a), c) ten, kdo vykonává rozhodující vliv na řízení této právnické osoby, jestliže jeho jednání bylo alespoň jednou z podmínek vzniku následku zakládajícího trestní odpovědnost právnické osoby, nebo d) zaměstnanec nebo osoba v obdobném postavení (dále jen "zaměstnanec") při plnění pracovních úkolů, i když není osobou uvedenou v písmenech a) až c).“ Přičitatelné je spáchání trestného činu právnické osobě tehdy, jestliže byl spáchán buď „*jednáním orgánů právnické osoby nebo osob uvedených v odstavci 1 písm. a) až c)“,* nebo *„zaměstnancem uvedeným v odstavci 1 písm. d) na podkladě rozhodnutí, schválení nebo pokynu orgánů právnické osoby nebo osob uvedených v odstavci 1 písm. a) až c) anebo proto, že orgány právnické osoby nebo osoby uvedené v odstavci 1 písm. a) až c) neprovedly taková opatření, která měly provést podle jiného právního předpisu nebo která po nich lze spravedlivě požadovat, zejména neprovedly povinnou nebo potřebnou kontrolu nad činností zaměstnanců nebo jiných osob, jimž jsou nadřízeny, anebo neučinily nezbytná opatření k zamezení nebo odvrácení následků spáchaného trestného činu."*

Lze uzavřít, že všechny podmínky předpokládané Úmluvou ohledně odpovědnosti právnických osob jsou Zákonem o trestní odpovědnosti právnických osob splněny.

4.1.5 Dodatečné prvky, výhrady

Úmluva se pokouší harmonizovat boj s počítačovou kriminalitou tím, že vytváří katalog nových trestných činů pro tuto oblast. Smluvní strany se zavazují všechny tyto trestné činy recipovat do svého národního práva. Přesto ale - jak bylo naznačeno v předchozí kapitole - Úmluva nemá ambici dosáhnout zcela jednotné právní úpravy a respektuje legislativní i jiné odlišnosti smluvních států, neboť umožňuje stranám využít dodatečných prvků dle čl. 40 a výhrad dle čl. 42. Vzniklé rozdíly mezi národními úpravami mohou představovat určitou překážku harmonizace, proto je možné učinit výhrady i využít dodatečných prvků jen tam, kde to Úmluva výslovně dovoluje. Na smluvní stranu může být i vyvíjen diplomatický tlak dle čl. 43 odst. 3, který opravňuje generálního tajemníka Rady Evropy k pravidelnému dotazování se stran, které učinily jednu či více výhrad, zdali je již možné výhradu odvolat. Výhrady jsou totiž považovány jen za dočasná opatření a předpokládá se, že smluvní státy výhradu zcela nebo zčásti odvolají, jakmile to okolnosti dovolí (čl. 43 odst. 2). Odvolání výhrady ale není nijak vynutitelné, Úmluva nestanoví žádnou lhůtu ani sankci.

Česká republika při ratifikací Úmluvy učinila výhradu u článku 29 odst. 4, čímž si vyhradila právo odmítnout žádost jiného smluvního státu o urychlené uchování uložených počítačových dat dle čl. 29 Úmluvy v případech, kdy lze předpokládat, že by nebylo možno

naplnit podmínku vzájemné trestnosti. Česká republika tímto může u trestných činů jiných než popsaných v článcích 2 až 11 Úmluvy požadovat, aby šlo o čin trestný i podle jejího práva. U trestných činů popsaných Úmluvou nelze žádost odmítnout, a to ani v případě, že by některá z jednání dle článků 2 až 11 byla v budoucnu z jakéhokoliv důvodu českým právem dekriminalizována. Česká republika dále učinila prohlášení o dodatečných prvcích, dle kterého bude jednání popsané v článku 2 Úmluvy (tj. nezákonný přístup) kriminalizováno jen tehdy, dojde-li k překonání bezpečnostního opatření za účelem získat neoprávněný přístup k počítačovému systému nebo jeho části. Tím bude dosaženo souladu s čl. 2 Úmluvy bez nutnosti zásahu do českého právního řádu.[159]

4.1.6 Katalog trestných činů zavedený Úmluvou

Trestné činy dle Úmluvy jsou rozděleny do čtyř oblastí, přičemž kategorizace odpovídá mému rozčlenění uvedenému v první kapitole. Jedná se o tyto oblasti trestných činů:

1. Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
    a. Nezákonný přístup (čl. 2)
    b. Nezákonný odposlech (čl. 3)
    c. Zasahování do dat (čl. 4)
    d. Zasahování do systému (čl. 5)
    e. Zneužívání zařízení (čl. 6)
2. Trestné činy související s počítačem
    a. Počítačové padělání (čl. 7)
    b. Počítačový podvod (čl. 8)
3. Trestné činy související s obsahem
    a. Trestné činy související s dětskou pornografií (čl. 9)
4. Trestné činy týkající se porušení autorského práva a práva souvisejícího s právem autorským (čl. 10)

Tato práce se zaměřuje zejména na trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů. Tyto Úmluvou vyžadované trestné činy přiblížím v kapitole 5.

[159] § 230 TZ. Viz reference č. 173 na str. 71.

4.2 Evropské trestněprávní předpisy vztahující se ke kybernetické bezpečnosti

Jedním z dlouhodobých cílů Evropské unie je vytvoření a udržení evropského vnitřního trhu, jehož složkou je i jednotný digitální trh. Množství předpisů na evropské úrovni proto stanovuje regulační rámec pro trh elektronických telekomunikací. Kromě toho je snahou Evropské unie posilovat důvěru veřejnosti v kyberprostor při realizaci hospodářských vztahů. Výsledkem této snahy je ***směrnice o elektronickém obchodu***,[160] která vedle ustanovení o nevyžádaných obchodních sděleních či o uzavírání smluv elektronickou cestou zejména vytváří pravidla pro odpovědnost poskytovatelů služeb informační společnosti[161] a stanovuje některé jejich povinnosti. Směrnice výslovně neukládá žádnou obecnou povinnost plošného sledování příjemců služby. Z pohledu trestního práva je ale důležité, že členské státy mohou v některých případech uložit ISP povinnost informovat osoby činné v trestním řízení, zejména poskytnout informace vedoucí ke zjištění totožnosti příjemců jejich služeb. Tato povinnost, zakládající spolupráci mezi osobami činnými v trestním řízení a soukromými subjekty, je zásadní pro účinné vymáhání práva v kyberprostoru.

Povinnost ISP uchovávat některá data pro účely trestního stíhání stanovuje ***směrnice o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí***.[162] Tento předpis sice stanovuje povinnost uchovávat jen provozní a lokalizační údaje, které jsou nezbytné k lokalizaci uživatele kyberprostoru, a nevztahuje se na obsah přenášených elektronických sdělení, přesto se soulad některých ustanovení právních předpisů vzniklých na základě této směrnice stal předmětem řízení ústavních soudů několika členských států. Ústavní soudy, včetně českého, shodně konstatovaly, že plošné zaznamenávání těchto údajů je nepřiměřený zásah do principů právního státu. Jako problematické se jeví i náklady spojené s požadovaným ukládáním údajů.[163] V českém právním řádu byly nakonec požadavky

---

[160] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“).

[161] V této práci byla odpovědnost ISP zevrubně představena v kapitole 2.1.2.

[162] Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES.

[163] Viz nález Ústavního soudu České republiky ze dne 22. 3. 2011, Pl. ÚS 24/10. Blíže k vývoji ve Spolkové republice Německo srov. (v německém jazyce) HOEREN, T. *Internetrecht.* Universität Münster, Münster, 2012.

na uchovávání provozních a lokalizačních údajů v omezené míře stanoveny zákonem č. 273/2012 Sb.,[164] kterým byl novelizován jak zákon o elektronických komunikacích, tak trestní řád.

Významnou překážkou pro vytvoření jednotného digitálního trhu je kybernetická kriminalita. Základním legislativním instrumentem Evropské unie pro boj s kybernetickou kriminalitou je ***rámcové rozhodnutí Rady o útocích proti informačním systémům***.[165] Rozhodnutí obsahuje ustanovení velmi podobná Úmluvě - stanovuje trestné činy a upravuje některé hmotněprávní i procesní instituty s těmito trestnými činy souvisejícími, stejně jako některé aspekty mezinárodní spolupráce. Zabývá se výhradně oblastí trestných činů proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů. Dalšími oblastmi kybernetické kriminality se Evropská unie zabývá v předpisech zaměřených na potírání dětské pornografie na Internetu nebo na potírání počítačových podvodů.

K dosažení jednotného digitálního trhu je nutnou podmínkou zajištění bezpečnost kyberprostoru. Evropská unie vytváří na různých úrovních dokumenty vytyčující dlouhodobé strategie v této oblasti. V únoru roku 2013 zformovala Vysoká představitelka Evropské unie pro zahraniční věci a bezpečnostní politiku vize svého úřadu v dokumentu ***Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor***.[166] Tento dokument uznává výhradní postavení soukromého sektoru v kyberprostoru, ale zároveň konstatuje povinnost vlád zabezpečovat jeho otevřenost, respektovat a chránit v něm základní práva a zabezpečovat spolehlivost jeho provozu. Právě kybernetická kriminalita páchaná proti kritické infrastruktuře může tyto hodnoty ohrožovat.

V souvislosti s výše uvedenými dokumenty mají velkého významu i dva legislativní návrhy Evropské komise. ***Směrnice o útocích proti informačním systémům***[167] má nahradit

---

Str. 504. [online]. [citováno dne 9. října 2013]. Dostupné také z www: http://www.uni-muenster.de/Jura.itm/hoeren/lehre/materialien

[164] Zákon ze dne 18. července 2012, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony.

[165] Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005, o útocích proti informačním systémům.

[166] JOIN/2013/0001. Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů. Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor. Brusel, Vysoká představitelka Evropské unie pro zahraniční věci a bezpečnostní politiku, 2013. Dostupné také z www: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:CS:PDF [citováno dne 9. října 2013]

[167] Návrh směrnice Evropského parlamentu a Rady COM/2010/517 ze dne 30. 9. 2010 o útocích proti informačním systémům a zrušení rámcového rozhodnutí Rady 2005/222/SVV. První čtení v Evropském

rámcové rozhodnutí Rady o útocích proti informačním systémům, oproti kterému zejména rozšiřuje katalog trestných činů. Směrnice zůstává zaměřena toliko na útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů. ***Směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii***[168] si klade za cíl mimo jiné standardizovat bezpečnostní požadavky na povinné subjekty. Návrh směrnice ukládá členským státům povinnost zřídit odpovědný orgán, který bude dohlížet nad vykonáváním povinností uložených touto směrnicí povinným subjektům. Tyto orgány mají dle čl. 8 návrhu spolupracovat mezi sebou, s Evropskou komisí a též s Evropskou agenturou pro bezpečnost sítí a informací (ENISA).[169] Spoluprácí má vzniknout síť, jejíž orgány budou šířit včasná varování ohledně rizik a incidentů, zajišťovat koordinovanou spolupráci, vyměňovat si mezi sebou informace a osvědčené postupy, pořádat cvičení bezpečnosti sítí a též spolupracovat s Evropským centrem pro boj proti kybernetické kriminalitě (EC3).[170] Odpovědné orgány mohou dle čl. 15 návrhu vyžadovat po povinných orgánech informace potřebné k posouzení bezpečnosti jejich sítí a informačních systémů, nařídit jim bezpečnostní audit a zejména jim udělovat závazné pokyny, přičemž pojem „závazný pokyn" není směrnicí nadále nijak upraven.

K povinným subjektům návrh této směrnice řadí hospodářské subjekty a orgány veřejné správy. Hospodářským subjektem je dle čl. 3 čís. 8 této směrnice vedle provozovatelů kritické infrastruktury (dle Přílohy II k této směrnici např. dodavatelé elektřiny a plynu, letiště a přístavy, burzy cenných papírů, zdravotnická zařízení) i *„poskytovatel služeb informační společnosti, na nichž závisí poskytování dalších služeb informační společnosti",* k nimž dle Přílohy II patří mimo jiné sociální sítě, vyhledávače či elektronické obchody. Osobně nepovažuji takto široké vymezení povinných subjektů za vhodné, zejména pokud směrnice vybízí k poměrně rozsáhlé delegaci pravomocí (viz výše naznačená možnost odpovědného

---

parlamentu proběhlo 3. července 2013. Návrh směrnice byl schválen až po dopsání této kapitoly a byl publikován jako 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.

[168] Návrh směrnice Evropského parlamentu a Rady COM/2013/0027 ze dne 7. 2. 2013 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii. Dostupné z www: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:CS:PDF [citováno dne 9. října 2013]

[169] *European Network and Information Security Agency* - Evropská agentura pro bezpečnost sítí a informací. Blíže viz www: http://www.enisa.europa.eu/ [citováno dne 9. října 2013]

[170] *European Cyber Crime Center* - Evropské centrum pro boj proti kybernetické kriminalitě, které bylo zřízeno v rámci Europolu. Blíže viz www: http://www.europol.europa.eu/ec3 [citováno dne 9. října 2013]. EC3 bude porovnáno s českým Národním centrem kybernetické bezpečnosti v 6. kapitole této práce.

orgánu udílet závazné pokyny). Protože je ale návrh ve velmi rané fázi, je pravděpodobné, že ještě projde četnými změnami.

5. TRESTNĚPRÁVNÍ POSTIH INTERNETOVÉ A POČÍTAČOVÉ KRIMINALITY

5.1 Hmotněprávní postih kybernetických útoků

Kybernetické útoky proti počítačovým systémům, tj. útoky proti jejich důvěrnosti, integritě a dostupnosti, nelze subsumovat pod „tradiční“ skutkové podstaty. Již trestní zákon účinný do 31. 12. 2008 znal skutkovou podstatu neoprávněného zásahu do nosiče informací. Nový trestní zákoník přinesl skutkové podstaty nové - neoprávněný přístup k počítačovému systému a nosiči informací (§ 230), opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231) a poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232). Nové skutkové podstaty odpovídají požadavkům vyplývajícím z Úmluvy a lépe postihují nežádoucí jednání v kyberprostoru. Zároveň však nedochází k hypertrofii trestní represe - dle nových skutkových podstat nejsou postihovány bagatelní delikty. Ostatní formy páchání trestné činnosti popsané ve třetí kapitole této práce, tj. trestná činnost související s obsahem a trestná činnost, v níž je počítačový systém jen nástrojem usnadňujícím jeho spáchání, jsou postižitelné dle „tradičních“ skutkových podstat, případně může dojít k souběhu s trestnými činy dle nových skutkových podstat.

Objektem nových skutkových podstat je zájem na ochraně počítačových systémů před neoprávněnými přístupy a zásahy (tj. zájem na ochraně jejich důvěrnosti, integrity a dostupnosti), včetně počítačových dat v nich uložených.[171] Je tak chráněn počítačový systém jednak jako hmotný substrát, jednak jako nosič počítačových dat v něm inkorporovaných. Zaručením bezpečnosti počítačových systémů jsou taktéž chráněny další zájmy - soukromí jednotlivců, osobní údaje v počítačových systémech, autorská díla, obchodní tajemství a utajované informace a podobně.[172] K počítačovým systémům chráněných trestním zákonem patří i tzv. kritická infrastruktura, jejíž narušení může mít za následek plošné problémy s dodávkou základních služeb, například vody nebo elektřiny. Lze tak dovodit, že nepřímo je objektem těchto skutkových podstat též zájem společnosti na nerušených dodávkách základních služeb.

---

[171] NOVOTNÝ, O., VOKOUN, R., ŠÁMAL, P. a kol. *Trestní právo hmotné. Zvláštní část*. 6. vydání, Praha, Wolters Kluwer ČR, a. s., 2010, str. 209.

[172] Tamtéž.

Počítačový systém je zde vždy předmětem útoku, ale nadto bývá často též nástrojem v rukou pachatele trestné činnosti.

Pachatelem může být kdokoliv, pouze § 232 TZ vyžaduje speciální subjekt, neboť objektivní stránka předpokládá porušení povinnosti vyplývající ze zvláštního postavení pachatele. Všech trestných činů uvedených v § 230 - 232 TZ se může dle § 7 zákona o trestní odpovědnosti právnických osob dopustit i právnická osoba.

U všech skutkových podstat je vyžadováno úmyslné zavinění, pouze trestný čin dle § 232 je možné spáchat z nedbalosti. U některých kvalifikovaných skutkových podstat postačuje i nedbalostní forma.

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

§ 230 TZ v sobě zahrnuje pět skutkových podstat uvedených v Úmluvě: nezákonný přístup (čl. 2 Úmluvy, § 230 odst. 1 TZ), zasahování do dat [čl. 4 Úmluvy, § 230 odst. 2 písm. a), b) a d) TZ], zasahování do systému [č. 5 Úmluvy, § 230 odst. 3 písm. b) TZ], počítačové padělání [čl. 7 Úmluvy, § 230 odst. 2 písm. c) TZ] a počítačový podvod [čl. 8 Úmluvy, § 230 odst. 3 písm. a) TZ].

Základní skutková podstata uvedená v prvním odstavci (***neoprávněný přístup*** čili ***hacking***, česky je též někdy používáno pojmu průnikaření)[173] vyžaduje nejen neoprávněně získat přístup k počítačovému systému nebo jeho části, ale též pro tento účel překonat bezpečnostní opatření. Úroveň zabezpečení není nijak stanovena, pro naplnění skutkové podstaty postačuje i triviální zabezpečení.[174] Není tedy trestním právem postižitelné jednání, kdy někdo získá neoprávněný přístup ke zcela nezabezpečenému počítačovému systému, pokud zároveň nenaplní skutkovou podstatu uvedenou v druhém odstavci. Též není postižitelné jednání osoby, která sice překonala bezpečnostní opatření, ale k počítačovému systému má oprávněný přístup - tímto nevzniká trestní odpovědnost například osobě, která se pomocí počítačové sítě připojí ke svému počítači nebo hackerům typu white hats.[175]

Článek 2 Úmluvy, z něhož § 230 odst. 1 TZ vychází, umožňuje smluvním státům stanovit pro kriminalizaci trestného činu neoprávněného přístupu jako dodatečný prvek

---

[173] § 230 odst. 1 TZ: *„Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“*

[174] ŠÁMAL, P. a kol. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání, Praha, C. H. Beck, 2012. Str. 2305.

[175] Viz kapitola 3.1.1 této práce.

porušení bezpečnostních opatření. Pokud je totiž počítačový systém zabezpečen, dává tím jeho oprávněný uživatel najevo, že jsou v něm obsažena data, která si uživatel explicitně nepřeje jakkoliv zpřístupnit ostatním. Takováto data by proto měla být dle mého názoru chráněna vyššími standardy než data v nezabezpečeném počítačovém systému. Proto právě překonání bezpečnostního opatření je *„samo o sobě natolik nebezpečné jednání, že již nezáleží na závažnosti činu, který pachatel hodlá spáchat."*[176]

Jak vyplývá z výše uvedeného, český trestní zákon tento dodatečný prvek skutečně využívá, a proto bylo při ratifikaci Úmluvy učiněno prohlášení o dodatečných prvcích.[177] Ačkoliv Úmluva umožňuje jako dodatečný prvek stanovit i specifický úmysl, tj. trestní odpovědnost by vznikla jen v případě, pokud by pachatel jednal v úmyslu získat počítačová data nebo s jiným nečestným úmyslem, Česká republika tuto možnost nevyužila (specifický úmysl je prvkem kvalifikovaných skutkových podstat uvedených v druhém až pátém odstavci) a je kriminalizováno i jednání, kdy je hacking cílem sám o sobě. Pokud by součástí skutkové podstaty tohoto trestného činu byl i výše uvedený specifický úmysl, jistě by vznikly potíže s jeho dokazováním. Například v případě, kdy by útočník překonal bezpečnostní opatření počítačového systému a zde získaná data za úplatu poskytl jinému, přičemž by byl prokázán neoprávněný přístup i překonání bezpečnostního opatření, ale již nikoliv poskytnutí získaných dat třetí osobě, nebylo by možné uvedené jednání postihnout. Naopak samotné překonání bezpečnostního opatření je dle mého názoru snazší na dokazování, ale i pokud není možné útočníkovi překonání bezpečnostního opatření prokázat, je možné jeho jednání případně postihnout podle skutkových podstat uvedených v druhém až pátém odstavci.[178]

Otázkou zůstává, zda koncepce § 230 odst. 1 TZ nepostihuje i některá jednání s velmi nízkou nebo i nulovou společenskou nebezpečností. Mnozí hackeři neoprávněně pronikají do počítačových systémů bez škodlivého úmyslu anebo dokonce s úmyslem zvýšit zabezpečení počítačového systému (např. hackeři typu grey hats[179]), což přiznává i důvodová

---

[176] ŠÁMAL, P. a kol. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání, Praha, C. H. Beck, 2012. Str. 2305.

[177] Viz kapitola 4.1.5 této práce.

[178] V uvedeném případě, bude-li prokázáno poskytnutí dat získaných v počítačovém systému třetí osobě, je dle současně platného trestního práva takové jednání postižitelné dle § 230 odst. 2 písm. a) TZ, aniž by bylo nutné prokazovat překonání bezpečnostního opatření. V úvahu by též připadal trestný čin porušování tajemství listin a jiných dokumentů uchovávaných v soukromí dle § 183 TZ.

[179] Grey hats pronikají do počítačových systémů neoprávněně, mnohdy pro zábavu, někdy mohou nabídnout administrátorovi napadeného systému opravu objevených chyb. Blíže viz kapitola 3.1.1 této práce.

zpráva k Úmluvě.[180] V pojetí českého trestního práva je jejich jednání v kyberprostoru ohraničeno soukromím jednotlivců. Tato hodnota je chráněna v případě zneužití soukromí, nebo pokud je pro získání soukromých dat potřeba překonat bezpečnostní opatření. Komentář k TZ popisuje tři způsoby překonání bezpečnostního opatření, a to překonání hesla, spoofing a využití exploitu.[181]

Zatímco první odstavec § 230 TZ chrání primárně důvěrnost (tj. poskytuje počítačovým systémům právní ochranu před hrozbou úniku informací či před hrozbou nelegitimního užití) a počítačový systém je chráněn jako celek, ustanovení druhého odstavce je zaměřeno na integritu a dostupnost (tj. chrání před hrozbou narušení integrity) a jsou jím tak chráněna počítačová data a počítačové programy před neoprávněnými zásahy.[182] Ve druhém odstavci § 230 TZ se objevují dvě další skutkové podstaty vyžadované Úmluvou, a to zásah do dat [písm. a), b) a d) tohoto ustanovení] a počítačové padělání [písm. c) tohoto ustanovení].[183] Pro naplnění alespoň jedné z těchto skutkových podstat musí pachatel vždy získat přístup k počítačovému systému nebo nosiči informací (přičemž přístup může být na rozdíl od skutkové podstaty neoprávněného přístupu uvedené v prvním odstavci i oprávněný) a následně jej některým z vymezených způsobů „zneužít".

Zneužití dat může být u skutkové podstaty ***zásahu do dat*** trojího druhu. Prvním případem je počítačová špionáž, kdy pachatel *„neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací".* Tento případ postihuje § 230 odst. 2 písm. a) TZ. Neoprávněným užitím dat se dle komentáře k TZ rozumí neoprávněná manipulace s daty, tj. užití v rozporu s právní normou (např. porušení obchodní tajemství, použití písemností

---

[180] *The Explanatory Report of the Convention on Cybercrime.* Dostupné z www: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm [citováno dne 9. října 2013]

[181] ŠÁMAL, P. a kol. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání, Praha, C. H. Beck, 2012. Str. 2307. Možnosti překonání hesla a pojmy spoofing a exploit, stejně jako další způsoby provedení kybernetických útoků, vysvětluje kapitola 3.1.1 této práce.

[182] GŘIVNA, T. Offences against the confidentiality, integrity, and availability of computer data in the new Czech Criminal Code. In: HERCZEG, J. HILGENDORF, E. GŘIVNA, T. (Hrsg). *Internetkriminalität und die neuen Herausforderungen der Informationsgesellschaft des 21. Jahrhunderts*. Praha, Wolters Kluwer, 2010.

[183] § 230 odst. 2 TZ: *„Kdo získá přístup k počítačovému systému nebo k nosiči informací a a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací, b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými, c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty."*

osobní povahy), v rozporu s původním účelem nebo bez vědomí či souhlasu autorizovaného uživatele, mimo jiné též nedovolené kopírování na jiný nosič informací.[184]

Počítačová špionáž čili neoprávněné užití dat může přejít v počítačovou sabotáž, kdy pachatel *„data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými“.* Tyto zásahy do integrity nebo dostupnosti dat postihuje § 230 odst. 2 písm. b) TZ. Oproti textu Úmluvy se v tomto ustanovení navíc vyskytuje „jiný způsob zničení dat“ a „učinění dat neupotřebitelnými“. Z pohledu Úmluvy je vymazáním dat ekvivalentem zničení hmotné věci, tedy například i fyzické zničení nosiče obsahujícího data, což je ovšem dle českého trestního zákona chápáno jako jiné zničení dat. Učinění dat neupotřebitelnými, kdy například pachatel data nezmění, ale pouze zakóduje, osobně chápu jako jeden ze způsobů potlačení dat, kterým je zasahováno do dostupnosti počítačových dat.[185]

Poslední trestním právem postižitelný způsob zásahu do dat je počítačová sabotáž dle § 230 odst. 2 písm. d) TZ, kdy pachatel *„neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat“.* Rozdíl mezi poškozením dat, jejich změnou a vložením dat je poněkud neostrý - zatímco při poškození dat dochází k nahrazení části původních dat, při změně jsou původní data zachována, ale jsou doplněna o data nová. Souvislost nových a starých dat ale změní informaci získanou z těchto výsledných dat. U vložení dat dochází k vytvoření zcela nových dat bez ohledu na data stávající.[186] Jiným zásahem se rozumí neoprávněné jednání nesubsumovatelné pod písmena a) až c).[187]

Výše uvedené zneužití dat se může projevit i dle § 230 odst. 2 písm. c) jako tzv. ***počítačové falšování***, kdy pachatel *„padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná*

---

[184] ŠÁMAL, P. a kol. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání, Praha, C. H. Beck, 2012. Str. 2309.

[185] K pojmům vymazání, jiné zničení dat, poškození dat, snížení kvality dat, změna dat, učinění dat nepoužitelnými a potlačení dat blíže viz ŠÁMAL, P. a kol. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání, Praha, C. H. Beck, 2012. Str. 2309.

[186] ŠÁMAL, P. a kol. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání, Praha, C. H. Beck, 2012. Str. 2309 a násl.

[187] Tamtéž, str. 2312.

a srozumitelná“. Tuto skutkovou podstatu může naplnit i oprávněný uživatel počítače, nejedná se proto o útok proti důvěrnosti, integritě ani dostupnosti počítačových dat.

Třetí odstavec § 230 TZ[188] obsahuje dvě kvalifikované skutkové podstaty pro výše uvedená jednání, jejichž naplnění umožňuje užití vyšší trestní sazby. Jedná se o ***počítačový podvod*** u pachatele, který jednal v *„úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch“*. Jde o kriminalizaci širšího okruhu jednání, než vyžaduje Úmluva ve svém čl. 8, neboť je zahrnuto i způsobení škody či jiné újmy (např. na cti).

Druhou kvalifikovanou skutkovou podstatou uvedenou ve třetím odstavci § 230 TZ je ***zasahování do systému***. Tato skutková podstata má odpovídat čl. 5 Úmluvy a chrání primárně před hrozbou potlačení služby. Pokud pachatel spáchal čin uvedený v odstavcích 1 nebo 2 § 230 TZ *„v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat“,* budou splněny podmínky pro užití vyšší trestní sazby. Odlišnost oproti Úmluvě je v prvé řadě v tom, že pachatel musí získat přístup k počítačovému systému nebo k nosiči informací. Jak bylo uvedeno v kapitole 3.1.1, pro uskutečnění hrozby potlačení služby například DDoS útokem nemusí hacker nutně získat přístup k počítačovému systému, a proto není typický DDoS útok postižitelný dle tohoto ustanovení, ale podle trestného činu poškození cizí věci uvedeného v § 228 odst. 1 TZ. Protože je ale nutným předpokladem pro vznik trestní odpovědnosti dle § 228 odst. 1 TZ způsobení na cizím majetku škody nikoliv nepatrné, není česká úprava zcela v souladu s čl. 5 Úmluvy. Na druhou stranu Úmluva vyžaduje kriminalizaci jen závažných omezení funkčnosti, zatímco v § 230 odst. 3 písm. b) TZ i v § 228 odst. 1 TZ není závažnost vyžadována.

Odst. 4 a 5 § 230 TZ vyjmenovává další okolnosti podmiňující použití vyšší trestní sazby, mimo jiné získání značného prospěchu či způsobení značné škody (odst. 4) a získání prospěchu velkého rozsahu či způsobení škody velkého rozsahu (odst. 5). U zmíněných okolností postačí nedbalostní forma zavinění.[189]

---

[188] § 230 odst. 3 TZ: *„Odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2 a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat."*

[189] ŠÁMAL, P. a kol. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání, Praha, C. H. Beck, 2012. Str. 2314.

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

Smyslem tohoto ustanovení je kriminalizovat jednání, které je fakticky pouhou přípravou či pokusem buď k trestnému činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1, 2 TZ, nebo k trestnému činu porušení tajemství dopravovaných zpráv dle § 182 odst. 1 písm. b), c) TZ. Objektem je *„zájem na ochraně společnosti a osob před možným ohrožením vyplývajícím z nekontrolovaného opatření a přechovávání zařízení, nástrojů a prostředků,"*[190] které primárně slouží ke spáchání výše uvedených trestných činů. Ke znakům tohoto trestného činu dle prvního odstavce[191] patří jednak úmysl spáchat trestný čin dle § 230 odst. 1, 2 TZ nebo dle § 182 odst. 1 písm. b), c) TZ,[192] jednak jednání pachatele spočívající v opatření a přechovávání daného prostředku. U přechovávání zákon počítá s tím, že pachatel nemusí mít prostředek u sebe - postačí, že ho má své moci, např. uložený na serveru, k němuž se pachatel může kdykoliv připojit.[193]

Trestné je opatření a přechovávání jak prostředků, které byly primárně vyrobeny k získání neoprávněného přístupu (tj. *„zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části“)*, tak prostředků, které byly původně vytvořeny pro zajištění autorizace oprávněného uživatele (tj. *„počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části“*).

V odstavcích 2 a 3 tohoto ustanovení jsou popsány okolnosti podmiňující užití vyšší trestní sazby, tj. spáchání činu jakožto člen organizované skupiny, a dále zisk značného

---

[190] ŠÁMAL, P. a kol. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání, Praha, C. H. Beck, 2012. Str. 2317.

[191] § 231 odst. 1 TZ: *„Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části, bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti."*

[192] Tyto trestné činy odpovídají požadavkům čl. 6 Úmluvy.

[193] ŠÁMAL, P. a kol. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání, Praha, C. H. Beck, 2012. Str. 2318.

prospěchu pro sebe nebo pro jiného. Ještě vyšší trestní sazba je v případě získání prospěchu velkého rozsahu.

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

Jedním ze specifik kybernetické kriminality je možnost velmi snadno způsobit nevyčíslitelné škody, a to mimo jiné též i neodborným zásahem do počítačového systému. Objekt trestného činu dle § 232 TZ proto chrání *„data a technické či programové vybavení počítačového systému před nedbalostním poškozovacím jednáním, pokud je těmito zásahy způsobena značná škoda."*[194] Aby nedošlo k přílišné kriminalizaci dle § 232 odst. 1 TZ,[195] je nedbalostní způsobení škody podmíněno způsobením značné škody a hrubou nedbalostí.

Pachatelem je právnická nebo fyzická osoba určitého postavení - taková, které ze zaměstnání, povolání, postavení či funkce vyplývá určitá povinnost, nebo kterou zvláštní povinnost ukládá zákon či ji dobrovolně převzala smluvně. Pokud porušením této povinnosti pachatel z hrubé nedbalosti jedná způsobem obdobným ustanovení § 230 odst. 2 písm. b) nebo d) TZ a způsobí tím na cizím majetku značnou škodu, naplní skutkovou podstatu tohoto trestného činu.

Tento trestný čin postihuje zejména některá jednání na pracovišti, například taková, kdy zaměstnanec i přes opakované výtky stále používá výpočetní techniku zaměstnavatele ke svým soukromým účelům. Pokud navštíví webovou stránku pochybného charakteru, v důsledku čehož se do počítačové sítě zaměstnavatele rozšíří virus mazající počítačová data, čímž vznikne na majetku zaměstnavatele značná škoda, naplní tím zaměstnanec skutkovou podstatu tohoto trestného činu.

Ve druhém odstavci tohoto ustanovení je jako okolnost podmiňující použití vyšší trestní sazby uvedeno způsobení škody velkého rozsahu.

---

[194] ŠÁMAL, P. a kol. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání, Praha, C. H. Beck, 2012. Str. 2322.

[195] § 232 odst. 1 TZ: *„Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat, a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty."*

5.1.4 Nezákonný odposlech dat - porušení tajemství dopravovaných zpráv (§ 182) a porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183)

Smyslem čl. 3 Úmluvy, v němž je vyžadována kriminalizace ***nezákonného odposlechu dat***, je ochrana tajemství zpráv dopravovaných v prostředí kyberprostoru. Trestný je úmyslný a neoprávněný odposlech neveřejného přenosu počítačových dat, který je prováděn technickými prostředky. Není rozhodující, zda je prováděn odposlech přenosu směřujícího do nebo z počítačového systému či jen v jeho rámci. Přenosem se rozumí i elektromagnetické vyzařování z počítačového systému, neboť je z něj možné přenášená data rekonstruovat. Přenos musí být neveřejný - nezáleží na veřejnosti či neveřejnosti dat, neboť i neveřejná data mohou být přenášena veřejně; důležitý je jen způsob přenosu.[196] Textu čl. 3 Úmluvy zcela odpovídá ustanovení § 182 odst. 1 písm. c) TZ.

S kybernetickou kriminalitou též souvisí ustanovení § 182 odst. 1 písm. b) TZ, které za trestný prohlašuje i neoprávněný odposlech datové, textové, hlasové, zvukové či obrazové zprávy zasílané prostředím kyberprostoru. Zpráva musí být přiřaditelná ke konkrétnímu, identifikovatelnému adresátu.

Porušením tajemství se rozumí neoprávněné seznámení se s obsahem neveřejného přenosu či přepravované datové či jiné zprávy. V případě prozrazení nebo využití takového tajemství bude pachatel potrestán vyšší sazbou dle druhého odstavce.

Možnosti zákonného prolomení tajemství dopravovaných zpráv osobami činnými v trestním řízení jsou stanoveny odpovídajícími ustanoveními trestního řádu (jedná se o ustanovení § 86 a 87 TŘ, § 88 a 88a TŘ a § 158d odst. 3, 4 TŘ).

Další možnosti postihu kybernetického útoku jsou dány trestným činem porušení ***tajemství listin a jiných dokumentů uchovávaných v soukromí*** dle § 183 TZ, který oproti předcházejícímu ustanovení chrání tajemství hodnot (ve vztahu ke kybernetické kriminalitě jsou těmito hodnotami zejména počítačová data) uchovávaných v soukromí. § 183 TZ postihuje pachatele, který tyto hodnoty poruší tím, že je zveřejní, zpřístupní třetí osobě nebo je jiným způsobem použije. Kybernetické útoky mohou též směřovat k získání dat obsahujících osobní údaje. Podobné útoky postihuje trestný čin ***neoprávněného nakládání s osobními údaji*** dle § 180 TZ, který postihuje i nedbalostní jednání. Chráněny jsou pouze osobní údaje, které byly shromážděné v souvislosti s výkonem veřejné moci, nebo pokud bylo

[196] GŘIVNA, T. K ustanovením Úmluvy o počítačové kriminalitě. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

jejich neoprávněné nakládání provedeno porušením státem uložené nebo uznané povinnosti mlčenlivosti a v souvislosti s touto povinností mlčenlivosti byly i získané. Neoprávněné nakládání s osobními údaji je trestné jen v případě, že nakládání s nimi způsobilo vážnou újmu na právech nebo oprávněných zájmech osoby, které se osobní údaje týkají.

5.1.5 Hmotněprávní postih jednání uvedených v kapitole 3

Možnosti postihu útoků proti počítačovým systémům a počítačovým datům, čili ***kybernetické útoky***, byly detailněji popsány v kapitolách 5.1.1 až 5.1.4. Nyní se pokusím obecné formy hackingu popsané v kapitole 3.1 přiřadit ke konkrétním ustanovením trestního zákoníku, podle kterých by tato jednání mohla být často postižitelná.

Pro *útoky směřující k potlačení služby* se nabízí postih dle § 230 odst. 3 písm. b) TZ, ale protože útočník mnohdy nezíská přístup k počítačovému systému, je v případě způsobení nikoliv nepatrné škody reálný spíše postih dle trestného činu poškození cizí věci § 228 TZ. Útočníci často pro umožnění útoku tohoto typu získávají neoprávněný přístup k počítačovým systémům, z nichž útoky provádějí. Slovy trestního zákoníku tedy překonávají bezpečnostní opatření a získávají tak neoprávněně přístup k počítačovému systému nebo jeho části v úmyslu neoprávněně omezit funkčnost počítačového systému - ovšem jiného než toho, kterého původně napadli, a proto nelze ustanovení § 230 odst. 3 písm. b) TZ ani v tomto případě použít.

Útoky směřující k úniku informací jsou zejména různé metody odposlechu, které porušují tajemství datových či jiných zpráv, tajemství neveřejného přenosu počítačových dat nebo tajemství počítačových dat uchovávaných v soukromí. Proto jsou postižitelné podle § 182 odst. 1 písm. b), c) TZ nebo § 183 TZ. Pokud je pro provedení tohoto útoku získán přístup k počítačovému systému, je dle okolností možné i posouzení dle § 230 odst. 1 TZ (pokud je útok neoprávněný a jsou překonána bezpečnostní opatření) nebo § 230 odst. 2 TZ (pokud útočník jednal ve specifickém úmyslu). V úvahu přichází též uplatnění § 180 TZ.

Mezi *útoky směřující k narušení integrity* jsem v kapitole 3.1 zahrnul útoky pomocí škodlivých programů, které útočníku zajistí neoprávněný přístup a překonání bezpečnostního opatření. Proto je útok pomocí těchto programů postižitelný dle § 230 odst. 1 TZ, v některých případech i dle odstavce 2 písm. a), b) nebo c) nebo odstavce 3 písm. a) nebo b).

Útoky směřující k nelegitimnímu užití se pokoušejí překonat bezpečnostní opatření. Úspěšným útokem proti počítačovému systému nebo jeho části bude vždy naplněna skutková

podstata dle § 230 odst. 1, ale dle chování útočníka v ovládnutém počítačovém systému přichází v úvahu víceméně jakákoliv z výše uvedených skutkových podstat.

Metody sociálního inženýrství jsou způsobilé naplnit skutkovou podstatu trestného činu podvodu dle § 209 TZ. Typicky totiž využívají něčího omylu, čímž se pachatel obohatí a způsobí na cizím majetku škodu nikoliv nepatrnou.

U ***trestné činnosti, při níž je počítačový systém prostředkem jejího páchání***, přichází v úvahu velké množství skutkových podstat, které by dané jednání mohly postihnout, a to zejména trestné činy uvedené v páté hlavě trestního zákoníku. Co se týče trestněprávního postihu spamu, který jsem do této kategorie zařadil v kapitole 3.2, jeho rozesílání by bylo trestné zejména v případě, kdy by mohlo způsobit potlačení služby (viz výše) nebo pokud by trestnost vyplývala z obsahu rozesílaných zpráv (viz níže).

Trestná činnost související s obsahem a s porušením práv duševního vlastnictví může naplňovat skutkové podstaty velkého množství trestných činů. Jistě nepřekvapí trestné činy související s šířením některých druhů pornografie (§ 191 - 193 TZ), trestné činy narušující soužití lidí a související s extremismem (§ 352 - 356 TZ, § 403 - 405 TZ) nebo trestné činy proti průmyslovým právům a proti autorskému právu (zejména § 268 TZ a § 270 TZ). V kyberprostoru je též poměrně častým a velmi snadno proveditelným trestným činem pomluva (§ 184 TZ) nebo šíření poplašné zprávy (§ 357 TZ). S ohledem na kybernetickou bezpečnost je ale nutné zdůraznit též i možnost jednání v kyberprostoru, které může naplnit skutkovou podstatu trestných činů vlastizrady, rozvracení republiky, teroristického útoku, teroru a sabotáže (§ 309 - 314 TZ).

6. KYBERNETICKÁ BEZPEČNOST A JEJÍ PŘEDPOKLÁDANÉ ZÁKONNÉ VYMEZENÍ JAKO SOUČÁST BOJE PROTI POČÍTAČOVÉ KRIMINALITĚ

Boj proti kybernetickému zločinu probíhá na několika úrovních. Z hlediska represe se jedná o zaznamenání nežádoucího jednání popsaného v předcházejících kapitolách, jeho následné vyšetření osobami činnými v trestním řízení a zejména udělení sankčního postihu za toto jednání. Neméně důležitá je ovšem i preventivní složka boje proti kybernetické kriminalitě, jejímž cílem je spáchání trestné činnosti co nejvíce ztížit. Jedna z forem prevence tohoto druhu kriminality je legislativní vymezení kybernetické bezpečnosti, kdy se stát pokouší o zajištění bezpečnosti kyberprostoru a zásadní ztížení nejzávažnějších kybernetických útoků. V současné době jsou předpisy upravující kybernetickou bezpečnost připravovány jak ve světě a v Evropské unii, tak v České republice.

Obor kybernetické bezpečnosti se pohybuje na značně neostré hranici mezi zájmem na ochraně uživatelů kyberprostoru před kybernetickými útoky a zájmem na zachování tzv. práva na informační sebeurčení.[197] Ilustrativním příkladem překročení této hranice jsou okolnosti nedávné aféry vyvolané únikem informací z americké NSA (*National Security Agency*) o projektu PRISM.[198] Ovšem bez určitých zákonem umožněných zásahů do práv na informační sebeurčení nelze ochranu kyberprostoru realizovat, a ostatně i vyšetřování kybernetické trestné činnosti by bylo velice ztížené - dilema mezi ochranou uživatelů a jejich soukromím již bylo naznačeno v kapitole 2.2 této práce.

Důsledkem neschopnosti státu reagovat na kybernetické hrozby mohou být dalekosáhlé potíže. Jen samotná existence kybernetických útoků ohrožuje zájmy jednotlivců i státu; útoky ale mohou dosáhnout takové intenzity a komplexnosti, že může dojít až k paralýze chodu státu. Jako historicky první příklad takových útoků bývá uváděna situace v Estonsku v roce 2007, kdy byly masivními DoS útoky vyřazeny z provozu na několik dní některé součásti kritické infrastruktury státu. K podstatně nebezpečnějším kybernetickým útokům patří rozšiřování škodlivých programů cílených na napadání řídicích systémů kritické

[197] Právo na informační sebeurčení označuje katalog absolutních informačních práv, který zahrnuje jednak ochranu diskrétní informační sféry (především ochrana soukromí a ochrana osobních údajů), jednak právo aktivně přijímat, zpracovávat a komunikovat informace. Blíže viz: *Důvodová zpráva k návrhu zákona o kybernetické bezpečnosti*. Národní bezpečnostní úřad, 2013. Str. 48 - 49. Dostupné také z www: http://www.nbu.cz/cs/aktuality/1398-navrh-zakona-o-kyberneticke-bezpecnosti-byl-predlozen-vlade-ceske-republiky/ [citováno dne 9. října 2013]

[198] Dle některých novinových článků měla NSA bez vědomí veřejnosti získávat od největších světových ISP data o obsahu komunikace v kyberprostoru, k čemuž jí tito ISP měli pomáhat.

infrastruktury. Velmi sofistikovaný červ *Stuxnet* se rozšířil v letech 2009 a 2010, přičemž napadal zejména počítače umístěné v Íránu. Jeho cílem byla počítačová sabotáž íránských zařízení na výrobu obohaceného uranu, což se mu skutečně podařilo.[199] V zemích Blízkého východu se zhruba ve stejné době pravděpodobně rozšiřuje program *Flame*, který byl ale detekován až v polovině roku 2012. Flame je schopen velice sofistikovaně zaznamenat v podstatě jakoukoliv činnost napadeného počítačového systému, a to s velmi nízkou pravděpodobností objevení. Důmyslné provedení tohoto programu naznačuje, že jeho vývoj musel dosáhnout značných nákladů. Dále i s ohledem na skutečnost, že se cíleně rozšířil především v oblasti Blízkého východu, je velmi pravděpodobné, že jej vyvinuli státem podporovaní hackeři.[200] Těmto programům je podobný nebezpečný špionážní program *Red October*, který od roku 2007 získával citlivá vládní a průmyslová data z napadených počítačů, přičemž odhalen byl až v roce 2013.[201]

Z uvedených příkladů je zjevné, že způsobit astronomické škody kybernetickými útoky je stále snazší, nově ale je již reálné způsobit intenzivními útoky například i obecné ohrožení či škody na zdraví (např. ovládnutím či vyřazením z provozu řídicí systém jaderné elektrárny nebo nemocnice). Objevuje se reálné nebezpečí „kyberterorismu".[202] Proti tomuto trendu se v současné době snaží bojovat legislativy mnoha států legislativním zakotvením kybernetické bezpečnosti.

V České republice právě vznikající Zákon o kybernetické bezpečnosti ukládá některým subjektům povinnosti, jejichž evidence může za jistých okolností nalézt značné uplatnění i pro osoby činné v trestním řízení při vyšetřování kybernetické kriminality. Nesplnění některých jiných povinností může vést dle mého názoru až k trestněprávnímu postihu. Z těchto důvodů věnuji výrazný prostor této tématice i v rámci této práce. Jedná

---

[199] DENNING, D. E. *Whither Cyber Terror* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://essays.ssrc.org/10yearsafter911/whither-cyber-terror/

[200] KUŽEL, S. *Kybernetická kriminalita IV: Hacktivismus a kyberterorismus* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://www.businessit.cz/cz/kyberneticka-kriminalita-iii-hacktivismus-a-kyberterorismus.php

[201] SEDLÁK, J. *Na Evropu a země bývalého SSSR útočil komplexní virus.* 14. 1. 2013 [online]. [citováno dne 9. října 2013]. Dostupné z www: http://connect.zive.cz/clanky/na-evropu-a-zeme-byvaleho-sssr-utocil-komplexni-virus/sc-320-a-167139/default.aspx

[202] Kyberterorismus lze chápat jako *„zneužití počítačových technologií proti osobám či majetku za účelem vyvolání strachu nebo vydírání a vymáhání ústupků, zaměřené proti vládním institucím nebo civilní populaci, případně proti jejich segmentům, pro podporu politických, sociálních, ekonomických, případně jiných cílů, zaměřené na informační systémy používané cílovým objektem."* POŽÁR, J. a kol. *Základy teorie informační bezpečnosti.* Praha, Vydavatelství Policejní akademie České republiky, 2007, str. 152.

se o problematiku novou, k níž zatím není dostupná odpovídající odborná literatura, proto jsou níže uvedené jen mé vlastní závěry.

6.1 Úprava kybernetické bezpečnosti mimo Českou republiku

Vyspělé státy světa si uvědomují nebezpečí kybernetických útoků a pokoušejí se případné hrozby minimalizovat. V oblasti kybernetické bezpečnosti produkují množství dokumentů strategického charakteru. USA k ochraně kyberprostoru přistupují z vojenského pohledu - kyberprostor povýšily na svou „pátou válečnou doménu“ (vedle souše, vzduchu, moře a vesmíru), kybernetické velitelství (*US Cyber Command*) podřídily vojenskému velitelství a jedním z hlavních cílů je ochrana vojenské sítě (sítě s doménou nejvyššího řádu .mil) a kritické infrastruktury.[203] Naproti tomu proklamovaným konečným cílem Evropské unie v této oblasti je vytvoření jednotného digitálního trhu, k čemuž je nutnou podmínkou existence bezpečného kyberprostoru.[204] Dokumenty Evropské unie směřující k dosažení kybernetické bezpečnosti byly popsány v kapitole 4.2 této práce.[205]

Z připravovaných směrnic Evropské unie vyplývá povinnost členských států zřídit orgány odpovědné za bezpečnost sítí a informačních systémů a vedle nich nebo i v rámci nich též tým reagující na kybernetické hrozby, tzv. CERT (*Computer Emergency Response Team*).[206] Standardem řady zemí Evropské unie i mimo ní je existence CERT pracovišť na vládní a národní úrovni, přičemž tyto týmy spolupracují mezi sebou, s vnitrostátními ISP i se zahraničními CERT pracovišti.

Počátkem roku 2013 byla oficiálně zahájena činnost již zmíněného ***Evropského centra pro boj proti kybernetické kriminalitě*** (dále jen „**EC3**“), které má plné funkčnosti dosáhnout do roku 2015. EC3, které bylo zřízeno v rámci Europolu, je zaměřeno na závažné formy

---

[203] Ke shrnutí úsilí jednotlivých států - nejen USA - v oblasti kybernetické bezpečnosti viz *Věcný záměr zákona o kybernetické bezpečnosti.* Národní bezpečnostní úřad, 2013. Str. 41 - 43. Dostupné z www: http://www.govcert.cz/cs/legislativa/legislativa/ [citováno dne 9. října 2013]

[204] JOIN/2013/0001. Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů. Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor. Brusel, Vysoká představitelka Evropské unie pro zahraniční věci a bezpečnostní politiku, 2013. Dostupné také z www: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:CS:PDF [citováno dne 9. října 2013]

[205] Zejména Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů. Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor, a dále též návrh směrnice Evropského parlamentu a Rady COM/2013/0027 ze dne 7. 2. 2013 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii. Blíže viz kapitola 4.2 této práce.

[206] Někdy se lze setkat s označením CSIRT - *Computer Security Incident Response Team*.

kybernetické kriminality, zejména organizovaný zločin, kriminalitu spojenou se sexuálním zneužíváním dětí a kybernetické útoky ohrožující kritickou infrastrukturu a informační systémy v Evropské unii.[207] Zároveň má zaručovat svobodný a otevřený Internet.[208] Patrně největším úspěchem EC3 doposud byla spolupráce se španělskou policií vedoucí k dopadení mezinárodní organizované zločinecké sítě, která šířením ransomware[209] dosáhla dle odhadů výdělku až jednoho milionu eur ročně.[210] Předpokládá se dále také spolupráce EC3 s CERT pracovišti členských států.

6.2 Připravovaná úprava kybernetické bezpečnosti v České republice - návrh zákona o kybernetické bezpečnosti

Návrh zákona o kybernetické bezpečnosti, jehož paragrafové znění bylo vypracováno Národním bezpečnostním úřadem (NBÚ), v dubnu 2013 odesláno k meziresortnímu připomínkovému řízení a v červenci 2013 byl návrh zákona předložen vládě,[211] se pokouší mimo jiné i vyhovět požadavkům vyplývajícím z již zmíněných návrhů směrnic Evropské unie. Vymezuje dohledová pracoviště (tj. vládní CERT a národní CERT) a jejich oprávnění na jedné straně a okruh povinných subjektů a jejich povinnosti na straně druhé. **Vládní CERT** je jakožto součást Národního centra kybernetické bezpečnosti (NCKB), jehož činnost je zajišťována NBÚ, v provozu sice již dnes, ale pouze na základě podzákonného právního předpisu, tj. bez zákonného zmocnění. **Národní CERT** je právnická osoba, která uzavře veřejnoprávní smlouvu s NBÚ za účelem spolupráce v oblasti kybernetické bezpečnosti. Cílem zákona je proto nastavit standardy kybernetické bezpečnosti zejména ve státní správě a dát pravomoci NBÚ (resp. NCKB) k tomu potřebné. Tím budou vymezeny zákonné mantinely pro činnost NBÚ jakožto ústředního správního úřadu v oblasti kybernetické bezpečnosti.

---

[207] Blíže viz www: http://www.europol.europa.eu/ec3 [citováno dne 9. října 2013]

[208] *EU cybercrime centre launched by Commissioner Malmström.* BBC, 9. 1. 2013. Dostupné také z www: http://news.bbc.co.uk/democracylive/hi/europe/newsid_9782000/9782597.stm [citováno dne 9. října 2013]

[209] Jedná se o ransomware popsané v referenci č. 127 na str. 51.

[210] *European Cybercrime Centre dismantles its first criminal network [online].* NewEurope Online 14. 2. 2013. [citováno dne 9. října 2013] Dostupné z www: http://www.neurope.eu/article/european-cybercrime-centre-dismantles-its-first-criminal-network

[211] *Návrh zákona o kybernetické bezpečnosti.* Národní bezpečnostní úřad, 2013. Dostupné také z www: http://www.nbu.cz/cs/aktuality/1398-navrh-zakona-o-kyberneticke-bezpecnosti-byl-predlozen-vlade-ceske-republiky/ [citováno dne 9. října 2013]

Zmíněné vymezení mantinelů má podle vyjádření ředitele NCKB Vladimíra Rohela zajistit soulad se zásadou enumerativnosti veřejnoprávních pretenzí zakotvenou v čl. 2 Listiny základních práv a svobod[212] a má tak zamezit jednáním, které je laickou veřejností vnímáno jako „cenzura Internetu“ nebo „odpojování od Internetu“.[213] Zákon má do soukromé sféry zasahovat jen minimálně a do soukromí běžných uživatelů vůbec, neboť pod povinné subjekty běžní uživatele Internetu nespadají. Soukromé subjekty již dnes spolupracují s národním CERT pracovištěm na bázi dobrovolnosti.

Povinné osoby jsou vymezeny v § 3 zákona a lze je rozdělit na dvě skupiny. První - větší - skupina povinných osob má již některé povinnosti uložené Zákonem o elektronických komunikacích. Nový zákon jim přidává jen povinnost oznamovat kontaktní údaje národnímu CERT, přičemž v zákoně není uvedena žádná možnost kontroly ani případné sankce za nesplnění této povinnosti. Další povinnosti lze ukládat a jejich plnění lze kontrolovat za stavu kybernetického nebezpečí.[214] Druhá skupina povinných subjektů má oznamovací povinnost vůči vládnímu CERT, dále povinnost zavést bezpečnostní opatření dle standardů stanovených prováděcím předpisem, vyhledávat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty vládnímu CERT pracovišti a provádět protiopatření ukládaná NBÚ. Do druhé skupiny mají spadat správci informačních nebo komunikačních systémů kritické informační infrastruktury a správci významných informačních systémů. Pravděpodobně se bude jednat o letiště, některá zdravotnická zařízení, některé elektrárny, přenosové soustavy energetických sítí a podobně. Rozdělení subjektů do skupin bude záležitostí prováděcího předpisu. Kritériem tedy není, zdali se jedná o soukromý či veřejný subjekt, ale význam sítě jím provozované a případné ohrožení vzniklé z její nedostupnosti.

Významnou institucí pro kybernetickou bezpečnost je ***Národní centrum kybernetické bezpečnosti***, jehož kompletní funkčnost se očekává až v roce 2015. Plní na národní úrovni

---

[212] Čl. 2 odst. 2 Listiny základních práv a svobod: *„Státní moc lze uplatňovat jen v případech a v mezích stanovených zákonem, a to způsobem, který zákon stanoví.“* Usnesení České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.

[213] ROHEL, V. Interview. In: *Hyde Park ČT 24*. TV, ČT 24, 11. 3. 2013, 20:05. Dostupné také z www: http://www.ceskatelevize.cz/specialy/hydepark/11.3.2013/ [citováno dne 9. října 2013]

[214] Stav kybernetického nebezpečí dle § 24 - 25 Zákona o kybernetické bezpečnosti vyhlašuje předseda vlády České republiky na návrh ředitele NBÚ. V tomto režimu se působnost zákona rozšířit i na subjekty spadající do první skupiny, nikoliv však na běžné uživatele kyberprostoru. Podmínkou pro vyhlášení tohoto stavu je ohrožení základních funkcí státu, kdy by mohly být ohroženy komunikační toky mezi orgány státu nebo narušena kritická infrastruktura. Samotná nedostupnost www stránek je pro vyhlášení stavu kybernetického nebezpečí značně nedostatečná. ROHEL, V. Interview. In: *Hyde Park ČT 24*. TV, ČT 24, 11. 3. 2013, 20:05. Dostupné také z www: http://www.ceskatelevize.cz/specialy/hydepark/11.3.2013/ [citováno dne 9. října 2013]

obdobnou úlohu jako EC3, rozsah jeho věcné působnosti je však značně užší - nemá ambici ani nástroje jakkoliv reagovat na kriminalitu související s obsahem nebo na kriminalitu související s počítači. Jedná se o technický tým koordinující spolupráci ostatních subjektů činných při vyšetřování kybernetických útoků. NCKB má spolupracovat s osobami činnými v trestním řízení, s národním CERT i se zahraničními CERT pracovišti a s ISP. Podnětem činnosti NCKB mají být zejména hlášení subjektů, ať již činěna dobrovolně nebo z povinnosti uložené zákonem (§ 9 Zákona o kybernetické bezpečnosti). NKCB ale nemůže nařídit přímé zásahy v kyberprostoru, jako například odpojení uživatele od Internetu - k tomu jsou oprávněny jen osoby činné v trestním řízení.

6.3 Trestněprávní souvislosti se zákonem o kybernetické bezpečnosti

Ačkoliv Zákon o kybernetické bezpečnosti není normou trestního práva, spatřuji v něm několik důsledků, které mohou nalézt své uplatnění i v trestněprávní rovině. Jedná se o zvýšení preventivních opatření, dále o posílení spolupráce mezi jednotlivými subjekty při vyšetřování kybernetické kriminality, a též o stanovení nových povinností, jejichž nesplnění lze posoudit jako hrubou nedbalost dle § 232 TZ odst. 1.

6.3.1 Kybernetická bezpečnost jako prevence kybernetické kriminality

Standardizaci bezpečnostních organizačních i technických opatření považuji za silný nástroj prevence. Z rozsáhlého seznamu organizačních a technických opatření předpokládaných zákonem o kybernetické bezpečnosti[215] vyplývá, že bezpečnostní opatření nejsou chápána jen jako pouhá pasivní obrana před kybernetickými útoky, která mají za cíl zabránit cílenému průniku. Moderním trendem je neposilovat pouze tuto pasivní obranu, ale zaměřit se více na monitoring systému (schopnost včas detekovat bezpečnostní incident

[215] § 6 Zákona o kybernetické bezpečnosti vymezuje rozsah bezpečnostních opatření, která některé povinné subjekty budou mít za povinnost dodržovat. Jedná se o organizační opatření uvedená ve druhém odstavci (*systém řízení bezpečnosti informací, řízení rizik, bezpečnostní politika, organizační bezpečnost, stanovení bezpečnostních požadavků pro dodavatele, řízení aktiv, bezpečnost lidských zdrojů, řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému, řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému, akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů, zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, řízení kontinuity činností a kontrola a audit kritické informační infrastruktury a významných informačních systémů*) a technická opatření uvedená ve třetím odstavci (*fyzická bezpečnost, nástroj pro ochranu integrity komunikačních sítí, nástroj pro ověřování identity uživatelů, nástroj pro řízení přístupových oprávnění, nástroj pro ochranu před škodlivým kódem, nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a správců, nástroj pro detekci kybernetických bezpečnostních událostí, nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí, aplikační bezpečnost, kryptografické prostředky, nástroj pro zajišťování úrovně dostupnosti informací a bezpečnost průmyslových a řídících systémů*). Konkrétní obsah bezpečnostních opatření stanoví prováděcí právní předpis.

a správně jej analyzovat) a na reakci (schopnost správně zakročit proti bezpečnostnímu incidentu).[216] Zákon též přisuzuje význam i jiným než technickým složkám bezpečnostních opatření.

Pokud se podaří nastavit a dodržovat vysoké standardy bezpečnosti počítačových systémů, lze odůvodněně předpokládat, že možnosti útočníků v kyberprostoru budou při páchání některých forem kybernetické kriminality značně ztížené. Otázkou ovšem zůstává, zda je ke standardizaci bezpečnosti potřeba zvláštního zákona, když jistě existuje racionální motivace uživatelů kyberprostoru (tedy nejen povinných subjektů dle Zákona o kybernetické bezpečnosti) k zajištění svých vlastních bezpečnostních opatření pro odvracení kybernetických útoků. Požadavek na standardy, které povinné subjekty - správci informačních nebo komunikačních systémů kritické informační infrastruktury a správci významných informačních systémů; ostatním subjektům bude standardizace jen doporučena - budou muset dodržovat, se tak může snadno stát jen novou byrokratickou přítěží. Vše ovšem záleží na konkrétním vymezení těchto povinností v prováděcím předpise.

Jako dobrou příležitost pro zvýšení prevence spatřuji i v předpokládané spolupráci mezi vládním a národním CERT, mezi těmito týmy a jejich zahraničními protějšky, mezi těmito týmy a soukromými subjekty a zejména též mezi těmito týmy a osobami činnými v trestním řízení. Určitá spolupráce mezi většinou těchto subjektů již existuje na bázi dobrovolnosti, která bude režimem Zákona o kybernetické bezpečnosti zachována. Nově budou v oblasti spolupráce vymezeny další povinnosti některých povinných subjektů vůči vládnímu CERT a některých subjektů vůči národnímu CERT. Tento režim jen posílí současnou spolupráci státu a definičních autorit v kyberprostoru, která je pro řádnou vymahatelnost práva nezbytná.[217] Existence fungujícího orgánu (NCKB) koordinujícího vnitrostátní spolupráci a schopného rychlé komunikace se zahraničními orgány (zahraniční CERT, EC3, ENISA, zprostředkovaně skrze tyto orgány i zahraniční orgány činné v trestním řízení) by též mělo vést k lepší spolupráci při vyšetřování kybernetické kriminality.

---

[216] SVOBODA, I. Aktuální kybernetické hrozby a možnosti jejich prevence, detekce a řešení. In: *Konference o kybernetické bezpečnosti, Poslanecká sněmovna Parlamentu České republiky*, 16. 5. 2013. Audiozáznam a prezentace dostupné z www: http://www.viktorpaggio.cz/prezentace-a-audiozaznam-ze-seminare-o-kyberneticke-bezpecnosti-16-kvetna-2013/ [citováno dne 9. října 2013]

[217] K vymahatelnosti práva a roli definičních autorit v kyberprostoru viz kapitoly 2.1 a 2.2 této práce.

6.3.2 Evidence bezpečnostních incidentů jako podklad využitelný v trestním řízení

Při vyšetřování kybernetické kriminality existuje obecná povinnost vyhovět dožádání orgánů činných v trestním řízení dle § 8 odst. 1 TŘ.[218] V této souvislosti je proto zajímavé ustanovení § 10 návrhu zákona o kybernetické bezpečnosti, podle kterého vede NBÚ tzv. *evidenci incidentů*, která obsahuje pro každý kybernetický bezpečnostní incident údaje o jeho hlášení, o identifikačních údajích systémů napadených tímto incidentem, o zdroji tohoto incidentu, a postup při jeho řešení. Součástí evidence incidentů mohou být [§ 10 odst. 2 v souv. s § 22 písm. e) až g)] i údaje o subjektech, které nejsou dle zákona chápány jako povinné. Tyto subjekty mohou totiž NBÚ poskytnout údaje o sobě např. při dobrovolném nahlášení bezpečnostního incidentu nebo při spolupráci s národním CERT. Součástí evidence incidentů se tedy mohou často stát i údaje od soukromých subjektů, které jinak stojí mimo působnost zákona, což považuji za nevhodné a ve svém výsledku i kontraproduktivní.[219]

Údaje z evidence incidentů může NBÚ dle § 10 odst. 3 Zákona o kybernetické bezpečnosti poskytovat jen *„orgánům veřejné moci pouze pro plnění úkolů v rámci jejich působnosti,“* tedy zákon jde nad rámec § 8 odst. 1 TŘ, neboť je možné údaje poskytnout nejen orgánům činným v trestním řízení. Na základě správního uvážení může dále NBÚ údaje dle čtvrtého odstavce téhož ustanovení poskytnout *„národnímu CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným subjektům působícím v oblasti kybernetické bezpečnosti,“* ale těmto subjektům pouze *„v rozsahu nezbytném pro zajištění ochrany kybernetického prostoru.“* V následujícím ustanovení (§ 11) je uveden zákaz poskytnout některé údaje z evidence incidentů, ale výjimkou z tohoto zákazu jsou subjekty vymezené v § 10 odst. 3, 4 zákona. Zvláštní na této formulaci je zejména fakt, že subjektům jiným než uvedeným v této výjimce nemůže NBÚ údaje vůbec poskytnout. Jediné zákonné zmocnění pro poskytování údajů je totiž uvedeno právě v § 10 odst. 3, 4 Zákona o kybernetické bezpečnosti. Pro subjekty vymezené v těchto ustanoveních je tedy možné poskytnout všechny údaje z evidence incidentů, a proto -

[218] Již uvedená v kapitole 2.1.2 této práce.

[219] Rozsah evidovaných údajů není zákonem stanoven a bude tak záležet na prováděcím předpise, resp. správním uvážením NBÚ. Je otázka, jak vysoká bude vůle osob podávajících hlášení o bezpečnostních incidentech takto postupovat dobrovolně, když nebudou mít jistotu, jak je s danými údaji nakládáno. Bude-li v praxi NBÚ pro hlášení bezpečnostních incidentů vyžadovat velké množství údajů o osobě podávající hlášení, ochota ke spolupráci bude velmi malá. Domnívám se, že z tohoto důvodu by některé údaje měly být vyňaty z evidence incidentů.

v souvislosti se závěrem z předchozího odstavce - může dojít k zásahu do oprávněných zájmů i jiných než povinných osob.

V současné době jsou kybernetické bezpečnostní incidenty zaznamenávány více subjekty a evidence incidentů neexistuje v žádné centrální podobě. Vznik takové databáze může velmi usnadnit vyšetřování kybernetických incidentů i úsilí orgánů činných v trestním řízení při potírání kybernetické kriminality. Bude ovšem velmi záležet na praxi NBÚ, jestli údaje z evidence naleznou své praktické uplatnění, nebo zda se evidence incidentů stane pouhým nástrojem byrokratického obtěžování. Též je třeba zdůraznit, že se může jednat o vysoce citlivé údaje o zabezpečení velkého množství identifikovatelných počítačových systémů, které by v rukou kybernetických útočníků mohly napáchat značné škody - v takovém případě by poněkud paradoxně mohlo dojít k celkovému zničení kybernetické obrany jen v důsledku nepovedené snahy státu ji zvýšit.

6.3.3 Nesplnění povinností vyplývajících ze zákona o kybernetické bezpečnosti jako hrubá nedbalost dle § 232 TZ

K povinnostem, které zákon o kybernetické bezpečnosti v současné verzi ukládá povinným osobám, patří povinnost hlásit kybernetické bezpečností incidenty, nahlásit kontaktní údaje a provádět tzv. protiopatření uložená NBÚ. Nad výkonem těchto povinností vykonává NBÚ kontrolu a zjistí-li nedostatky, uloží nápravná opatření k jejich odstranění. Za běžného režimu, tj. není-li vyhlášen stav kybernetického nebezpečí, je možné kontrolovat, ukládat nápravná opatření a případné sankce (až do výše 100.000,- Kč) jen správcům informačního nebo komunikačního systému kritické informační infrastruktury a správcům významného informačního systému.

V praxi může dojít k situaci, kdy se povinný subjekt nebude řídit protiopatřeními uloženými NBÚ, nebude respektovat ani nápravná opatření a proto mu bude uložena sankce. Může ovšem i nadále porušovat tuto povinnost uloženou podle zákona. Domnívám se, že pak může být za určitých okolností vhodné posuzovat opakované porušování zákonných povinností jako hrubou nedbalost v souvislosti s § 232 odst. 1 písm. a) TZ.[220]

Povinnosti vyplývající ze zákona o kybernetické bezpečnosti, tedy povinnosti provádět protiopatření uložená NBÚ, jsou bezesporu požadavkem náležité opatrnosti. Její porušení

[220] K trestnému činu poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti dle § 232 TZ viz výklad kapitoly 5.1.3.

může nasvědčovat o takovém přístupu pachatele k tomuto požadavku, který svědčí o zřejmé bezohlednosti k zájmům chráněným trestním zákonem. Opakované porušování povinnosti provádět protiopatření uložená NBÚ tak dle mého názoru může být (samozřejmě v závislosti na dalších okolnostech případu) hrubou nedbalostí podle § 16 odst. 2 TZ.

Pro naplnění skutkové podstaty § 232 odst. 1 písm. a) TZ je dále třeba, aby pachatel data uložená v počítačovém systému nebo na nosiči informací zničil, poškodil, pozměnil nebo učinil neupotřebitelnými, a tím způsobil na cizím majetku značnou škodu.

Pokud subjekt opakovaně nerespektuje protiopatření, v důsledku čehož skutečně dojde ke kybernetickému útoku s následkem zničení, poškození, pozměnění dat nebo učinění dat neupotřebitelnými, čímž bude způsobena na cizím majetku značná škoda, může být proto trestně odpovědný dle uvedeného ustanovení. V některých extrémních případech, kdy by subjekt zaujal k nebezpečí škodlivého následku lhostejnost, by v případě nerespektování protiopatření mohlo jít až o nepřímý úmysl, a hrozil by tak postih dle ustanovení § 230 odst. 2 písm. b).

Je ovšem třeba při výkladu pojmu hrubé nedbalosti postupovat zdrženlivě, aby ustanovení § 232 TZ *„postihovalo jen ty pachatele, kteří se nedbalostního jednání dopustí v důsledku nedodržení dostatečné míry náležité opatrnosti při zřejmé bezohlednosti k ochraně zájmů chráněných trestním zákonem, a nebude docházet k postihu „běžných lidských selhání“, ke kterým dojde i při zachování náležité opatrnosti.“*[221] Nemyslím si, že by bylo správné postihovat trestním právem například bankovní ústav, který nenahlásil kybernetický bezpečnostní incident ve svém informačním systému kritické infrastruktury.[222] V tomto případě by ovšem bylo značně obtížné dokázat příčinnou souvislost mezi porušením povinnosti (nenahlášení bezpečnostního incidentu) a vznikem značné škody.

Dalším případem trestní odpovědnosti může být zaměstnanec NBÚ, který se podílel na řešení kybernetických bezpečnostních incidentů. Zaměstnanec může porušit povinnost mlčenlivosti stanovenou § 12 návrhu zákona o kybernetické bezpečnosti a zpřístupnit veřejnosti údaje z evidence incidentů, s jejichž využitím dojde k sérii kybernetických útoků

---

[221] HRUŠÁKOVÁ, M. Vybrané majetkové trestné činy v novém trestním zákoníku ve srovnání s aktuální úpravou, se zaměřením na nedbalostní trestné činy. In: *Bulletin advokacie.* 10/2009, s. 73 a násl.

[222] Již v současnosti je neochota oznamovat orgánům činným v trestním řízení bezpečnostní incidenty v kyberprostoru značně nízká mimo jiné u bankovních ústavů. Důvodem je obava ze ztráty důvěryhodnosti v očích veřejnosti. Dle některých odhadů míra latence u počítačových bankovních podvodů v minulosti dosahovalo i poměru jednoho oznámeného případu na dvacet tisíc neoznámených. SMEJKAL, V. *Internet a §§§.* Praha; Grada, 2001, str. 162 a násl.

způsobujících značnou škodu. Mezi porušením povinnosti mlčenlivosti a těmito útoky je souvislost spočívající v tom, že takový následek zaměstnanec mohl a měl předpokládat - jistě byl v tomto ohledu zvlášť proškolen. Proto v tomto jednání spatřuji naplnění skutkové podstaty § 232 odst. 1 písm. a) TZ.

Domnívám se tedy, že zákonem o kybernetické kriminalitě dojde k rozšíření povinností, jejichž porušením může být naplněna skutková podstata uvedená v § 232 odst. 1 písm. a) TZ, resp. též § 230 odst. 2 písm. b).

Ve světle výše uvedených skutečností, dle kterých může být povinný subjekt trestně odpovědný za nerespektování nápravných opatření uložených NBÚ, si dovoluji zpochybnit oprávněnost sankce uložené za toto nerespektování. Jsem přesvědčen o tom, že v mnohých případech může vhodné nápravné opatření zvolit lépe sám povinný subjekt, k čemuž mě vedou tři důvody. Zaprvé považuji totiž za nesporné, že povinný subjekt bude svou síťovou infrastrukturu znát lépe než vzdálený státní úřad, a může proto odůvodněně zvolit jiné řešení než to nařizované úřadem. Zadruhé, racionálně uvažující povinný subjekt má svou vlastní motivaci k zabezpečení svých sítí a proto sám aktivně hledá nejlepší možné řešení. Naproti tomu úředník NBÚ může být motivován jen svou paušální odměnou za práci, pročež může zvolit řešení jednoduché, zato neúčinné, zbytečné či kontraproduktivní. A zatřetí, nejlepší odborníci v oboru informačních technologií jsou málokdy zaměstnáni ve státním sektoru, neboť soukromý sektor jim dokáže nabídnout podstatně zajímavější platové ohodnocení. Proto soukromý subjekt, zaměstnávající velmi dobře placené specialisty, může přijít s řešením bezpečnostního incidentu, které je diametrálně odlišné od nápravného opatření uloženého NBÚ - a to navzdory faktu, že úředník NBÚ bude mít přístup do evidence bezpečnostních incidentů a z toho plynoucí informace o bezpečnostních incidentech a jejich řešení.

Dle současného návrhu Zákona o kybernetické bezpečnosti by tento soukromý subjekt dostal vysokou pokutu bez ohledu na to, zda jeho odlišné řešení bezpečnostního incidentu bylo dobré či špatné. Pokud by sankce ale vůbec neexistovala a nápravné opatření by mělo jen doporučující charakter, měl by povinný subjekt možnost volby - buď se řídit doporučením daným státem, nebo zvolit své vlastní řešení bezpečnostního incidentu, ale přijmout za něj plnou odpovědnost. V případě, že by vlastní řešení prokazatelně vedlo ke vzniku škody, přicházela by v úvahu trestní odpovědnost dle výše uvedených závěrů. Tento režim by umožnil povinným subjektům aktivně hledat vlastní řešení bezpečnostních incidentů

a nespoléhat se jen na NBÚ, a zároveň by nápravná opatření nemohla být lehkomyslnými povinnými subjekty zcela ignorována.

Odlišně by musel být upraven režim pro státní povinné subjekty, neboť trestní odpovědnost České republiky a územních samosprávných celků při výkonu veřejné moci je zákonem o trestní odpovědnosti právnických osob zcela vyloučena.[223] Ovšem ani režim navrhovaný zákonem není pro státní povinné subjekty nejvhodnější. Jistě není totiž ideální řešení, kdy stát trestá pokutou sám sebe nebo územně samosprávný celek, a lze argumentovat proti efektivnosti takové sankce.

[223] § 6 odst. 1 zákona o trestní odpovědnosti právnických osob.

ZÁVĚR

Cílem diplomové práce bylo vysvětlit pojmy spadající do oblasti internetové a počítačové kriminality a charakterizovat tuto v dnešní době velice aktuální složku trestního práva. Z důvodu chystaného zákona o kybernetické bezpečnosti jsem se zaměřil na trestnou činnost ohrožující kybernetickou bezpečnost, nešlo ale pominout ani obecnější otázky legitimity a působnosti trestněprávní regulace v kyberprostoru.

Z důvodu současného ratifikačního procesu Úmluvy o počítačové kriminalitě jsem považoval za vhodné posoudit též soulad s požadavky plynoucími z mezinárodního práva a evropských předpisů. Z tohoto důvodu jsem provedl rozbor odpovídajících trestněprávních norem, zejména § 182, 183 a 230 - 232 trestního zákoníku, kde jsou uvedeny skutkové podstaty nejvíce související s internetovou a počítačovou kriminalitou ohrožující kybernetickou bezpečnost. Zkoumání jsem podrobil i další ustanovení trestního zákoníku a trestního řádu, ale též i jiné normy, například zákon o trestní odpovědnosti právnických osob a řízení proti nim. Závěrem mohu konstatovat, že český zákonodárce při provádění mezinárodních a evropských závazků nijak zásadně neselhává, a že široká paleta možností kybernetických zločinců je z pohledu trestního práva hmotného postižitelná v téměř celém svém rozsahu.

Práce se dále zabývala chystaným zákonem o kybernetické bezpečnosti, zejména jeho vlivem na trestní právo. Trestněprávní důsledky tohoto zákona spatřuji ve zvýšení preventivních opatření, v možném usnadnění vyšetřování kybernetické kriminality, a též ve stanovení povinností, jejichž nesplněním může být za určitých podmínek založena trestní odpovědnost. Bohužel důsledky chystaného zákona nelze v současnosti přesně odhadnout. Velmi totiž záleží na prováděcím předpise k tomuto zákonu, zda se zákon o kybernetické bezpečnosti stane účinným nástrojem boje proti internetové a počítačové kriminalitě.

SEZNAM POUŽITÉ LITERATURY

Učebnice

NOVOTNÝ, O., VOKOUN, R., ŠÁMAL, P. a kol. *Trestní právo hmotné.* Zvláštní část. 6. vydání, Praha, Wolters Kluwer ČR, a. s., 2010.

POŽÁR, J. a kol. *Základy teorie informační bezpečnosti.* Praha, Vydavatelství Policejní akademie České republiky, 2007.

ŠIMOVČEK, I. a kol. *Kriminalistika.* Plzeň, Aleš Čeněk, 2011.

Komentáře

ŠÁMAL, P. a kol. *Trestní zákoník I. § 1 až 138. Komentář.* 2. vydání, Praha, C. H. Beck, 2012.

ŠÁMAL, P. a kol. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání, Praha, C. H. Beck, 2012.

Monografie

JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Druhé vydání, Praha, 2013.

JIROVSKÝ, V. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, 2007.

MALEK, K. *Strafsachen im Internet*. Heidelberg, Müller, 2005.

MCQUADE, S. C. *Encyclopedia of cybercrime.* Westport, Conn, Greenwood Press, 2009.

POLČÁK, R. *Internet a proměny práva*. Praha, Auditorium, 2012.

POLČÁK, R. *Právo na internetu: Spam a odpovědnost ISP*. Brno, Computer Press, 2007.

SMEJKAL, V. *Internet a §§§*. Praha, Grada, 2001.

Články

BRECHLEROVÁ, D. Sociální inženýrství. In: *IT Systems, 3/2007*. Dostupný také z www: http://www.systemonline.cz/it-security/socialni-inzenyrstvi.htm [citováno dne 9. října 2013].

GŘIVNA, T. K ustanovením Úmluvy o počítačové kriminalitě. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

GŘIVNA, T. Offences against the confidentiality, integrity, and availability of computer data in the new Czech Criminal Code. In: HERCZEG, J. HILGENDORF, E. GŘIVNA, T. (Hrsg). *Internetkriminalität und die neuen Herausforderungen der Informationsgesellschaft des 21. Jahrhunderts*. Praha, Wolters Kluwer, 2010.

HRUŠÁKOVÁ, M. Vybrané majetkové trestné činy v novém trestním zákoníku ve srovnání s aktuální úpravou, se zaměřením na nedbalostní trestné činy. In: *Bulletin advokacie, 10/2009*.

POLČÁK, R. Autoritativní regulace kyberprostoru a legitimita trestního práva. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008.

SMEJKAL, V. Legislativa na rozcestí. In: *CHIP, 7/1999.* Dostupný také z www: http://www.jvproject.cz/Archiv_CHIP/1999/Chip_07_99.pdf [citováno dne 9. října 2013].

VALERIUS, B. Zum Anwendungsbereich nationaler Rechtsordnungen im Zeitalter des Internets. In: HERCZEG, J. HILGENDORF, E. GŘIVNA, T. (Hrsg). *Internetkriminalität und die neuen Herausforderungen der Informationsgesellschaft des 21. Jahrhunderts*. Praha, Wolters Kluwer, 2010.

ZAVRŠNIK, A. Definiční problémy a kriminologická specifika kyberzločinu. In: GŘIVNA, T., POLČÁK, R. (eds.). *Kyberkriminalita a právo.* Praha, Auditorium, 2008

Judikatura a rozhodovací praxe

ČESKO. Nález Ústavního soudu č. 94/2011, sp. zn. Pl. ÚS 24/10. In: *Sbírka zákonů*. 22. 3. 2011, ročník 2011, částka 35.

ČESKO. Rozsudek Nejvyššího soudu ze dne 16. 01. 2001, sp. zn. 4 Tz 265/2000, dostupné na www.nsoud.cz.

NĚMECKO. Rozsudek Bundesgerichtshof (Spolkový soudní dvůr, nejvyšší instance v trestních věcech Spolkové republiky Německo) 1 StR 184/00 ze dne 12. 12. 2000. In: *BGHSt 46, 212.* Dostupné z www: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=20678&pos=0&anz=1 [citováno dne 9. října 2013].

SPOLEČNOST NÁRODŮ. Rozsudek Stálého dvora mezinárodní spravedlnosti ze dne 7. 9. 1927. In: *Publications of the Permanent Court of International Justice, Series A - No. 10; Collection of Judgments*. Leyden, A. W. Sijthoff's Publishing Company, 1927. Dostupné také z www: http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm [citováno dne 9. října 2013].

Právní předpisy

ČESKO. Usnesení České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky. In: *Sbírka zákonů*. 16. 12. 1992, ročník 1993, částka 1.

ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In: *Sbírka zákonů.* 29. 11. 1961, ročník 1961, částka 66.

ČESKO. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. In: *Sbírka zákonů*. 4. 4. 2000, ročník 2000, částka 32.

ČESKO. Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). In: *Sbírka zákonů.* 29. 7. 2004, ročník 2004, částka 166.

ČESKO. Zákon č. 127/2005, o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). In: *Sbírka zákonů.* 22. 2. 2005, ročník 2005, částka 43.

ČESKO. Zákon č. 273/2008 Sb, o Policii České republiky. In: *Sbírka zákonů.* 17. 7. 2008, ročník 2008, částka 91.

ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In: *Sbírka zákonů.* 8. 1. 2009, ročník 2009, částka 11.

ČESKO. Zákon č. 89/2012 Sb., občanský zákoník. In: *Sbírka zákonů.* 22. 3. 2012, ročník 2012, částka 33.

EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu). Dostupné z www: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:25:32000L0031:CS:PDF [citováno dne 9. října 2013].

EVROPSKÁ UNIE. Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům. Dostupné z www: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:CS:PDF [citováno dne 9. října 2013].

EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES. Dostupné z www: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:cs:PDF [citováno dne 9. října 2013].

EVROPSKÁ UNIE. Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů JOIN/2013/0001 ze dne 7. 2. 2013. Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor. Dostupné také z www: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:CS:PDF [citováno dne 9. října 2013].

EVROPSKÁ UNIE. Návrh směrnice Evropského parlamentu a Rady COM/2013/0027 ze dne 7. 2. 2013 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii. Dostupné z www: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:CS:PDF [citováno dne 9. října 2013].

EVROPSKÁ UNIE. 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. Dostupné z www: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:CS:PDF [citováno dne 9. října 2013].

NĚMECKO. Strafgesetzbuch. In der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 6 Absatz 18 des Gesetzes vom 10. Oktober 2013 (BGBl. I S. 3799). (Německý trestní zákon.)

RADA EVROPY. Úmluva Rady Evropy č. 185 ze dne 23. 11. 2001 o počítačové kriminalitě. Dostupná také z http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [citováno dne 9. října 2013]. Český překlad srov. Sněmovní tisk č. 890, 6. volební období.

Kvalifikační práce

POLČÁK, R. *Normativní regulace soutěže v prostředí informačních sítí.* Brno, 2006. Disertační práce. Právnická fakulta Masarykovy univerzity v Brně. Vedoucí práce prof. JUDr. Petr Hajn, DrSc.. Dostupné také z www: http://is.muni.cz/th/21177/pravf_d/ [citováno dne 9. října 2013].

Internetové zdroje

CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks [online]. [citováno dne 9. října 2013]. Dostupné z www: http://www.cert.org/advisories/CA-1996-21.html

ČÍŽEK, J. *TOR: Skutečně anonymní internet* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://www.zive.cz/clanky/tor-skutecne-anonymni-internet/sc-3-a-149055/default.aspx

DENNING, D. E. *Whither Cyber Terror* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://essays.ssrc.org/10yearsafter911/whither-cyber-terror/

HOEREN, T. *Internetrecht.* Universität Münster, Münster, 2012. [online]. [citováno dne 9. října 2013]. Dostupné z www: http://www.uni-muenster.de/Jura.itm/hoeren/lehre/materialien

HOUSER, P. *Kolik lze vydělat počítačovou kriminalitou* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://computerworld.cz/securityworld/kolik-lze-vydelat-pocitacovou-kriminalitou-47816

HRUSKA, J. *US Cyber Command Admits Offensive Cyberwarfare Capabilities, Fundamental Shift In US Doctrine* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://hothardware.com/News/US-Cyber-Command-Admits-Offensive-Cyberwarfare-Capabilities-Fundamental-Shift-In-US-Doctrine/

KUŽEL, S. *Kybernetická kriminalita IV: Hacktivismus a kyberterorismus* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://www.businessit.cz/cz/kyberneticka-kriminalita-iii-hacktivismus-a-kyberterorismus.php

MILLS, E. *Old-time hacktivists: Anonymous, you've crossed the line* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://news.cnet.com/8301-27080_3-57406793-245/old-time-hacktivists-anonymous-youve-crossed-the-line/

NÝVLT, V. *Internet mimo provoz? DDoS útok lze koupit za pár korun* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://technet.idnes.cz/ddos-hrozba-cxk-/sw_internet.aspx?c=A130305_072420_sw_internet_nyv

POLČÁK, R. *Legislativa v České republice* [online].[citováno dne 9. října 2013]. Dostupné z www: http://www.cybersecurity.cz/law.html.

SEDLÁK, J. *Na Evropu a země bývalého SSSR útočil komplexní virus.* 14. 1. 2013 [online]. [citováno dne 9. října 2013]. Dostupné z www: http://connect.zive.cz/clanky/na-evropu-a-zeme-byvaleho-sssr-utocil-komplexni-virus/sc-320-a-167139/default.aspx

TIŠNOVSKÝ, P. *Jak se zrodil procesor* [online]. [citováno dne 9. října 2013]. Dostupný z www: http://www.root.cz/clanky/jak-se-zrodil-procesor/

TOLAR, O. *Lze dospět k sebevraždě díky Internetu?* [online]. [citováno dne 9. října 2013]. Dostupné z www: http://www.lupa.cz/clanky/lze-dospet-k-sebevrazde-diky-internetu/

European Cybercrime Centre dismantles its first criminal network [online]. NewEurope Online 14. 2. 2013. [citováno dne 9. října 2013]. Dostupné z www: http://www.neurope.eu/article/european-cybercrime-centre-dismantles-its-first-criminal-network

European Cybercrime Centre [online]. [citováno dne 9. října 2013]. Dostupné z www: http://www.europol.europa.eu/ec3

Electronic Frontier Foundation [online]. [citováno dne 9. října 2013]. Dostupné z www: http://www.eff.org/

Symantec Internet Security Threat Report - 2013 [online]. [citováno dne 9. října 2013]. Dostupné z www: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

Hesla, hesla, hesla… [online]. [citováno dne 9. října 2013]. Dostupné z www: http://www.viry.cz/hesla-hesla-hesla/

Ostatní

ČSN ISO/IEC 2382-1:1998. *Informační technologie - Slovník - Část 1: Základní termíny*. Praha, Český normalizační institut, 1998.

Doporučení ITU-T X.1205 - Overview of Cybersecurity. Organizace spojených národů, Mezinárodní telekomunikační unie, 2008. Dostupné také z: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.1205.

Důvodová zpráva k návrhu zákona o kybernetické bezpečnosti. Národní bezpečnostní úřad, 2013. Dostupné také z www: http://www.nbu.cz/cs/aktuality/1398-navrh-zakona-o-kyberneticke-bezpecnosti-byl-predlozen-vlade-ceske-republiky/ [citováno dne 9. října 2013]

EU cybercrime centre launched by Commissioner Malmström. BBC, 9. 1. 2013. Dostupné také z www: http://news.bbc.co.uk/democracylive/hi/europe/newsid_9782000/9782597.stm [citováno dne 9. října 2013]

GATES, Bill. *The road ahead: completely revised and up-to-date*. Druhé vydání. London, Penguin Books, 1996.

GIBSON, W. *Jak vypálit Chrome.* Brno, Návrat, 2004. Překlad Ondřej Neff.

GIBSON, W. *Neuromancer.* Plzeň, Laser, 1992.

LESSIG, L. *Free Culture*. New York, The Penguin Press, 2004. Pod licencí Creative Commons k volnému stažení z www: http://www.free-culture.cc/freeculture.pdf [citováno dne 9. října 2013]

Návrh zákona o kybernetické bezpečnosti. Národní bezpečnostní úřad, 2013. Dostupné také z www: http://www.nbu.cz/cs/aktuality/1398-navrh-zakona-o-kyberneticke-bezpecnosti-byl-predlozen-vlade-ceske-republiky [citováno dne 9. října 2013]

ROHEL, V. Interview. In: *Hyde Park ČT 24*. TV, ČT 24, 11. 3. 2013, 20:05. Dostupné také z www: http://www.ceskatelevize.cz/specialy/hydepark/11.3.2013/ [citováno dne 9. října 2013]

SVOBODA, I. Aktuální kybernetické hrozby a možnosti jejich prevence, detekce a řešení. In: *Konference o kybernetické bezpečnosti, Poslanecká sněmovna Parlamentu České republiky, 16. 5. 2013.* Audiozáznam a prezentace dostupné z www: http://www.viktorpaggio.cz/prezentace-a-audiozaznam-ze-seminare-o-kyberneticke-bezpecnosti-16-kvetna-2013/ [citováno dne 9. října 2013]

The Explanatory Report of the Convention on Cybercrime. Budapešť, Výbor ministrů Rady Evropy, 2001. Dostupné také z www: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm [citováno dne 9. října 2013]

Věcný záměr zákona o kybernetické bezpečnosti. Národní bezpečnostní úřad, 2013. Dostupné také z www: http://www.govcert.cz/cs/legislativa/legislativa/ [citováno dne 9. října 2013]

NÁZEV PRÁCE V ANGLICKÉM JAZYCE

Internet and computer criminality.

ABSTRAKT

Internetová a počítačová kriminalita je součástí kybernetické kriminality, což je značně široká a poměrně nestejnorodá skupina trestných činů. Diplomová práce se zaměřuje na trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů. Tyto kybernetické útoky mohou ohrozit kybernetickou bezpečnost na úrovni státu a způsobit nedozírné škody. V současné době je v České republice připravován zákon o kybernetické bezpečnosti, jehož cílem je reagovat na tyto útoky. Diplomová práce zkoumá zejména trestněprávní aspekty tohoto zákona. Velký prostor je v práci dále věnován nedávno ratifikované Úmluvě o počítačové kriminalitě.

Kromě zmíněných dvou právních norem diplomová práce vychází z právních předpisů a rozhodovací praxe české i zahraniční, k čemuž využívá odborné literatury dostupné v českém, anglickém či německém jazyce. S ohledem na zvolené téma bylo nutné využít též značné množství neprávní literatury.

Celá práce je rozdělena do šesti kapitol. První kapitola předkládá krátký úvod do tématu a též stručné vysvětlení základních pojmů. Kapitola druhá klade otázky ohledně oprávněnosti a užitečnosti státní regulace v kyberprostoru, které jsou částečně filosofické povahy. Tato část též popisuje specifika v kyberprostoru, která je třeba vzít v úvahu při posuzování kybernetické kriminality, stejně jako před prováděním zákonné regulace kyberprostoru. Třetí kapitola se zaměřuje na způsoby provedení trestných činů v kyberprostoru. Čtvrtá kapitola shrnuje zásadní evropské a mezinárodní právní instrumenty pro boj s útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů. Kapitola pátá se zabývá trestnými činy relevantními k tomuto tématu v českém trestním zákoníku. Závěrečná kapitola zhodnocuje trestněprávní důsledky vyplývajícími z budoucího zákona o kybernetické bezpečnosti.

ABSTRACT

The internet and computer criminality is a part of a cybercrime which is a very wide and relatively inhomogeneous category of criminal offences. The master's thesis focuses on criminal offences against confidentiality, integrity and availability of computer data and computer systems. These cyber attacks can endanger the cyber security at the national level and inflict immeasurable damage. In the present day, a Cybersecurity Act is being prepared in the Czech Republic whose goal is to respond to these attacks. Master's thesis examines especially penal aspects of this law. Moreover, a large space in the thesis is devoted to the recently ratified Convention on Cybercrime.

Besides the two above-mentioned legal norms the master's thesis arises from the Czech and foreign legal regulation and case law, for which it uses literature available in the Czech, English or German language. With regard to the chosen topic, it has been necessary to use also considerable amount of a non-legal literature.

The whole work is divided into six chapters. The first chapter provides a brief introduction into the topic and also short explanations of the basic terms. Chapter two provides questions about legitimacy and beneficial effect of a state regulation in the cyberspace which are of a partially philosophical character. This section also describes specifics in the cyberspace which should be taken into account while judging the cybercrime and before every legal regulation of the cyberspace as well. Chapter three focuses on *modus operandi* of the criminal offences committed in the cyberspace. Chapter four summarizes fundamental European and international legal instruments for fighting the attacks against confidentiality, integrity and availability of computer data and computer systems. Chapter five deals with the criminal offences in the Czech Criminal Code which are relevant to the topic. The last chapter evaluates the penal consequences which are arising from the future Cybersecurity Act.

KLÍČOVÁ SLOVA

Kybernetická bezpečnost

Kybernetická kriminalita

KEYWORDS

Cybersecurity

Cybercrime