Kybernetická kriminalita

1 Úvod

Vývoj v oblasti výpočetní techniky je rok od roku rychlejší. V roce 2016 mělo více než 46 % světové populace přístup k internetu.[1] Každá nová technologie však s sebou přináší i rizika. V kybernetickém prostoru se jedná především o rizika bezpečnostní, zejména zneužití informačních systémů a útoky na ně. Trestná činnost v kybernetickém prostoru je nejvýnosnějším a nejrychleji se rozvíjejícím odvětvím kriminality. Důvody, proč tomu tak je, jsou zmíněny v kapitole 3.

Obecně lze říci, že nejvíce kybernetických zločinů pochází z rozvojových států.[2] Vždy však nelze jednoznačně určit, jestli útok ve skutečnosti nemá původ jinde a přes danou zemi neprochází proto, aby bylo obtížnější pachatele vysledovat. Některé z těchto zemí totiž nemají žádné zákony, které by kybernetickou kriminalitu upravovaly, případně dochází k distančnímu deliktu, pokud se cíl útoku nachází na území jiného státu. V takových případech často zůstávají pachatelé bez trestu.[3] Prioritou by tedy mělo být globální zajištění trestní odpovědnosti v oblasti kyberkriminality.

Obětí kybernetického útoku se může stát kdokoliv od jednotlivců po vlády. Může se jednat o krádež identity, ale i o koordinovaný útok s cílem poškodit nepřítele.

Hned v úvodu je nutné říct, že pro pojmy jako kyberprostor či kybernetický zločin neexistuje jednotná definice, což je jednou ze zásadních komplikací v boji s tímto typem kriminality.[4]

2 Kyberprostor

Přes značné rozpory se lze shodnout alespoň na základní definici kybernetického prostoru (angl. cyberspace). Encyklopedie Britannica vysvětluje kyberprostor jako "virtuální svět tvořený propojením počítačů, zařízení s přístupem k internetu, serverů, routerů a jiných komponentů internetové infrastruktury".[5] I když se tedy může zdát, že kyberprostor a internet jsou totožné pojmy, není tomu tak. Zatímco internet je globální sítí tvořenou fyzickými servery, kyberprostor je spíše symbolickým vyjádřením onoho nehmotného světa, který kromě internetu zahrnuje i místní sítě (LAN) či systémy, které jsou z bezpečnostních důvodů záměrně izolovány od veřejně přístupných sítí. Navíc se pojem kyberprostor užíval již v dobách Arpanetu (1969), což byla síť převážně vojenského charakteru a předchůdce dnešního internetu.[6]

3 Kybernetické zločiny

Obdobně jako u kyberprostoru neexistuje ani pro kybernetickou kriminalitu jednotná definice. S tím souvisí i nenalezení shody na tom, jaké aktivity jsou nezákonné či by měly být za nezákonné považovány. Obecnější definici můžeme získat z takzvané triády CIA.[7] Ta vymezuje jako kybernetické zločiny takové aktivity, které narušují dostupnost, integritu nebo důvěrnost počítačových sítí a dat na nich uložených. Z mezinárodních dokumentů poskytuje dělení kybernetických zločinů například Úmluva o kyberkriminalitě, která byla přijata Radou Evropy v roce 2004.[8] Ta byla do roku 2017 ratifikována 55 státy. I nadále zůstává Ruská federace jediným členem Rady Evropy, jenž tento dokument nepodepsal. Mezi nečleny, kteří odmítli Úmluvu podepsat, patří Ghana, Maroko, Mexiko, Nigérie, Argentina, Kolumbie, Peru, či Filipíny.[9] Dělení z Úmluvy o kyberkriminalitě je následující:

1. Trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů	1.1. Nezákonný přístup
	1.2. Nezákonný odposlech
	1.3. Zasahování do dat
	1.4. Zasahování do systému
	1.5. Zneužívání zařízení
2. Trestné činy související s počítačem	2.1. Počítačové padělání
	2.2. Počítačový podvod
3. Trestné činy související s obsahem	3.1. Trestné činy související s dětskou pornografií
4. Trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským	

Mezi nejčastější případy zneužití informačních technologií patří napadení e-mailové schránky, krádež identity a podvody s kreditními kartami.[10] V českém prostředí lze v tomto kontextu zmínit hackerský útok na systém Ministerstva zahraničních věcí ČR nebo mediálně známou kauzu napadení e-mailového účtu premiéra Bohuslava Sobotky.[11],[12] Tyto a další činnosti jsou mnohem častějšími formami kriminality než například krádež, loupež či odcizení auta.[13] Největší zásluhu na tom mají vlastnosti kyberprostoru jako takového. V první řadě se jedná o dostupnost internetu a možnost připojit se k němu téměř odkudkoliv. Dále je to anonymita, která je však jen málokdy absolutní (např. skrytí IP adresy skrze tzv. software s cibulovým směrováním[14]). Ta velkou mírou znesnadňuje sběr důkazů a snižuje šanci na postih pachatele.

4 Právní úprava

S příchodem nových technologií se objevily i nové otázky a rozpory týkající se kybernetického prostoru. V dobách vzniku internetu se o regulacích příliš nehovořilo. Prvními uživateli byli univerzitní profesoři a vědečtí pracovníci. Se stále se rozšiřující základnou uživatelů, která postupně pronikala i do soukromé sféry, však přestala vyhovovat dosavadní autoregulace, jelikož se ve velkém množství začaly objevovat zločiny v kyberprostoru.[15] Autoritou, která internet dodnes reguluje, je každý jednotlivý stát. Ten ale může zasahovat jen do té části internetu, která se nachází v jeho kompetenci. Zde vznikají komplikace, neboť každý stát reguluje internet jiným způsobem, který nemusí být kompatibilní s jinými státy, a některé státy internet neregulují vůbec. Příkladem takové neregulace je svoboda slova ve Spojených státech, kterou garantuje první dodatek v Ústavě.[16] V roce 2002 uplatnil Nejvyšší soud USA tento dodatek v kauze American Civil Liberties Union vs. Ashcroft. Verdikt zněl, že jakákoliv omezení internetu ze strany státu by byla protiústavní.[17]

Jinak tomu je v Ruské federaci, kde byl v roce 2014 schválen zákon, díky kterému může vláda bez udání důvodu blokovat libovolnou webovou stránku. Tento a další zákony jsou nejčastěji obhajovány jako prostředky tzv. informační bezpečnosti.

4.1 Mezinárodní právo

Trestnou činností v kyberprostoru se na mezinárodní úrovni zabývá mnoho organizací. Mezi ně patří Evropská unie (EU), výše zmíněná Rada Evropy a samozřejmě i Organizace spojených národů (OSN). Mimo Úřad OSN pro drogy a kriminalitu (UNODC) se stejnou agendou zabývá i Výbor pro odzbrojení a mezinárodní bezpečnost Valného shromáždění OSN (DISEC), Ekonomická a sociální rada OSN (ECOSOC) a samozřejmě Valné shromáždění OSN.

V roce 2000 schválilo Valné shromáždění OSN rezoluci, jejímž cílem byl boj se zneužíváním informačních technologií. Státy v ní žádá, aby svými zákony

umožňovaly jednodušší přístup k informacím v rámci kriminálních vyšetřování. V jednom z dalších bodů Valné shromáždění volá po snadnější identifikaci síťových zařízení, která by vedla opět k usnadnění kriminalistické činnosti.[18]

Prvním dokumentem Komise pro prevenci kriminality a trestnou činnost (CCPCJ), jež se týkala kybernetické kriminality, byla rezoluce 20/7 (2011).[19] V ní Komise vyzvala UNODC a členské státy ke kooperaci s poskytovateli internetových služeb a mezinárodními organizacemi. Jednou z takových organizací je například Interpol, který kromě analytické činnosti zprostředkovává spolupráci investigativních složek v různých státech.

4.2 Národní právo

Z celého světa má 139 států kybernetickou bezpečnost zákonem alespoň částečně ukotvenou.[20] Nejčastěji se jedná o samostatné zákony o kyberkriminalitě v trestním právu. V případech spojených s ochranou osobnosti se nachází i v právu občanském. Některé z těchto zákonů jsou opatřeny vlastní definicí kybernetického zločinu. Oproti tomu nemá 37 států ani návrh zákona, který by se trestné činnosti v kyberprostoru týkal. Mezi tyto státy patří kupříkladu Afghánistán, Čad, Demokratická republika Kongo, Libanon, Libye, Guinea, Mongolsko, Somálsko a Papua-Nová Guinea.[21]

5 Comprehensive Study on Cybercrime

Valné shromáždění OSN pověřilo v rezoluci 65/230 (2010) CCPCJ sestavením otevřené mezivládní skupiny expertů, která by provedla detailní studii v oblasti kybernetické kriminality.[22] Dokument se měl zabývat především dosavadními právními postupy v oblasti kybernetické kriminality na národní i mezinárodní úrovni a měl obsahovat možná řešení a budoucí postupy. Skupina expertů poprvé zasedala v lednu 2011 ve Vídni a dohodla se na odborných metodách, jakými danou studii provede. Ve své rezoluci 67/189 (2012) ocenilo Valné shromáždění OSN pokrok skupiny v její práci.[23] V roce 2013 skupina expertů zveřejnila návrh studie, jejímž obsahem je i shrnutí možných řešení, jak dále postupovat v boji s kyberkriminalitou. Mezi taková řešení patří vytvoření modelového zákona o kyberkriminalitě a modelových multilaterálních smluv o sdílení dat pro potřeby kriminalistické činnosti.[24] Podstatná část studie vznikla na základě dotazníku, který sestavila skupina expertů a na který odpověděly mnohé mezinárodní organizace, akademické instituce a 69 členských států OSN. Mezi nimi byli zástupci USA, Ruska, Číny, Brazílie, Saúdské Arábie a podstatné části Evropské unie. Chyběly však odpovědi většiny afrických států, Indie, Izraele, Itálie, Turecka nebo Švédska.[25]

5.1 Návrhy na změny

V úvodu studie lze najít souhrn možností nových opatření a posílení opatření stávajících. Mezi ně patří vytvoření modelového zákona o kyberkriminalitě, který by sloužil jako vzor pro státy, které dosud takovými zákony nedisponují. Modelovými zákony o kyberkriminalitě se zabývala i Rada Evropy a ve své studii pod názvem "Cybercrime Model Laws" provedla rozbor některých existujících modelových legislativ. Dospěla však k názoru, že současné modelové zákony jsou spíše ke škodě a jejich implementace může negativně ovlivnit mezinárodní spolupráci.[26] Dalším návrhem je vývoj multilaterálního nástroje se zaměřením na sběr elektronických důkazů o trestné činnosti, který by fungoval na principu mezinárodní spolupráce.

6 Závěr

V otázce kybernetického zločinu existuje mnoho různých přístupů a řešení. Cílem CCPCJ by mělo být vytvoření dokumentu, který posílí boj s tímto druhem zločinu na mezinárodní úrovni. Může se jednat o vypracování univerzálního návrhu legislativy pro jednotlivé státy, či o přijetí rezoluce, jež by zvýšila tlak na státy, které dosud opatření proti kybernetickým zločinům nezavedly.

Otázky pro stanovisko

- Platí ve vašem státě zákony týkající se kybernetické kriminality?
- Jakým způsobem řeší váš stát tzv. informační bezpečnost?
- Jak je váš stát nakloněn mezinárodní spolupráci ve věci kybernetické kriminality?
- Měl by vzniknout vzorový návrh zákona o kyberkriminalitě? Pokud ano, co vše by měl obsahovat?

Otázky pro jednání

- Měl by být vyvíjen tlak na státy, které nemají zákonem ukotvenou kybernetickou kriminalitu?
- Jakým způsobem reagoval váš stát na Úmluvu o kyberkriminalitě?
- Jaká jsou rizika modelových zákonů o kyberkriminalitě?
- Jak souvisí kybernetická kriminalita s cenzurou internetu?
- Jaké jsou rozdíly mezi informační a kybernetickou bezpečností?
- Kde leží hranice mezi bezpečností a zásahem do soukromí obyvatel?

Seznam doporučených a rozšiřujících zdrojů

Copmrehensive Study on Cybercrime:
https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf
Návrh studie shrnující podstatné informace z oblasti kybernetické kriminality.

Cybercrime Model Laws: https://rm.coe.int/1680303ee1
Studie Rady Evropy obsahující rozbory dosavadních modelových zákonů o kyberkriminalitě.

Cybercrime Repository: https://www.unodc.org/cld/v3/cybrepo/
Přehled zákonů jednotlivých států, které se zaobírají kybernetickou bezpečností.

Where Cybercrime Goes to Hide:
https://www.youtube.com/watch?v=CashAq5RToM
Krátký investigativní dokument o datových centrech a problému nedotknutelnosti některých kybernetických zločinců.

The unlikely history of Tor: https://www.expressvpn.com/internet-privacy/tor/history/
Článek shrnující historii webového prohlížeče Tor (The Onion Routing

1 Number of Internet Users (2016). Internet Live Stats [online]. 2016 [cit. 2017-08-15]. Dostupné z: http://www.internetlivestats.com/internet-users/

2 Pro tento dokument je za rozvojový stát stejně jako v Comprehensive Study on Cybercrime považován takový, který má index lidského rozvoje (HDI) nižší než 0,8.

3 MALBY, Steven, Mace ROBIN, Anika HOLTERHOF, Cameron BROWN, Stefan KASCHERUS a Eva IGNATUSCHTSCHENKO. Comprehensive Study on Cybercrime [online]. 2013 [cit. 2017-07-11]. Dostupné z:

https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

4 Cybercrime: Issues. Parliament of Canada [online]. 2011 [cit. 2017-07-22]. Dostupné z: https://lop.parl.ca/Content/LOP/ResearchPublications/2011-36-e.htm#a2

5 Cybercrime. In: Encyclopedia Britannica [online]. 2013 [cit. 2017-07-11]. Dostupné z: https://www.britannica.com/topic/cyberspace

6 Difference between Cyberspace and Internet. Difference Between | Descriptive Analysis and Comparisons [online]. [cit. 2017-07-22]. Dostupné z: http://www.differencebetween.info/difference-between-cyberspace-and-internet

7 Zde se nejedná o americkou zpravodajskou agenturu. Pro vymezení se často využívá zkratky AIC (Availability-Integrity-Confidentiality)

8 Úmluva o počítačové kriminalitě [online]. 2001 [cit. 2017-07-22]. Dostupné z: https://rm.coe.int/16804931c0

9 Chart of signatures and ratifications of Treaty 185. Council of Europe [online]. 2017 [cit. 2017-08-15]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=tVwM1uVV

10 MALBY, Steven, Mace ROBIN, Anika HOLTERHOF, Cameron BROWN, Stefan KASCHERUS a Eva IGNATUSCHTSCHENKO. Comprehensive Study on Cybercrime [online]. 2013 [cit. 2017-07-11]. Dostupné z:

https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

11 Hackeři úspěšně napadli e-maily ministerstva zahraničí. Dostali se i ke komunikaci samotného ministra. Živě.cz [online]. 2017 [cit. 2017-10-01]. Dostupné z: https://www.zive.cz/bleskovky/hackeri-uspesne-napadli-e-maily-ministerstva-zahranici-dostali-se-i-ke-komunikaci-samotneho-ministra/sc-4-a-185892/default.aspx

12 FEREBAURER, Václav. Hackeři tvrdí, že se nabourali do e-mailové schránky premiéra Sobotky. IDnes [online]. 2016 [cit. 2017-08-20]. Dostupné z: http://zpravy.idnes.cz/hackeri-nabourali-e-mail-premiera-sobotky-fgd-/domaci.aspx?c=A160105_132452_domaci_fer

13 Tamtéž

14 Tor – volně šiřitelný software umožňující anonymní komunikaci na internetu (viz doporučené zdroje).

15 Právo a internet. Wikisofia [online]. 2016 [cit. 2017-08-20]. Dostupné z: https://wikisofia.cz/wiki/Pr%C3%A1vo_a_internet

16 Tento dodatek konkrétně zamezuje Kongresu USA schválení zákona, který by jakkoliv omezoval svobodu vyznání, slova, projevu, tisku, shromažďování a požadování odškodného od státu.

17 Ashcroft v. American Civil Liberties Union 535 U.S. 564 (2002). JUDISTIA: US Supreme Court [online]. [cit. 2017-10-22]. Dostupné z: https://supreme.justia.com/cases/federal/us/535/564/

18 Rezoluce Valného shromáždění OSN A/RES/55/63: Combating the criminal misuse of information technologies [online]. 2000. Dostupné také z: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/55/63

19 Rezoluce Komise pro prevenci kriminality a trestnou činnost 20/7 [online]. 2011. Dostupné také z: https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2011/CCPCJ/Resolution_20-7.pdf

20 Cybercrime Legislation Worldwide. United Nations Conference on Trade and Development [online]. 2017 [cit. 2017-07-22]. Dostupné z: http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

21 Tamtéž

22 Rezoluce Valného shromáždění OSN A/RES/65/230: Twelfth United Nations Congress on Crime Prevention and Criminal Justice [online]. 2010. Dostupné také z: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/65/230

23 Rezoluce Valného shromáždění OSN A/RES/67/189: Strengthening the United Nations crime prevention and criminal justice programme, in particular its technical cooperation capacity. 2012. Dostupné také z: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/67/189

24 MALBY, Steven, Mace ROBIN, Anika HOLTERHOF, Cameron BROWN, Stefan KASCHERUS a Eva IGNATUSCHTSCHENKO. Comprehensive Study on Cybercrime [online]. 2013 [cit. 2017-07-11]. Dostupné z: https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

25 Tamtéž

26 Cybercrime model laws. Council of Europe [online]. 2014 [cit. 2017-07-23]. Dostupné z: https://rm.coe.int/1680303ee1

Pražský studentský summit

Pražský studentský summit je unikátní vzdělávací projekt existující od roku 1995. Každoročně vzdělává přes 300 studentů středních i vysokých škol o současných globálních tématech, a to především prostřednictvím simulace jednání čtyř klíčových mezinárodních organizací – OSN, NATO, EU a OBSE.

www.studentsummit.cz
summit@amo.cz
www.instagram.com/praguestsudentsummit
www.facebook.com/studentsummit
www.twitter.com/studentsummit
www.youtube.com/studentsummitcz

Asociace pro mezinárodní otázky (AMO)

AMO je nevládní nezisková organizace založená v roce 1997 za účelem výzkumu a vzdělávání v oblasti mezinárodních vztahů. Tento přední český zahraničně politický think-tank není spjat s žádnou politickou stranou ani ideologií. Svou činností podporuje aktivní přístup k zahraniční politice, poskytuje nestrannou analýzu mezinárodního dění a otevírá prostor k fundované diskusi.

+420 224 813 460
www.amo.cz
info@amo.cz
Žitná 608/27, 110 00 Praha 1
www.facebook.com/AMO.cz
www.twitter.com/amo_cz
www.linkedin.com/company/amocz
www.youtube.com/AMOcz

Jan Doležal

Jan Doležal je spolupracovníkem Asociace pro mezinárodní otázky a členem přípravného týmu Pražského studentského summitu.

Background report je materiál pro žáky středních škol účastnících se Pražského studentského summitu. Všichni partneři projektu jsou uvedeni zde.

The Kellner Family Foundation

Generální partner
Pražského studentského summitu

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Ministerstvo zahraničních věcí České republiky

PRAHA PRAGUE PRAGA

KB

Evropská komise
Zastoupení v České republice

METROPOLITNÍ UNIVERZITA PRAHA

US embassy

TOP
partneři

PRAHA 3

SCIO

Velvyslanectví Spolkové republiky Německo v České republice

Embassy of Canada
Ambassade du Canada

AUTO_ZRUCKY

OSCE

Městská část Praha 6

Partneři

HOSPODÁŘSKÉ NOVINY

RESPEKT

Mediální
partneři

VŠE

interhotel AMBASSADOR ZLATÁ HUSA

KONGRESOVÉ CENTRUM PRAHA

United Nations
Information Centre Prague
Informační centrum OSN v Praze

Microsoft

Za
podpory