UNIVERSITA KARLOVA V PRAZE

PRÁVNICKÁ FAKULTA

Eliška Nováčková

Evropská právní úprava kyberzločinů s porovnáním právní úpravy kyberzločinů ve Spojených státech amerických

Diplomová práce

Vedoucí diplomové práce: JUDr. Ing. Jiří Zemánek, CSc.

Katedra evropského práva

Datum uzavření rukopisu 20. 3. 2015

Čestné prohlášení

Prohlašuji, že předloženou diplomovou práci jsem vypracovala samostatně a že všechny použité zdroje byly řádně uvedeny. Dále prohlašuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne 25. 3. 2015

……

Eliška Nováčková

Poděkování

Děkuji JUDr. Ing. Jiřímu Zemánkovi, CSc., za podporu a podnětné připomínky při zpracování diplomové práce.

Obsah

1. Úvod

Trestná činnost realizovaná prostřednictvím informačních sítí, která nabývá v dnešní době mnoha různých podob, představuje závažný problém. Z důvodu nárůstu trestných činů souvisejících kromě jiného s neoprávněným zachycením informací, s dětskou pornografií či s porušením autorského práva se jeví jako přirozený důsledek podrobnější zaměření právní normotvorby na tuto oblast, kterou charakterizuje rychlý vývoj. Rychlost se tedy musí následně promítat i do tvorby právních norem. Závažná je i otázka možností vynucování postihu porušení těchto norem spojená s problematikou ukládání trestu zákazu přístupu k internetu či zákazu užívání počítače.[1] V souvislosti s rozšiřujícími se kybernetickými hrozbami roste také potřeba prevence a je nutné zajistit dostatečné povědomí o souvisejících rizicích pro všechny uživatele kybernetického prostoru.

Závažnost trestné činnosti v kyberprostoru lze spatřovat jak v kvalitativním, tak v kvantitativním narušení informační společnosti. Z hlediska kvantitativního se může jednat například o otázku úrovně datové základny, v kvalitativním měřítku lze pozorovat závažnost například v zásazích do individuálních subjektivních práv.[2]

Kyberkriminalita má vzhledem k povaze svého prostředí podstatný přeshraniční rozměr, a proto si klade tato práce za cíl porovnání programových dokumentů a právní úpravy kyberzločinů v Evropské unii (dále „Unie“) s regulací ve Spojených státech amerických (dále „USA“). Po prvotním vymezení klíčových pojmů následuje stručný popis vývoje právní úpravy USA související s bezpečností kybernetického prostoru a uvedení dvou základních strategií dané oblasti, Národní strategie ochrany kyberprostoru a Mezinárodní strategie pro kyberprostor. Poté je přiblížen rámec primárního i sekundárního práva Unie v oblasti trestního práva kyberprostoru a uveden stručný rozbor Úmluvy o počítačové kriminalitě (dále „Úmluva“). Mimo jiné jsou nastíněny i některé otázky související s ochranou osobních údajů či problematiky spolupráce

[1] HABIB, Jessica. Cyber Crime and Punishment: Filtering Out Internet Felons. *Fordham Intellectual Property, Media and Entertainment Law Journa*. 2004, Volume XIV, Book 4, s. 14. Dostupné z: http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1290&context=iplj.

[2] *Kyberkriminalita a právo*. Vyd. 1. Editor Tomáš Gřivna, Radim Polčák. Praha: Auditorium, 2008, s. 24 - 25. ISBN 978-809-0378-674.

veřejného a soukromého sektoru směřující k vyšší úrovni bezpečnosti kybernetického prostoru.

Následuje komparace výše uvedených programových a právních dokumentů i odpovídajících současných politik USA a Unie, které se bezpochyby významnou měrou ovlivňují a determinují také další postup jednotlivých částí světa k zajištění bezpečného kyberprostoru. Předně se jedná o komparaci strategických dokumentů a dále porovnání se současnou podobou Úmluvy. Následně jsou rovněž porovnány vybrané právní předpisy USA a Unie, které směřování politiky k zajištění kybernetické bezpečnosti podrobněji rozvádějí. V závěru práce jsou popsány hlavní body spolupráce USA a Unie v oblasti kybernetického prostoru, včetně společných přijatých právních dokumentů i společně organizovaných akcí, jakou bylo například cvičení Cyber Atlantic 2011. Práci uzavírá shrnutí přijatých dokumentů v USA a Unie v rámci problematiky kyberzločinů, jejich shodné a rozdílné znaky a zhodnocení současné podoby spolupráce. Cílem práce je uvést přehledný souhrn strategických dokumentů v prostoru kybernetické bezpečnosti USA a Unie, vybraných navazujících právních předpisů a zhodnotit je ve světle legislativního i technologického postupu a zmapovat hlavní kroky transatlantické spolupráce v boji proti kyberzločinům.

2. Informační systém a kyberzločiny

2.1. Pojem informace

Dnešní společnost definuje sama sebe jako informační společnost. Informace se stala klíčovým pojmem, neboť všechno vědění vychází z informací, které produkujeme a hromadíme. Lidé nemohou bez informací žít a jsou sami sobě informačními systémy.[3] Informaci lze uchopit mnoha způsoby, lze ji interpretovat jako znalost, jako věc nebo jako proces.[4] Je tedy obtížné definovat její obsah co nejpřesněji, a lze tak čerpat z mnoha různých definic. Jednu z nich uvádí i zakladatel kybernetiky Norbert Wiener, když informaci označuje za obsah toho, co se vyměňuje s vnějším světem, když se mu přizpůsobujeme, a tímto přizpůsobováním na něj působíme.[5] Účelem informací je pak organizování elementů do systematických celků.[6] K následnému sběru, uchování a zpracování informací slouží informační systémy, které jsou tvořeny dvěma složkami. Těmito složkami jsou ektosystém, tvořený uživateli, investorem a tím, kdo systém provozuje, a endosystém, který se skládá z použitého hardware a software.[7] Informační systémy se mezi sebou značně odlišují v závislosti na zdroji informace.

2.2. Pojem kyberprostoru

Potřeba ochrany kyberprostoru je v dnešní době jednou ze samozřejmých priorit všech vyspělých států světa. Strategické dokumenty zpravidla již ve svém názvu odkazují k tomuto pojmu, proto je potřebné pojem i pro účely této práce vymezit. Pojmy kyberprostor a kybernetický prostor se v dnešní době používají synonymně, stejně tak

[3] BURGIN, Mark. *Theory of information: fundamentality, diversity and unification*. Hackensack, N.J.: World Scientific, 2010, xvi, s. 1. ISBN 9789812835499.
[4] BUCKLAND, Michael Keeble. *Information and information systems: fundamentality, diversity and unification*. New York: Praeger, 1991, xv, s. 43. World Scientific series in information studies. ISBN 02-759-3851-4.
[5] BURGIN, Mark. *Theory of information: fundamentality, diversity and unification*. Hackensack, N.J.: World Scientific, 2010, xvi, s. 3. ISBN 9789812835499.
[6] *Kyberkriminalita a právo*. Vyd. 1. Editor Tomáš Gřivna, Radim Polčák. Praha: Auditorium, 2008, s. 12. ISBN 978-809-0378-674.
[7] HRONEK, Jiří. *Informační systémy* [online]. Olomouc, 2007 [cit. 2015-01-24]. Dostupné z: http://phoenix.inf.upol.cz/esf/ucebni/infoSys.pdf. Učební text. Univerzita Palackého.

tomu bude v této práci. Definování kyberprostoru se opírá o tři základní složky. První z nich je virtuální povaha kyberprostoru, tedy absence požadavku současné přítomnosti zúčastněných osob na jednom místě. Druhou složkou je vztah mezi kyberprostorem a sítí, neboť kyberprostor vzniká na základě propojení počítačových sítí. Třetí složka je označována jako interakce, umožnění vzájemného působení podnětů a následných reakcí.[8]

První složka je bezesporu klíčová, neboť absence územních hranic způsobuje přetrhávání pouta mezi zeměpisným umístěním a uplatňováním moci orgánů místní správy v rámci kontroly online chování, vyvolává otázku legitimity právní úpravy územně vymezených suverénů regulovat tuto globální problematiku a mění význam pojmu poloha. Reálná poloha subjektů je totiž zcela druhořadá, významnou se stala poloha ve virtuálním prostoru, skládající se z jednotlivých tzv. adres. Například v případě doménových jmen, kdy je určitému přístroji přiřazena adresa IP (Internet Protocol), která se shoduje se skutečným umístěním přístroje, přístroj může být přemístěn bez vlivu na doménové jméno. Případně vlastník doménového jména může požádat o přeřazení tohoto jména ke zcela odlišnému přístroji, který se fyzicky nachází na odlišném místě. Tudíž například server označený jako „*.uk*“ nemusí být umístěn ve Spojeném království Velké Británie a Severního Irska.[9]

Definice uváděné v právních dokumentech bývají v tomto ohledu spíše strohé. Příkladem může být Národní strategie ochrany kyberprostoru Spojených států amerických z roku 2003 [10], která vymezuje kyberprostor jako provázanou síť infrastruktur informační technologie. V celé řadě případů se ovšem pojem využívá bez jeho předchozí definice, jako je tomu například u Strategie Evropské unie v oblasti

[8] PLOUG, Thomas. *Ethics in cyberspace how cyberspace may influence interpersonal interaction*. Dordrecht: Springer, 2009, s.69-71. ISBN 978-904-8123-704.

[9] Johnson, David R. and Post, David G., Law and Borders - The Rise of Law in Cyberspace. Stanford Law Review, Vol. 48, 1996, s. 1370-1371. Dostupné z SSRN: http://ssrn.com/abstract=535 nebo http://dx.doi.org/10.2139/ssrn.535.

[10] United States Computer Emergency Readiness Team. *The National Strategy to Secure Cyberspace* [online]. 2003 [cit. 2014-03-16]. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

kybernetické bezpečnosti, anebo se pojem nevyužívá vůbec (příkladem může být současná Strategie pro oblast kybernetické bezpečnosti České republiky).[11]

2.3. Kybernetické hrozby

Nejen při tvorbě legislativních či jiných právních podkladů, které se vztahují k ochraně kybernetického prostoru, ale také například při zjišťování slabých článků počítačových softwarů je nutné vycházet z analýzy rizika a identifikovat možné kybernetické hrozby. Informační systémy, které dnešní společnost neustále využívá, slouží zejména ke zpřístupňování informací pro oprávněné subjekty a jejich úkolem je zajistit bezpečnost chráněných dat a jejich integritu. Proti těmto funkcím informačních systémů jsou vedeny útoky, které mohou mít značný destruktivní dopad. Samotná hrozba představuje možnost změny informace či chování systému, uskutečněním hrozby je pak útok. Jirovský[12] rozčleňuje hrozby podle některých základních rysů do tří skupin. Jedná se o hrozby základní (například únik informace), hrozby aktivační (příkladem může být trojský kůň) a hrozby podkladové, které slouží jako podklad pro uskutečnění základních hrozeb (například tajný odposlech).

Informační a komunikační technologie jsou v současnosti jednou z klíčových komponentů fungování celosvětového hospodářství. Zvyšuje se tím však také závislost na využívání tohoto systému a tedy i realizace hrozeb prostřednictvím kybernetických útoků. Důvody těchto útoků mohou být různé, častý je kriminální, ekonomický či teroristický motiv.[13]

[11] Národní centrum kybernetické bezpečnosti. *Strategie pro oblast kybernetické bezpečnosti ČR a období 2012-2015* [online]. 2003 [cit. 2014-03-16]. Dostupné z: http://www.govcert.cz/cs/legislativa/dalsi-dokumenty/.

[12] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007. Hacking, s. 20-22. ISBN 978-802-4715-612.

[13] Národní centrum kybernetické bezpečnosti. *Strategie pro oblast kybernetické bezpečnosti ČR a období 2012-2015* [online]. 2003 [cit. 2014-03-16]. Dostupné z: http://www.govcert.cz/cs/legislativa/dalsi-dokumenty/.

2.4. Pojem kyberzločin

Pojem kyberzločin zahrnuje protiprávní jednání, kterých se lidé dopouštějí ve virtuálním prostoru. Termín měl zejména symbolizovat online nebezpečí a rizika a užíval se spíše nežli v právním pojmosloví v oblasti sociologie a přilehlých společenskovědních oborech. Kyberzločiny jsou však dnes chápány jako trestná či škodlivá jednání, která spočívají v získávání informací nebo v manipulaci s nimi za účelem dosažení zisku a která jsou uskutečňována prostřednictvím síťových technologií.[14]

Obsah pojmu je v teoretické rovině rozebírán z několika úhlů. V legislativní rovině se hovoří o stanovení hranic přijatelného chování, zatímco v akademické debatě se určují základní poznatky mimo jiné z kriminologie, sociologie, informačního managementu či ekonomiky. Dále je to sféra odborná, která studuje počítačovou trestnou činnost a její jednotlivé prvky, a oblast laická, která umožňuje širší studium aktuálních problémů.[15] Právní úprava kyberzločinů, která musí být přesná, aktuální a dostatečně obšírná, se v každém státě liší. Identifikace odlišností a vývoje této právní úpravy ve Spojených státech amerických a v Evropské unii je nastíněna v této práci.

[14] WALL, David S. *Cybercrime: the transformation of crime in the information age*. Reprint. Cambridge: Polity, s. 10. ISBN 978-074-5627-359.
[15] WALL, David S. *Cybercrime: the transformation of crime in the information age*. Reprint. Cambridge: Polity, s. 12-13. ISBN 978-074-5627-359.

3. Právní úprava Spojených států amerických

3.1. Počátky regulace počítačové kriminality

Jednou z prvních zemí, která přijala zákon vztahující se k počítačovým trestným činům, byly Spojené státy americké. Již od roku 1872 byl definován jako federální zločin podvod využívající pošty nebo telegrafní sítě.[16] Tímto zákonem tak bylo zakázáno podvodné jednání využívající komunikační sítě v národním či mezinárodním obchodu. Zákon je stále účinný a lze jej aplikovat i na některé případy počítačové trestné činnosti. V takovém případě musejí být splněny dvě podmínky. Předně musí být prokázán úmysl podvodu ve vztahu k penězům či majetku a dále musí být trestný čin spáchán za současného užití národní či mezinárodní sítě.[17] Tento zákon ovšem nebyl vytvořen s ohledem na postih kyberkriminality a i když jeho aplikace byla vztáhnuta i na počítačovou síť, zdaleka nemohl postihnout veškerou problematiku. Proto v roce 1986 americký Kongres schválil návrh zákona o počítačových podvodech a zneužívajícím jednání (dále „CFAA“).[18]

CFAA je jedním z nejdůležitějších zákonů vztahujících se k počítačové kriminalitě. Téměř každý další přijatý zákon v této oblasti jej totiž novelizuje. Trestným se stalo jednání vědomého přístupu k počítači bez oprávnění, získávání neoprávněných informací s podvodným úmyslem a způsobení škody chráněnému počítači. Klíčovým kritériem pro možné odsouzení se stal požadavek takového jednání *bez oprávnění*. Zákon ukládal za taková jednání možný trest až ve výši pěti let odnětí svobody a pro recidivisty byla hranice navýšena dvojnásobně. Zákon ovšem nebylo možné aplikovat na případy jednání osob, které oprávněním k přístupu k počítači disponovaly. Stejně tak tento zákon nestanovil jako trestné takové jednání, kterým se osoba dopustila neoprávněného přístupu, avšak pouze z důvodu využití počítače jako takového. Pouhé seznámení se s daty v počítači tak nebylo podle CFAA trestné. Tento federální zákon

[16] *Wire Fraud Statute*
[17] MAY, Maxim. Federal Computer Crime Laws. *SANS Institute* [online]. 2004, s. 2-4 [cit. 2015-01-24]. Dostupné z: http://www.sans.org/reading-room/whitepapers/legal/federal-computer-crime-laws-1446?show=federal-computer-crime-laws-1446&cat=legal.
[18] *The Computer Fraud and Abuse Act (CFAA)*

byl následně mnohokrát novelizován a dodnes je základním zdrojem právní úpravy i na úrovni jednotlivých amerických států.[19]

Významná novelizace CFAA proběhla v roce 1994, kdy se stal trestným přenos programu, informace, kódu či příkazu do počítače či počítačového systému s úmyslem způsobit škodu počítači, informaci v počítači nebo zabránit užití systému. Za trestné bylo rovněž považováno jednání s hrubou nedbalostí vedoucí k závažným a neospravedlnitelným rizikům škody nebo újmy. V roce 1996 byl přijat zákon o národní informační infrastruktuře[20], který umožnil i postih neoprávněného přístupu k počítači s pouhým seznámením se s informacemi.

V témže roce byl také schválen zákon na federální úrovni zaměřený na slušné chování na internetu[21]. Podle tohoto zákona nesměly být mladistvým předloženy zjevně nepřístojné popisy či zobrazení sexuálních nebo vyměšovacích aktivit nebo orgánů. Pro určení pojmu zjevně nepřístojný se předpokládalo užití současných mravních kritérií. Nejvyšší soud však o rok později tento zákon částečně zrušil s odůvodněním, že se jedná o zásah do ústavně chráněného práva na svobodu projevu. Část zákona, která zůstala zachována, nadále poskytovala ochranu poskytovatelům internetového připojení před trestním stíháním, pokud byl trestný obsah poslán prostřednictvím jejich systémů.[22]

Ochrana soukromí elektronické komunikace byla zajištěna přijetím federálního zákona v roce 1986[23]. Trestným se tak stalo zachycení uložených či přenášených elektronických sdělení bez příslušného oprávnění. Zákon také zajistil možnost vládním subjektům požadovat po poskytovatelích internetového připojení sdělovat tento obsah, avšak pouze s dodržením řádného zákonného procesu a se soudním povolením. Zákon byl významně novelizován v roce 1994, kdy byla poskytovatelům internetového

[19] ROSS, Jeffrey Ian. *Cybercrime*. New York: Chelsea House, 2010, s. 97. ISBN 978-143-8117-980.
[20] *The National Information Infrastructure Act (NIIA)*
[21] *The Communications Decency Act (CDA)*
[22] ROSS, Jeffrey Ian. *Cybercrime*. New York: Chelsea House, 2010, s. 97. ISBN 978-143-8117-980.
[23] *The Electronic Communications Privacy Act (ECPA)*

připojení uložena povinnost technicky zajistit možnost elektronického sledování jednotlivců. Nutnost zákonného podkladu ovšem zůstala nedotčena.[24]

V roce 2002 byly přijaty dva velmi významné zákony. Jednalo se o zákon zajišťující zlepšení bezpečnosti kyberprostoru[25] a zákon určený k zajištění vnitřní bezpečnosti[26]. První ze jmenovaných zákonů mimo jiné zpřísnil tresty stanovené CFAA či umožnil poskytovatelům internetového připojení na základě vlastní úvahy sdělit vládním úřadům osobní údaje svých zákazníků v případě důvodného podezření, že informace se může vztahovat k závažnému trestnému činu.

3.2. Současná právní úprava

CFAA je v současné době znám jako paragraf 1030 18. části Sbírky zákonů USA[27]. Za trestné je označeno sedm druhů počítačových aktivit. Předně je popsán neoprávněný přístup k počítači za účelem získání informace z národní bezpečnosti v úmyslu poškodit USA nebo zajistit prospěch jinému státu. Dále se jedná o neoprávněný přístup k počítači za účelem získání finanční nebo úvěrové informace, neoprávněný přístup k počítači využívanému federální vládou, neoprávněný přístup k chráněnému počítači v úmyslu se obohatit na úkor jiného, úmyslné poškození chráněného počítače, podvodné obchody s počítačovými hesly nebo jinými informacemi umožňující přístup k chráněnému počítači a ohrožování chráněného počítače v úmyslu vynucení poskytnutí peněz nebo jiných hodnot.[28] Chráněným počítačem se podle zákona rozumí počítač využívaný finanční institucí vládou USA nebo počítač využívaný ve vnitřním či mezinárodním obchodu.

V roce 2014 Kongres schválil čtyři zákony související se zlepšením federální ochrany kybernetické bezpečnosti, které následně prezident USA 18. prosince 2014 podepsal.

[24] MAY, Maxim. Federal Computer Crime Laws. *SANS Institute* [online]. 2004, s. 2-4 [cit. 2015-01-24]. Dostupné z: http://www.sans.org/reading-room/whitepapers/legal/federal-computer-crime-laws-1446?show=federal-computer-crime-laws-1446&cat=legal.
[25] *The Cyber Security Enhancement Act (CSEA)*
[26] *The Homeland Security Act (HSA)*
[27] *Title 18 U.S.C Section 1030*
[28] MALMSTRÖM, Cecilia. Next step in the EU - US cooperation on Cyber security and Cybercrime. In:*European Commission* [online]. 2013 [cit. 2015-01-24]. Dostupné z: http://europa.eu/rapid/press-release_SPEECH-13-380_en.htm.

Jedná se o zákon o modernizaci federální informační bezpečnosti[29], zákon o ochraně národní kybernetické bezpečnosti[30], zákon o posílení kybernetické bezpečnosti[31] a zákon o posouzení kybernetické bezpečnosti pracovní síly[32]. První z výše uvedených zákonů posiluje roli Ministerstva vnitřní bezpečnosti, které má pomáhat řediteli Kanceláře řízení a rozpočtu (The Office of Management and Budget) v implementaci informačních a bezpečnostních metod v rámci federálních informačních systémů a zároveň sekretariát ministerstva získává dohled nad implementací závazných operačních směrnic, které také může rozvíjet. Těmito závaznými operačními směrnicemi jsou myšleny pokyny dávané úřadům za účelem ochrany federálních informačních systémů z důvodů známé nebo pravděpodobné bezpečnostní hrozby, zranitelnosti nebo rizika.[33]

Druhý jmenovaný se vztahuje k ochraně kritické infrastruktury. Ministerstvo vnitřní bezpečnosti podle tohoto zákona má zřídit národní centrum, které umožní sdílení informací o kybernetických rizicích, mimořádných událostech, zpracování analýz a zajistí varování federálních i ostatních subjektů. Současně by mělo zamezit zbytečnému duplicitnímu předávání informací a zajistit, že předávané informace jsou poskytovány jen oprávněným subjektům.[34]

Zákon o posílení kybernetické bezpečnosti rozebírá spolupráci mezi soukromým a veřejným sektorem k zajištění kybernetické bezpečnosti (primárně se jedná o úkoly uložené ředitelství Národního institutu standardů a technologie), zaměřuje se na výzkum a vývoj kybernetické bezpečnosti (zákon obsahuje výčet subjektů, které mají každé čtyři roky aktualizovat strategický plán výzkumu a vývoje), rozšiřuje požadavky na vzdělávání a rozvoj znalostí a dovedností pracovníků, přičemž ministerstva by měla

[29] *The Federal Information Security Modenization Act*
[30] *The National Cybersecurity Protection Act*
[31] *The Cybersecurity Enhancement Act*
[32] *The Cybersecurity Workforce Assessment Act*
[33] MEADE, Catlin a Susan CASSIDY. FISMA Updated and Modernized. In: *Covington's Government Contracts* [online]. 2014 [cit. 2015-01-24]. Dostupné z: http://www.insidegovernmentcontracts.com/2014/12/fisma-updated-and-modernized/.
[34] USA. National Cybersecurity Protection Act of 2014. In: *S. 2519 (113th)*. 2014. Dostupné z: https://www.govtrack.us/congress/bills/113/s2519#summary.

podporovat různé podoby soutěží, jednak aby získala ty nejlepší zaměstnance, jednak aby stimulovala vývoj nových technologií a programů.[35]

Posledně jmenovaný se zaměřuje na pracovníky Ministerstva vnitřní bezpečnosti. Předmětem posuzování je připravenost a způsobilost pracovníků tohoto Ministerstva, dále posouzení informací, kteří pracovníci Ministerstva jsou jeho stálými zaměstnanci, kteří nezávislými dodavateli a kteří zaměstnanci jiných federálních úřadů. Dále tento zákon hovoří také o komplexní strategii pracovníků, ve které bude popsán několikafázový plán přijímání nových zaměstnanců, překážky přijetí do pracovního poměru a desetiletý předpoklad požadavků z hlediska kybernetické bezpečnosti na zaměstnance Ministerstva.[36]

Ministerstvo vnitřní bezpečnosti spravuje dva klíčové programy pro ochranu kyberprostoru, Národní systém kybernetické výstrahy [37] a Národní skupinu pro koordinaci kybernetické reakce [38] a také dohlíží na bezpečnostní cvičení Cyber Storm. Ve své strategii pro kybernetickou bezpečnost ministerstvo identifikovalo dva strategické cíle, ochranu kritické informační infrastruktury a posílení kybernetického ekosystému, které se promítají do jednotlivých programů. [39] Problematice se také věnuje Ministerstvo obrany, které ve své strategii z roku 2011 vymezilo pět strategických iniciativ. [40] Jedná se o rozšířené využití kyberprostoru, přijetí nových obranných konceptů, posílení spolupráce s ostatními ministerstvy a soukromým sektorem, upevnění vztahů na mezinárodní úrovni a investování do nových technologií a dostatečně kvalifikovaných pracovních sil. Z pohledu národní bezpečnosti je tak ochrana kyberprostoru především úkolem americké armády.

[35] USA. Cybersecurity Enhancement Act of 2014. In: *S. 1353 (113th)*. 2014. Dostupné z: https://www.govtrack.us/congress/bills/113/s1353#summary.
[36] USA. Cybersecurity Workforce Assessment Act. In: *H.R. 2952 (113th)*. 2014. Dostupné z: https://www.govtrack.us/congress/bills/113/hr2952.
[37] National Cyber Alert System
[38] National Cyber Response Coordination Group
[39] LEVIN, Avner a Daria ILKINA. *International Comparison of Cyber Crime*. Toronto, Canada, 2013. Dostupné z: http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf. Ryerson University.
[40] MINISTERSTVO OBRANY USA. *Department of Defense Strategy for Operating in Cyberspace*. 2011. Dostupné z: http://www.defense.gov/news/d20110714cyber.pdf.

3.3. Národní strategie ochrany kyberprostoru

Národní strategie ochrany kyberprostoru, zveřejněná v únoru 2003, vymezuje tři strategické cíle[41]. Jedná se o předcházení kybernetických útoků proti americké kritické infrastruktuře, zmírnění zranitelnosti země proti těmto útokům a minimalizování škod, které by mohly být způsobeny, společně s následným návratem do původního stavu. Tato strategie zdůraznila možnost poškození amerických informačních sítí útoky ze strany teroristických organizací. Zajišťování bezpečného kyberprostoru je nejen povinností federální vlády a vlád jednotlivých států, ale také soukromého sektoru. Národní strategie ochrany kyberprostoru předpokládá integraci všech lidí, operací a technologií z různých odvětví společnosti a také podporuje dobrovolné činnosti soukromého sektoru směřující k ochraně kyberprostoru. To vše především z důvodu, že bezpečný kyberprostor je důležitý jak pro jednotlivce, tak pro úřady, má přeshraniční povahu a je jedním z předpokladů fungování veřejného i soukromého sektoru.

Strategie vyzdvihuje pět kritických priorit. Předně se jedná o národní systém reakce v oblasti bezpečného kyberprostoru[42], který zahrnuje včasné varování, sdílení informací či krizový management. Hlavní odpovědnost byla za tímto účelem svěřena Ministerstvu vnitřní bezpečnosti, které má na starosti Národní systém pro kybernetickou reakci[43] fungující dvacet čtyři hodin denně sedm dní v týdnu. Jedním z úkolů ministerstva je podporovat rozvoj schopností soukromého sektoru, a přispět tak k bezpečnému kyberprostoru, což se projevuje například ve spolupráci s centry sdílení a analýzy informací [44] z oblastí finančních služeb, telekomunikací, informačních technologií, elektronických zařízení či poskytování různých dodávek zboží a služeb.[45] Ministerstvo dále provádí taktickou a strategickou analýzu možných hrozeb a identifikaci slabých článků počítačových softwarů.

[41] THE WHITE HOUSE, Washington, President Bush. *The National Strategy to Secure Cyberspace*. 2003. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
[42] *National Cyberspace Security Response System*
[43] *National Cyber Response System*
[44] *Information Sharing and Analysis Centers*
[45] THE WHITE HOUSE, Washington, President Bush. *The National Strategy to Secure Cyberspace*. 2003. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

Druhou prioritou je zmírnění hrozeb a zranitelnosti kyberprostoru[46]. V rámci této priority jsou zmíněny tři složky, jejichž postupným implementováním je pověřeno opět Ministerstvo vnitřní bezpečnosti. První složka spočívá ve snižování hrozeb a odstrašování potenciálních pachatelů, druhá část je definována jako identifikace a náprava zranitelných míst a třetí odkazuje na vývoj nových systémů se současnou predikcí jejich zranitelných míst. K dosažení této priority je nezbytná meziodvětvová spolupráce tak, aby bylo možné zhodnotit případný dopad útoku na kritickou infrastrukturu (například vyhodnocení dopadu selhání telekomunikačního sektoru na finanční služby) a také zajistit efektivní právní rámec postihu těchto útoků.[47]

Třetí priorita zdůrazňuje nutnost školení a přehledu v oblasti kybernetické bezpečnosti[48], při zapojení všech úrovní společnosti. Jedná se tedy o součinnost federální vlády se státními vládami, dále akademické působení, soukromý sektor i jednotliví domácí uživatelé. Činnost se projevuje například rozvojem programů ve školství, informováním o antivirových softwarech či pokročilým školením odborníků v oblasti kyberprostoru. Jedná se o navázání na předchozí federální legislativu, neboť v listopadu 2002 prezident podepsal zákon o výzkumu a vývoji v oblasti bezpečnosti kyberprostoru[49], kterým bylo poskytnuto oblasti výzkumu a vývoje přes devět set milionů dolarů na pět let.[50]

Čtvrtá priorita vytyčená v této strategii směřuje k zabezpečení vládního kyberprostoru.[51] Vládní sektor (ať již místní, státní či federální) se sice podílí na zajištění kritické infrastruktury jen v malém podílu, ovšem disponuje klíčovými funkcemi, jakými jsou například národní obrana, a dalšími nezbytnými službami. Pátou a poslední prioritou je zajištění bezpečnosti kyberprostoru v mezinárodní oblasti. Skládá se především ze zajištění americké národní bezpečnosti (například posílením činnosti kontrarozvědky v oblasti ochrany kyberprostoru) a z mezinárodní spolupráce (zahrnující zejména spolupráci s mezinárodními organizacemi a průmyslem). Zde se USA zavazují k aktivní

[46] *National Cyberspace Security Threat and Vulnerability Reduction Program*
[47] THE WHITE HOUSE, Washington, President Bush. *The National Strategy to Secure Cyberspace*. 2003. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
[48] *National Cyberspace Security Awareness and Training Program*
[49] *Cyber Security Research and Development Act*
[50] THE WHITE HOUSE, Washington, President Bush. *The National Strategy to Secure Cyberspace*. 2003. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
[51] *Securing Government´s Cyberspace*

roli zajišťování mezinárodní spolupráce, což dokládá například úmysl podporovat jiné státy k přijetí Úmluvy nebo k přijetí takových hmotných a procesních norem, které jsou minimálně stejně komplexní jako tato Úmluva.

Strategie je založena na partnerství mezi vládním a soukromým sektorem, v rámci kterého odpovědnost za zajištění bezpečného kyberprostoru spočívá na obou těchto subjektech. Doporučení vymezená ve strategii nejsou příliš konkrétní, přesto se jedná o jednu z významných aktivit pro současnou podobu ochrany kyberprostoru. Navíc lze připustit, že konkrétně vymezená nařízení a normy by současně vyžadovala potřebu časté revize s ohledem na neustálý technologický pokrok.

3.4. Mezinárodní strategie pro kyberprostor

Strategické cíle USA se zaměřují na dva klíčové problémy, zlepšení odolnosti proti kybernetickým útokům a snížení hrozeb v kyberprostoru. [52] Kyberprostor je označován jako součást kritické infrastruktury země, a proto je jeho bezpečné fungování klíčovou složkou hospodářství a národní bezpečnosti. V květnu 2011 prezident USA zveřejnil Mezinárodní strategii pro kyberprostor, která hned v úvodu vymezuje síťové technologie jako nesmírný potenciál nejen národa, ale celého světa.[53] Kyberprostor má být otevřený inovacím, bezpečný, spolehlivý a založený na mezinárodní spolupráci. Právní normy, které mají takový prostor zajistit, tedy musí vycházet zejména z principů respektování základních svobod, vlastnického práva, ochrany soukromí, práva na sebeobranu a ochranu před trestnými činy. USA se v této strategii opírají o tři základní pilíře, kterými jsou diplomacie (*diplomacy*), obrana (*defense*) a rozvoj (*development*). Diplomacie zahrnuje jednotné zapojení nejen států a mezinárodních či regionálních organizací, ale také samotných uživatelů, prodejců hardwarového a softwarového zařízení či poskytovatelů internetového připojení. Ve spojení s obranou USA konstatují, že na nepřátelské činy v kyberprostoru

[52] Cybersecurity. In: *The White House* [online]. 2015 [cit. 2015-01-24]. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
[53] THE WHITE HOUSE, Washington, President Obama. *International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World*. 2011. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

odpoví stejným způsobem jako na kteroukoliv jinou hrozbu. Za tímto účelem si vyhrazují právo použít všechny nezbytné prostředky, ať již diplomatické, informační, ekonomické či vojenské, použité v souladu s požadavky mezinárodního práva. Pilíř rozvoje zmiňuje nutnost zjednat výhody bezpečného a spolehlivého kyberprostoru dostupnějšími a za tímto účelem se USA, nacházející se v této oblasti ve vedoucí pozici, zavázaly umožnit využití svých technických zdrojů a odborných znalostí ostatními státy.

Strategie zmiňuje sedm základních priorit. První z nich představuje ekonomický závazek podporovat technologické inovace a obchod při současné ochraně práv duševního vlastnictví. Druhá priorita se vztahuje k zajišťování bezpečného kyberprostoru jak na národní, tak na mezinárodní úrovni. Třetí priorita zdůrazňuje nutnost účinného prosazování práva proti kyberzločinům včetně využití mezinárodních norem. Další priority spočívají ve vojenské spolupráci, zapojení více zúčastněných stran v problematice internetu, mezinárodní spolupráci a sdíleném rozvoji kyberprostoru při respektování základních práv a svobod.

Ve vyjádření k této strategii dne 16. května 2011 tehdejší ministryně zahraničních věcí USA Hillary Clintonová uvedla, že tato strategie nepředstavuje soubor nařízení, ale snahu vytvořit globální konsensus k vizi budoucí podoby kyberprostoru. Strategie tuto podobu definuje jako prostor otevřený inovacím, bezpečný, spolehlivý a založený na mezinárodní spolupráci a protože k jeho dosažení není možné stanovit pouze jednu možnou cestu, využívá tento dokument pouze prosazení principů a základních pilířů.[54] Strategie má tedy nejen reprezentovat přístup federální vlády USA k nadcházejícímu vývoji kyberprostoru, ale rovněž má představovat základní body mezinárodní spolupráce, a to nejen mezistátní, ale také ve spolupráci s mezinárodními organizacemi a soukromým sektorem.

[54] U.S. DEPARTMENT OF STATE. *Secretary Clinton on U.S. International Strategy for Cyberspace*. 2011. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

3.5. Současná politika USA týkající se kybernetické bezpečnosti

Z hlediska legislativního se stalo výrazným posunem přijetí čtyř zákonů v oblasti kybernetické bezpečnosti, které byly podepsány prezidentem USA dne 18. prosince 2014. Tyto zákony jednak rozšířily spolupráci veřejného a soukromého sektoru a požadavky na zaměstnance Ministerstva vnitřní bezpečnosti, jednak zdůraznily roli Národního institutu standardů a technologie. Tento institut sice není regulačním orgánem, nicméně jím vytvořené předpisy mohou být přijaty rovněž soukromými společnostmi a dokonce i soudy mohou využít těchto předpisů jako měřítko zajištění kybernetické bezpečnosti systému jakékoliv společnosti, tedy i té, která není vlastníkem prvku kritické infrastruktury[55].

Klíčovými oblastmi se pro Spojené státy v oblasti kyberzločinů stalo narušení počítačového systému (tzv. hacking), dále internetové pronásledování (tzv. cyberstalking) a využití počítačových znalostí při vyšetřování a ve forenzních vědách.[56] Sféře narušení počítačového systému se již od roku 2000 věnovala kalifornská jednotka CHIP (Computer Hacking/Intellectual Property), spadající pod americké ministerstvo vnitřní bezpečnosti a úzce spolupracující s policejními sbory, justicí, advokáty a soukromým sektorem. Právě jednotka CHIP napomohla trestnímu stíhání a odsouzení mnoha pachatelů, například v mediálně známém případě „Král spamů“[57]. Problematika kyberpronásledování se stala významnou zejména s ohledem na celosvětové rozšíření užívání sociálních sítí, ať se již jedná o uživatele Facebooku, Twitteru, MySpace či YouTube. Podle statistických údajů jsou v zemi za jeden rok registrovány asi tři miliony obětí trestného pronásledování. Každý čtvrtý z nich je pronásledován prostřednictvím internetu, zejména posíláním e-mailů či jiných zpráv,

[55] DAHL, Matt. Understanding the New Federal Cyber Laws. In: *Security Magazine* [online]. 2015 [cit. 2015-01-26]. Dostupné z: http://www.securitymagazine.com/articles/86057-understanding-the-new-federal-cyber-laws.

[56] THE DEPARTMENT OF JUSTICE USA. *Cyber Crime* [online]. 2014 [cit. 2015-01-24]. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

[57] Za „krále spamů“ je označován Robert Soloway, který využíval cizí počítače k posílání emailů a stal se jedním z největších spammerů (tedy osobou posílající spamy) na světě. V roce 2007 byl zadržen a o dva roky později odsouzen za emailové podvody, krádeže identit a praní špinavých peněz k téměř čtyřem letům vězení. Více např. na www.liveleak.com/view?i=dd5_1242169514.

blogy či webovými stránkami o oběti a internetovými diskusními stránkami.[58] Využití počítačových technik a znalostí při vyšetřování a ve forenzních disciplínách je vzhledem ke složitosti kyberzločinů samozřejmou nezbytností. Školení jednotlivých policistů, státních zástupců a soudců v trendech počítačové kriminality zajišťuje Národní počítačový soudní institut (the National Computer Forensics Institute neboli NCFI), vytvořený v roce 2007. Kromě vzdělávání v oblasti počítačových kriminálních metod je toto školení přínosné zejména pro studium práce s digitálními důkazy.[59]

Podle zveřejněných údajů ministerstva vnitřní bezpečnosti došlo k navýšení počtu specialistů na kyberzločiny v posledních dvou letech o pět set procent. Již pět let také funguje národní centrum zaměřené na varování před hrozbami kybernetického prostoru (the National Cybersecurity and Communications Integration Center, dále „NCCIC"), jehož hlavním úkolem je ochrana amerického kyberprostoru a řešení vzniklých incidentů. Součástí tohoto národního centra je i tým US-CERT (Computer Emergency Readiness Team), který úzce spolupracuje s antivirovými programy a poskytuje odbornou technickou podporu provozovatelům informačních systémů.[60]

[58] Bureau of Justice Statistics. [online]. 2015 [cit. 2015-01-24]. Dostupné z: http://www.bjs.gov/.
[59] WHITE VANCE, Joyce. Forensics: Secret Service Computer Forensics Training Facility. In: *The Department of Justice USA* [online]. 2014 [cit. 2015-01-24]. Dostupné z: http://www.justice.gov/usao/priority-areas/cyber-crime/forensics.
[60] Cybersecurity Results. In: *The Department of Homeland Security* [online]. 2013 [cit. 2015-01-24]. Dostupné z: http://www.dhs.gov/cybersecurity-results.

4. Právní úprava Evropské unie

4.1. Primární právo

Jelikož je kyberkriminalita součástí oblasti trestního práva, které je znakem státní suverenity, má zde Unie omezené pravomoci k regulaci. Soudní dvůr Evropské unie (dále „SDEU“) v mnoha svých rozsudcích zopakoval, že trestněprávní předpisy v zásadě stejně jako trestně procesní pravidla nejsou v pravomoci Unie.[61] SDEU však zároveň připomenul, že zákonodárci Společenství nelze bránit v přijímání opatření, vztahujících se k trestnímu právu členských států. Je tedy nezbytné, aby některé kompetence k tomu se vztahující mohla Unie vykonávat, ať již z důvodu odstraňování překážek pro fungování trhu mezi členskými státy, které vznikají v důsledku trestného jednání, tak i z důvodu lepší součinnosti v trestních věcech, která umožňuje stabilní ekonomický a společenský vývoj.[62]

Ustanovení o policejní a soudní spolupráci v trestních věcech ve Smlouvě o Evropské unii hovoří o užší spolupráci v prevenci a boji s trestnou činností, včetně sbližování předpisů trestního práva členských států. Smlouva o fungování Evropské unie již přímo hovoří o trestné činnosti v oblasti výpočetní techniky, kdy je možné formou směrnic stanovit minimální pravidla týkající se vymezení trestných činů a sankcí. Tato úprava je připuštěna zejména s ohledem na podstatný přeshraniční prvek, který je pro kyberprostor charakteristický. Navíc jsou Evropský parlament a Rada oprávněny přijímat pobídková a podpůrná opatření pro činnost členských států v rámci předcházení trestné činnosti.[63]

K nástrojům, které byly v oblasti spolupráce v trestním právu využity, patří i rámcová rozhodnutí. Tato podle smluvního textu neměla přímý účinek, avšak SDEU v případu Pupino konstatoval, že vnitrostátní soud je povinen vykládat všechna pravidla

[61] Rozsudek Soudního dvora ze dne 13. září 2005, Komise Evropských společenství proti Radě Evropské unie, C – 176/03. Rozsudek Soudního dvora ze dne 11. listopadu 1981, trestní řízení proti Guerrinu Casatiovi, C- 203/80. Rozsudek Soudního dvora ze dne 16. června 1998, trestní řízení proti Johannovi Martinovi Lemmensovi, C – 226/97.

[62] SAVIN, Andrej. *EU internet law: the transformation of crime in the information age*. Reprint. Cambridge: Polity, 2007, s. 233. ISBN 9781781006016.

[63] Smlouva o Evropské unii - čl. 29; Smlouva o fungování Evropské unie - čl. 83 a 84

vnitrostátního práva s ohledem na znění i účel rámcového rozhodnutí. Skutkově se jednalo o výklad článků 2, 3 a 8 rámcového rozhodnutí Rady 2001/220/SVV ze dne 15. března 2001 o postavení obětí v rámci trestních řízení. Učitelka v mateřské školce, M. Pupino, byla obviněna z ublížení na zdraví žáků mladších pěti let. Státní zástupce požadoval, aby výslech dětí byl proveden ve speciálním zařízení za podmínek, které chrání důstojnost, soukromí a duševní vyrovnanost dotčených nezletilých, případně i za připojení znalce v oboru psychologie, a to z důvodu citlivého charakteru a závažnosti skutků, jakož i z důvodu obtíží spojených s nízkým věkem obětí. Soudce byl podle italské právní úpravy nucen takovýto návrh zamítnout, avšak protože výše zmíněné rámcové rozhodnutí umožňuje návrhu vyhovět, položil předběžnou otázku ohledně výkladu předmětných článků rozhodnutí. SDEU zde rozšířil význam rámcových rozhodnutí, když zdůraznil povinnost členských států zohlednit rámcová rozhodnutí a jejich účel při výkladu vnitrostátních norem a předjímal tak užší vztah unijního a vnitrostátního práva v trestní sféře.[64]

Počátečními konkrétními nástroji, které Unie v oblasti kyberkriminality využila, jsou sdělení pocházející až z roku 2001 o vytvoření bezpečnější informační společnosti zlepšením bezpečnosti informačních infrastruktur a bojem proti počítačové kriminalitě[65] a sdělení o síťové a informační bezpečnosti: návrh k postoji evropské politiky[66]. Dalším krokem, který podstatně ovlivnil unijní přístup k boji proti počítačové kriminalitě, byla Úmluva o počítačové kriminalitě, která byla schválena výborem ministrů Rady Evropy v roce 2001[67] a která je podrobněji rozebrána níže. V následujících letech se pak právní opatření zaměřila především na problémy spojené se zásahy do počítačových systémů (včetně nevyžádaných emailů či spamů) a také na ochranu zvláště zranitelných osob na internetu (především na ochranu dětí).[68]

[64] Rozsudek Soudního dvora ze dne 16. června 2005, trestní řízení proti Marii Pupino, C – 105/03.
[65] Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime. In: Official website of the European Union [online]. 2000 [cit. 2014-03-16]. Dostupné z:http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193b_en.htm.
[66] *Network and Information Security: Proposal for a European Policy Approach*. 2001. Dostupné z: http://www.steptoe.com/assets/attachments/811.pdf.
[67] *Kyberkriminalita a právo*. Vyd. 1. Editor Tomáš Gřivna, Radim Polčák. Praha: Auditorium, 2008, s. 104. ISBN 978-809-0378-674.
[68] SAVIN, Andrej. *EU internet law*. Cheltenham, UK: Edward Elgar, 2013, xix, 266 pages. Hacking, s. 235. ISBN 9781845429379.

Lisabonská smlouva pozměňující Smlouvu o Evropské unii a Smlouvu o založení Evropského společenství (dále „Lisabonská smlouva“), která vstoupila v platnost v prosinci 2009, výslovně uznává unijní kompetenci v trestních věcech, a to formou směrnic. Evropský parlament a Rada mohou stanovit u mimořádně závažné trestné činnosti minimální pravidla k definování trestných činů a sankcí. Jedná se o kriminalitu přeshraniční povahy v oblastech, které jsou uvedeny v článku 83 Smlouvy o fungování Evropské unie. Výslovně je tak uvedena i trestná činnost v oblasti výpočetní techniky. Počítačové zločiny jsou tak svoji závažností postaveny na roveň terorismu, obchodu s lidmi a sexuálním vykořisťováním žen a dětí, nedovolenému obchodu s drogami, nedovolenému obchodu se zbraněmi či praní peněz. Uvedený výčet nemusí být konečný, neboť mimořádně závažná trestná činnost s přeshraničním rozměrem může být navázána na celou řadu dalších aktivit. V tomto kontextu je také nutné zmínit pravomoci Europolu či obsah podmínek spolupráce evropského zatýkacího rozkazu, kde jsou i trestné činy nikoliv uvedené ve výčtu článku 83. Konkrétní činnost Unie lze spatřovat ve dvojí podobě. Jednak na úrovni nadnárodní, tedy ve vytváření definic a podnikání klíčových kroků v trestní oblasti, jednak v podobě zprostředkovatele spolupráce mezi členskými státy. Spojení těchto dvou úrovní vyústilo například v návrh na vytvoření úřadu evropského veřejného žalobce. Požadavek zachovávání principu subsidiarity, který je v dané oblasti nezpochybnitelný, je rozvíjen a doplňován veřejným zájmem na účinném postihu závažné trestné činnosti v celé Unii. Činnost Unie je v tomto případě podmíněna závažností trestného činu, potřebou zapojení ucelenějšího justičního systému a nutností ochrany Unie (respektive jejích občanů jako celku) jako potenciální oběti.[69]

Lisabonská smlouva tak potvrdila další směřování Unie v této sféře, a to jak v oblasti právní, tak v oblasti strategické. V právní oblasti se jedná zejména o přijetí nových směrnic, mezi kterými lze uvést například směrnici o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii z roku 2011 (zabývající se i činy využívající informačních technologií) a směrnici o útocích proti informačním systémům z roku 2013 (zakotvující povinnost členských států evidovat statistické údaje o kyberzločinech). Ve strategické oblasti je zásadním průlomem zřízení Evropského

[69] EUROPEAN PARLIAMENT - DIRECTORATE- GENERAL FOR INTERNAL POLICIES.*Developing a Criminal Justice Area in the European Union*. Brussels, 2014.

centra pro boj proti kyberkriminalitě, které představuje platformu pro uplatňování unijního práva a možnost užší spolupráce mezi policejními složkami, obchodními společnostmi, výzkumnými centry, uživateli internetu a občany Unie.[70] Obě tyto úrovně se navzájem doplňují a tvoří základ holistického přístupu Unie k boji proti kyberkriminalitě. K zajištění účinnosti právních norem je bezesporu nutný úřad disponující odborníky na počítačovou kriminalitu. Předpokladem je ovšem uzákonění základních definic počítačových trestných činů a sankce za ně v jednotlivých členských státech.

V oblasti kyberprostoru je v současné době vytvořen komplexní soubor opatření, zejména se jedná o širokou řadu přijatých programů. V roce 2010 představila Evropská komise Digitální program pro Evropu.[71] V programu byla zdůrazněna potřeba řešit na evropské úrovni rostoucí počítačovou trestnou činnost, která byla označena za jednu z hlavních překážek digitálního programu. V roce 2011 byl na základě článku 71 Smlouvy o fungování Evropské unie zřízen Stálý výbor pro operativní spolupráci v oblasti vnitřní bezpečnosti. Ve výboru působí vysocí úředníci členských států Unie, ministři vnitra, zástupci Komise, Eurojustu, Europolu či Frontexu. Výbor se mimo jiné podílel i na vytvoření Evropského centra pro boj proti kyberkriminalitě, otevřeného počátkem roku 2013.

4.2. Sekundární právo

Zaměření se na problémy spojené se zásahy do počítačových systémů vyústilo v přijetí směrnice o útocích proti informačním systémům 2013/40/EU[72], která nahradila rámcové rozhodnutí Rady 2005/222/SVV[73]. Toto rámcové rozhodnutí Rady, přijaté v roce 2005, spočívalo především v harmonizaci trestního práva členských států ve vztahu

[70] BUONO, Laviero. Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (EC3). In: *New journal of European criminal law*. 2012, s. 332-334. ISSN 2032-2844.
[71] Digitální program pro Evropu. In: *Oficiální webové stránky Evropské unie* [online]. 2010 [cit. 2015-01-24]. Dostupné z: http://europa.eu/legislation_summaries/information_society/strategies/si0016_cs.htm.
[72] Směrnice Evropského parlamentu a Rady 2013/40/EU o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV. (Úřední věstník EU č. L 218/8 z 12. 8. 2013).
[73] Rámcové rozhodnutí Rady 2005/222/SVV o útocích proti informačním systémům. (Úřední věstník EU č. L 69 z 16. 3. 2005).

k informačním systémům. Bylo přijato v rámci třetího pilíře a členské státy zavazovalo s ohledem na výsledek, avšak ponechávalo úvaze států, jakou formu a metodu k zajištění cíle zvolí. Zmíněné rozhodnutí bylo přijato s ohledem na znění Úmluvy a s bližším zaměřením na boj proti trestné činnosti související s informačními systémy. V zásadě toto rozhodnutí směřuje ke dvěma cílům, jednak k zajištění společného právního základu této trestné oblasti napříč státy Unie a jednak k usnadnění stíhání pachatelů.[74]

Právě k zajištění prvního cíle je také v úvodu definováno několik základních pojmů, zejména pak pojem informační systém. Informačním systémem se rozumí jakýkoli přístroj, který provádí na základě programu automatické zpracování počítačových dat, jakož i data tímto přístrojem uložená, zpracovaná nebo přenesená za účelem jejich provozu, použití, ochrany a údržby.[75] Rozhodnutí rozlišuje tři druhy trestných činů. Prvním z nich je neoprávněný přístup do informačního systému. Jako trestný čin je vymezeno protiprávní úmyslné jednání, kdy se nejedná o případ menšího významu. Každý členský stát ale může rozhodnout, že jednání je trestné jen v případě, že bylo spácháno překonáním bezpečnostního opatření. Profesor Savin spatřuje jako výhodu tohoto opatření jeho značnou pružnost.[76] Toto ustanovení totiž umožňuje postih nejen neoprávněného přihlášení se do počítačového systému, ale také postih všech útoků se vzdálenějším cílem, v rámci kterých je ovšem nezbytný neoprávněný přístup do systému. Příkladem může být pachatelovo využití nedostatečně zabezpečeného systému k rozesílání tisíců nevyžádaných e-mailových zpráv.[77] Obecně se o neoprávněném přístupu do informačního systému nejčastěji hovoří v souvislosti s tzv. *hacking* (tedy neoprávněný přístup k počítači nebo sítí počítačů).[78]

Druhým trestným činem je protiprávní zásah do systému, při kterém dochází k úmyslnému závažnému narušení nebo přerušení fungování informačního systému.

[74] KLIMEK, Libor. Combating Attacks against Information Systems: EU Legislation and its Development. *Masaryk University Journal of Law and Technology*. 2012, č. 1. Dostupné z: http://mujlt.law.muni.cz/view.php?cisloclanku=2012070007.

[75] Rámcové rozhodnutí Rady 2005/222/SVV o útocích proti informačním systémům. (Úřední věstník EU č. L 69 z 16. 3. 2005).

[76] SAVIN, Andrej. *EU internet law*. Cheltenham, UK: Edward Elgar, 2013, xix, 266 pages. Hacking, s. 247. ISBN 9781845429379.

[77] SAVIN, Andrej. *EU internet law*. Cheltenham, UK: Edward Elgar, 2013, xix, 266 pages. Hacking, s. 247. ISBN 9781845429379.

[78] Proposal for a Council Framework Decision on attacks against information systems. *Liberty and Security* [online]. 2005 [cit. 2014-03-16]. Dostupné z: http://www.libertysecurity.org/article564.html.

I v tomto případě za trestný čin není považován případ menšího rozsahu. K závažnému narušení nebo poškození systému může dojít vložením, přenosem, poškozením, vymazáním, znehodnocením, pozměněním, potlačením nebo znepřístupněním počítačových dat, které bylo spácháno neoprávněně, avšak k samotnému přístupu do systému mohl pachatel být oprávněný. Příkladem takového jednání může být tzv. odmítnutí služby (*denial of service*), při kterém je webový server či poskytovatel internetových služeb přehlcen požadavky, které jsou automaticky generovány právě za účelem narušení systému.[79] Pod tento trestný čin také spadají útoky realizované prostřednictvím počítačových virů.

Třetí trestný čin vymezený tímto rozhodnutím je protiprávní zásah do dat. Zde dochází k neoprávněnému a úmyslnému vymazání, poškození, znehodnocení, pozměnění, potlačení nebo znepřístupnění počítačových dat v informačním systému, opět nejedná-li se o případ menšího rozsahu. Útok je tedy veden proti datům, zatímco v předchozím případě se jednalo o zásah do systému. Nejčastěji je útok proveden formou počítačových virů, ale také prostřednictvím programů, například v podobě tzv. trojského koně.

V článku 8 Rámcového rozhodnutí je zakotvena odpovědnost právnických osob za výše uvedené trestné činy. Členským státům tedy byla uložena povinnost přijmout nezbytná opatření k zajištění této odpovědnosti. Tato odpovědnost nastává za předpokladu, že trestný čin spáchala ve prospěch právnické osoby jakákoliv osoba působící v právnické osobě na vedoucím postavení, s oprávněním ji zastoupit, s pravomocí přijímat rozhodnutí jejím jménem nebo pravomoc vykonávat v jejím rámci kontrolu. Odpovědnost fyzické osoby, která byla pachatelem, návodcem nebo účastníkem tím není dotčena.

Článek 10 následně rozebírá otázku soudní pravomoci. Ta je klíčová, neboť jeden trestný čin může zasáhnout několik států. Pravomoc státu je dána, byl-li trestný čin zcela nebo zčásti spáchán na jeho území, je-li pachatel jeho státním příslušníkem nebo byl trestný čin spáchán ve prospěch právnické osoby, která má své sídlo na jeho

[79] Proposal for a Council Framework Decision on attacks against information systems. *Liberty and Security* [online]. 2005 [cit. 2014-03-16]. Dostupné z: http://www.libertysecurity.org/article564.html.

území. Pokud jde o první podmínku, ke vzniku pravomoci postačuje, aby byl pachatel fyzicky na území státu, bez ohledu na umístění informačního systému, ke kterému útok směřuje. Stejně tak postačí i přítomnost informačního systému na daném území, bez ohledu na skutečnou přítomnost pachatele. Soudní pravomoc může tedy být dána v jednom případě u více států, jelikož může dojít k zásahu dat umístěných na více územích. Typicky tento případ může nastat v případě webových stránek.[80]

Rámcové rozhodnutí bylo nedůsledné jak v definici trestného činu neoprávněného přístupu do informačního systému (neboť vymezení neoprávněného přístupu zde zcela chybí), tak ve vymezení protiprávního zásahu do systému. Zásah totiž může být dvojího charakteru a toto dělení se liší co do závažnosti jednání. V první skupině jsou například trestné činy v rámci organizovaného zločinu, zatímco v druhé skupině jsou útoky způsobené jednotlivci a vedené politickými důvody. Je samozřejmé, že obě tyto skupiny zahrnují protiprávní jednání, avšak v druhém případě se může jednat jen o určitý krátkodobý projev protestu, což zjevně nekoresponduje se závažností organizovaného zločinu. Proto by bylo užitečné odlišení závažnosti mezi těmito činy.[81]

Návrh Evropské komise (dále „Komise“) předcházející této směrnici zmiňoval pět cest k realizaci účinných opatření. První se opírala o princip status quo, takže by Unie nepřijímala žádná další opatření proti této trestné činnosti a pouze by pokračovala v probíhajících opatřeních. Druhá varianta odkazovala na nelegislativní opatření, která by podpořila koordinaci v rámci Unie, a na vytvoření evropské sítě kontaktních bodů pro spolupráci mezi veřejným a soukromým sektorem. Třetí varianta spočívala v cílené aktualizaci pravidel rámcového rozhodnutí (respektive přijaté směrnice), čtvrtá hovořila o zavedení uceleného souboru právních předpisů Unie proti kybernetické trestné činnosti a podle páté varianty by se politika měla zaměřit na aktualizaci Úmluvy, což by ovšem bylo spojeno se značně zdlouhavým procesem. Komise se ve svém návrhu přiklonila ke kombinaci druhé a třetí varianty, neboť konkrétně cílená právní úprava v kombinaci s nelegislativními opatřeními má pomoci zvýšit připravenost,

[80] SAVIN, Andrej. *EU internet law*. Cheltenham, UK: Edward Elgar, 2013, xix, 266 pages. Hacking, s. 249. ISBN 9781845429379.
[81] SAVIN, Andrej. *EU internet law*. Cheltenham, UK: Edward Elgar, 2013, xix, 266 pages. Hacking, s. 250. ISBN 9781845429379.

bezpečnost a odolnost kritické informační infrastruktury a zajistit výměnu osvědčených postupů.[82]

4.3. Usnesení o kybernetické bezpečnosti a ochraně

Usnesení o kybernetické bezpečnosti a ochraně schválené Evropským parlamentem dne 22. listopadu 2012 [83] vychází především ze Zprávy o provádění Evropské bezpečnostní strategie[84], z Úmluvy, ze zprávy Komise Digitální agenda pro Evropu a ze závěrů Rady o ochraně kritické informační infrastruktury. Usnesení poukazuje na závislost členských států Unie na bezpečný kyberprostor, připomíná, že informační a komunikační prostředky jsou využívány k represivním účelům a zdůrazňuje, že se kyberprostor stává centrální platformou pro uplatňování lidskoprávních požadavků a že tento neustále rozšiřující se prostor obsahuje stále nové hrozby a útoky. V usnesení se také objevuje výtka směrem k vnitřní i vnější spolupráci. Evropský parlament shledává spolupráci mezi členskými státy i mezi třetími partnery jako nedostatečnou. Stejně tak je definován problém nejednotné terminologie, neboť jednotlivé státy různě interpretují pojmy jako kybernetická bezpečnost či kybernetická ochrana. Z toho také logicky plyne požadavek jednotnosti strategií kybernetického prostoru orgánů Unie, členských států a komplexní Strategie EU, o které je pojednáno výše. Na členských státech leží kromě povinnosti dokončit (případně vyhotovit) tyto strategie také výzva vytvořit odborná soudní pracoviště, která se budou zabývat především narušením informačních systémů. Vytvoření soudů, které by se primárně zabývaly ochranou

[82] Návrh směrnice Evropského parlamentu a Rady o útocích proti informačním systémům a zrušení rámcové rozhodnutí Rady 2005/222/SVV. In: *2010/0273 (COD)*. 2010. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:CS:HTML.

[83] Usnesení Evropského parlamentu ze dne 22. listopadu 2012 o kybernetické bezpečnosti a ochraně. In: *2012/2096(INI)*. Štrasburk, 2012. Dostupné z: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0457&language=CS&ring=A7-2012-0335.

[84] Návrh usnesení Evropského parlamentu o provádění Evropské bezpečnostní strategie a EBOP. In: *2008/2003(INI)*. 2008. Dostupné z: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A6-2008-0186+0+DOC+XML+V0//CS.

soukromí v kybernetickém prostoru, již zvažuje například Spolková republika Německo.[85]

Usnesení obsahuje několik zásadních výtek směrem k současné situaci v oblasti kyberprostoru. V usnesení je tak zahrnut obecný požadavek na posílení spolupráce mezi vládním a soukromým sektorem, zejména pokud jde o zvýšení odolnosti informačních sítí a předávání informací o útocích. Mnoho soukromých společností například odmítalo nahlašování kybernetických útoků z obav o únik informací či poškození jména společnosti. Cestou z této nepříznivé situace je zajištění anonymity osob, které útoky nahlašují. Je třeba podotknout, že veřejný sektor ve většině členských států neřadil mezi své priority modernizaci informačních a komunikačních technologií a chyběl definovaný společný postup států v případě kybernetického útoku jednoho státu proti druhému. Kromě toho je aktuální a velmi významnou hrozbou možný útok ze strany teroristických skupin nebo jiných kriminálních uskupení. Zajímavý akcent je zde kladen na strategii „bílých hackerů" (někdy také označováni jako „etičtí hackeři"[86]), zejména pokud jde o nezletilé osoby, neboť lze využít jejich znalostí a zároveň zjednat nápravu jejich kriminální minulosti, případně se takové vyvarovat. Usnesení také hovoří o potřebě minimálních norem transparentnosti a zajištění odpovědnosti za bezpečný kyberprostor. Tato má být sdílena mezi veřejným a soukromým sektorem. Komise by zde měla sehrát sjednocující roli, neboť právě ona by měla definovat minimální normy kybernetické bezpečnosti a certifikačních systémů. Domnívám se, že potřeba transparentnosti je vztažena ke správě technologických prostředků a zajišťování bezpečného kyberprostoru. Za něj totiž sice odpovídá v konečném důsledku stát, ovšem spravujícími subjekty jsou zpravidla soukromé osoby. Citlivost oblasti je zřejmá již na první pohled, proto je potřeba stanovit základní požadavky právně závaznou cestou a považuji za vhodnou regulaci ze strany Komise, neboť se úpravy mohou v jednotlivých členských státech i výrazně lišit.

Evropský parlament také upozornil na skutečnost, že došlo ke snížení výdajů na výzkum a vývoj v oblasti obrany, což znesnadňuje udržování vysoké úrovně

[85] VASAGAR, Jeevan. Google could face ´cyber courts´ in Germany over privacy rights. *Financial Times* [online]. 2014 [cit. 2015-02-15]. Dostupné z: http://www.ft.com/cms/s/0/a7580826-e59d-11e3-8b90-00144feabdc0.html.

[86] ROUSE, Margaret. Ethical hacker. *Search Security* [online]. 2014 [cit. 2015-02-15]. Dostupné z: http://searchsecurity.techtarget.com/definition/ethical-hacker.

kybernetické bezpečnosti. Deleguje povinnost kontroly vhodných investic v této oblasti na Evropskou obrannou agenturu, která má dohlížet na zajišťování kybernetické bezpečnosti jednotlivými členskými státy. Podle výroční zprávy za rok 2014[87] také Evropská obranná agentura navázala spolupráci s talinskou sekcí NATO – *„Cooperative Cyber Defence Centre of Excellence“*, která se zabývá vzděláváním, školením, výzkumem a vývojem v oblasti kybernetické bezpečnosti. S výzkumem a vývojem také souvisí prohlubování systematického vzdělávání zaměstnanců soudních a bezpečnostních institucí a odborníků na informační systémy. Obecně je vzdělávání v této oblasti prioritou, na regionální úrovni mají být vytvořeny programy k podpoře bezpečného užívání nových technologií a sítí určené jak pro podnikatelskou sféru, tak pro jednotlivé fyzické osoby, a to již od raného věku. Vzdělávání se má projevit rovněž na úrovni krizového plánování a je považováno za samozřejmé, že analýza rizik nezbytná v rámci krizové připravenosti obsáhne rovněž kybernetické hrozby. I toto je jedna z oblastí, kde členské státy dosud spíše zaostávají, neboť ani orgány veřejné správy ani soukromé subjekty dlouho nevěnovaly v přípravě na mimořádné události a krize této oblasti dostatečnou pozornost.

Dalším důležitým požadavkem je vymezení jasných hranic mezi bezpečnostními opatřeními a lidskými a občanskými právy. Je třeba pamatovat na ochranu těchto práv i při zajišťování bezpečného kyberprostoru. V závěru je zdůrazněna nutnost spolupráce mezi Unií a USA v oblasti kybernetické bezpečnosti. V případě spolupráce je klíčová nejen výměna informací, ale také zaujetí společného postoje v otázce zachování lidských práv a svobod při současné ochraně kyberprostoru a prohloubení další spolupráce v boji proti kybernetickým útokům.

4.4. Strategie Evropské unie v oblasti kybernetické bezpečnosti

Evropská komise a vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku zveřejnily 7. února 2013 strategii počítačové bezpečnosti nazvanou Otevřený,

[87] Annual Report 2013. In: *European Defence Agency* [online]. 2014 [cit. 2015-02-15]. Dostupné z: http://www.eda.europa.eu/info-hub/publications/publication-details/pub/annual-report-2013.

bezpečný a spolehlivý kybernetický prostor (dále „Strategie EU“).[88] V úvodu tato Strategie EU připomíná základní principy ochrany kyberprostoru, které mají být respektovány nejen v rámci Unie, ale na celém světě. Jedná se o požadavek aplikace stejných zákonů a právních norem uplatňujících se jak v každodenním životě, tak v prostoru kybernetiky a o princip ochrany základních práv, zejména ochranu svobody projevu a ochranu soukromí. Dále Strategie EU zmiňuje požadavek zajištění přístupu k Internetu všem občanům, kontrolu digitálního světa nikoliv pouze jedním subjektem, ale při současném zapojení více účastníků, včetně nevládních organizací a soukromého sektoru. Tuto sekci principů Strategie EU uzavírá požadavkem sdílené odpovědnosti za bezpečnost kyberprostoru. Uvedený požadavek je stanoven s ohledem na vzrůstající závislost na informačních a komunikačních technologiích ve všech oblastech lidského života. Aby byl tedy systém méně zranitelným, je nutné aktivní zapojení nejen osob veřejného práva, ale také práva soukromého.

Ve Strategii EU se uznává, že zajištění bezpečnosti kyberprostoru je primárně povinnost jednotlivých členských států, ale k účinnému výsledku, definovanému v pěti prioritách, navrhuje několik společných kroků. Vytyčených pět priorit se vztahuje k dosažení kybernetické odolnosti, výraznému snížení počítačové kriminality, rozvoji politiky počítačové obrany a schopnostem souvisejícím se společnou bezpečnostní a obrannou politikou, rozvoji průmyslových a technologických zdrojů pro počítačovou bezpečnost a vypracování ucelené mezinárodní počítačové politiky pro Unii a propagaci základních hodnot Unie. K dosažení těchto priorit Unie rovněž představila návrh směrnice o bezpečnosti sítí a informací.[89] Podle této směrnice by měly členské státy povinnost přijmout strategii pro bezpečnost sítí a informací a pro tuto oblast určit příslušný orgán s kompetencemi pro prevenci a reakci na události, přičemž členský stát je povinen zajistit tento orgán vhodným technickým, finančním a personálním zázemím nezbytným

[88] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. In: 2013. Dostupné z: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

[89] Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii. In:*2013/0027/COD*. 2013. Dostupné z: http://eur-lex.europa.eu/procedure/EN/202368.

pro naplňování účelu směrnice. Dále má být vytvořen mechanismus spolupráce členských států s unijní úrovní, zejména pro včasná varování před riziky a událostmi a k zajištění jednotné aplikace směrnice. Směrnice také hovoří o povinnostech operátorů trhu (*market operator*), kterými se podle výkladového ustanovení rozumí poskytovatel služeb informační společnosti a provozovatel kritických infrastruktur ve vybraných odvětvích. Tito operátoři trhu, stejně jako orgány veřejné správy, jsou povinni hlásit ustanovenému orgánu v této oblasti (viz výše) všechny události, mající významný dopad na bezpečnost v okruhu jejich základních služeb. Členský stát je také povinen zajistit, aby orgány veřejné správy i operátoři trhu přijali vhodná technická a organizační opatření k zajištění bezpečnosti síťových a informačních systémů. Ustanovený orgán, kterému byly v oblasti svěřeny kompetence, může od orgánů veřejné správy i operátorů trhu vyžadovat všechny informace potřebné k posouzení bezpečnosti jejich síťových a informačních systémů a může od nich vyžadovat podstoupení bezpečnostního auditu provedeného nezávislým orgánem nebo státní mocí. Dále má mít tento orgán také pravomoc vydávat závazné pokyny vůči orgánům veřejné správy a operátorům trhu, přičemž všechny povinnosti, uložené těmto subjektům, musí být možné přezkoumat v soudním řízení.

Ve Strategii EU je zdůrazněna úloha Evropské agentury pro bezpečnost sítí a informací (ENISA) [90] vytvořená již v roce 2004. Zapojení této agentury umožnuje snazší dosažení kybernetické odolnosti především u průmyslových kontrolních systémů a v dopravní a energetické infrastruktuře. Za tímto účelem by agentura měla zajistit a rozvíjet nezbytnou odbornost, kontrolovat činnost bezpečnostních týmů pro koordinaci řešení bezpečnostních incidentů v počítačových sítích [91] v průmyslových kontrolních systémech či podporovat členské státy a evropské instituce při testech kyberspolupráce na panevropské úrovni [92].

K dosažení priority výrazného snížení počítačové kriminality se Komise touto strategií zavazuje naléhat na členské státy, které dosud neratifikovaly Úmluvu, aby tak učinily co nejdříve. Zároveň je zde zmíněna aktivní legislativní činnost v boji proti kyberzločinům, kterou dokládá například přijetí směrnice o boji proti pohlavnímu

[90] *The European Network and Information Security Agency*
[91] *Computer Security Incident Response Teams*
[92] *Pan-European Cyber Incident Exercises*

zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii či směrnice o útocích proti informačním systémům. Kromě spolupráce mezi členskými státy navzájem je připomenuta nutnost úzké spolupráce s Evropským centrem pro boj proti kriminalitě, Europolem a Eurojustem. Pro ilustraci lze uvést úkoly pro Eurojust, kterými jsou mimo jiné identifikace hlavních překážek soudní spolupráce při vyšetřování kyberzločinů mezi členskými státy Unie a ve vztahu s třetími státy či podpora vyšetřování a stíhání kyberzločinů jak na operativní, tak na strategické úrovni.

V mezinárodní počítačové politice Strategie EU odkazuje na úzkou spolupráci s celou řadou organizací, například s Radou Evropy, OSN či NATO, a na bilaterální úrovni staví na přední místo spolupráci s USA. Zejména se jedná o Pracovní skupinu EU - USA pro kyberbezpečnost a kyberzločiny, která vznikla po summitu Unie a USA v roce 2010. Spolupráce byla dále ještě více prohloubena, mimo jiné po dalším summitu v Bruselu v březnu 2014, především za účelem prohloubení průřezových kybernetických otázek a mezinárodní politiky.[93]

Unie se zavazuje podporovat kyberprostor v mezinárodním kontextu jako oblast základních práv a svobod, hovoří o společenské odpovědnosti firem[94] a připomíná, že není nutná tvorba nových mezinárodních právních nástrojů pro oblast kybernetického prostoru, ale je nutné dodržování závazků obsažených v Mezinárodním paktu o občanských a politických právech, Evropské úmluvě o lidských právech a Chartě základních práv Evropské unie i v online světě. V případě ozbrojeného konfliktu, který by se překlenul i do světa kyberprostoru, se Unie dovolává mezinárodního humanitárního práva.

V závěru Strategie EU z důvodu komplexnosti problematiky rozlišuje tři základní pilíře, kterými jsou síťová a informační bezpečnost, orgány činné v trestním řízení a obrana, a dále rozlišuje evropskou a národní úroveň. Evropská úroveň v pilíři síťové a informační bezpečnosti působí zejména prostřednictvím Komise, Evropské agentury pro bezpečnost sítí a informací, sítí ustanovených orgánů podle směrnice o bezpečnosti

[93] MANN, Michael. EU-US cooperation on cyber security and cyberspace. In: *Evropská služba pro vnější činnost* [online]. Brussels, 2014 [cit. 2015-02-21]. Dostupné z: http://www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf.

[94] *Corporate Social Responsibility*

sítí a informací a Evropským partnerstvím mezi veřejným a soukromým sektorem pro odolnost[95]. Druhý pilíř je na evropské úrovni zajištěn například činností Europolu a Eurojustu a poslední pilíř má na starosti především Evropská obranná agentura[96]. Na národní úrovni se pak v prvním pilíři jedná o skupiny CERT[97] a ustanovený orgán podle směrnice o bezpečnosti sítí a informací, v druhém pilíři se nacházejí národní útvary pro kyberzločiny a poslední pilíř na národní úrovni je tvořen orgány národní obrany a bezpečnosti.

4.5. Současná politika Evropské unie týkající se kybernetické bezpečnosti

Otázka kybernetické bezpečnosti se v Evropské unii stala jednou z prioritních a dynamicky se vyvíjejících oblastí. Z hlediska strategické úrovně byla zveřejněna jednak Strategie EU, jednak Rada pro spravedlnost a vnitřní věci v červnu 2013 označila kyberzločiny za jednu z devíti unijních priorit v boji proti závažnému a organizovanému zločinu pro léta 2014 - 2017[98]. Na operační úrovni došlo v roce 2004 k vytvoření Evropské agentury pro bezpečnost sítí a informací, přičemž od roku 2013 se hlavním centrem pro boj proti kyberzločinům stalo Evropské kybernetické centrum.[99] Významným nástrojem, který Unii pomáhá v boji proti pachatelům kyberzločinů, je Evropský zatýkací rozkaz. Podle zprávy Evropské komise hodnotící první rok činnosti Evropského kybernetického centra[100]byly zatčeny stovky lidí, kteří se dopustili kybernetických útoků, online pohlavního vykořisťování dětí či platebních podvodů.

[95] *European Public-Private Partnership for Resilience*
[96] *European Defence Agency*
[97] *Computer Emergency Response Team*
[98] THE COUNCIL OF THE EUROPEAN UNION. *Council conclusions on setting the EU's priorities for the fight against serious and organised crime between 2014 and 2017*. Luxembourg, 2013. Dostupné z: http://www.eurojust.europa.eu/Practitioners/operational/THB/Documents/JHA-2013-06-06_137401_EN.pdf.
[99] EU approach to cyber-security. In: *Evropský parlament*[online]. 2014 [cit. 2015-01-25]. Dostupné z: http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140775/LDM_BRI%282014%2914 0775_REV1_EN.pdf.
[100] EUROPEAN COMMISSION. *European Cybercrime Centre – one year on*. Brussels, 2014 [cit. 2015-01-25]. Dostupné z: http://europa.eu/rapid/press-release_IP-14-129_en.htm.

Z pohledu legislativní úrovně se jedná především o směrnici 2011/92/EU o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, směrnici 2013/40/EU o útocích na informační systémy a o návrh směrnice pro zajištění vysoké úrovně společné informační a síťové bezpečnosti [101], která by rozšířila počet subjektů odpovědných za bezpečnost vlastních systémů (například by se povinnosti dotýkaly i tržních operátorů či správců kritické infrastruktury). Posledně zmíněná navrhovaná směrnice také ukládá povinnost užší spolupráce s Evropskou agenturou pro bezpečnost sítí a informací a zřízení CERT[102] týmů.

Zpráva o posouzení hrozby internetového organizovaného zločinu z roku 2014 [103] sestavená Evropským kybernetickým centrem navrhuje celou řadu potřebných opatření, která mají být přijata jak na strategické, tak na taktické úrovni. Prosazování práva na internetu by mělo být silnější a zejména více zřejmé, tato viditelnost by totiž přispěla jak k úspěšnějšímu odstrašování od trestné činnosti, tak k posílení důvěry v bezpečnost internetu. Dále je ve zprávě zdůrazněna potřeba spolupráce veřejného a soukromého sektoru, především za účelem zvyšování povědomí o kybernetických hrozbách a rozšíření možností hlášení kyberzločinů. Prostor spolupráce v sobě obsahuje mimo jiné i sdílení statistických dat. Pro vyšetřování kyberzločinů je tedy kromě rozvoje příslušných technologických nástrojů nezbytné předávání informací. Právě proto, že kyberzločiny mají přeshraniční povahu a dotýkají se tedy více jurisdikcí, by měly být odpovídajícím způsobem dány do souladu zákonné požadavky jednotlivých států, přičemž právo by mělo zprostředkovat možnost snazší a efektivnější mezinárodní spolupráce. Mezi další požadavky patří dostatečná právní adaptace na přechod na internetový protokol verze 6, který představuje některá nová rizika[104].

[101] Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii. V:*2013/0027/COD*. 2013. Dostupné z: http://eur-lex.europa.eu/procedure/EN/202368.

[102] *Computer Emergency Response Team*

[103] The Internet Organised Crime Threat Assessment. In: *Europol* [online]. 2014 [cit. 2015-01-25]. Dostupné z: https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta.

[104] Podle Marca Heuseho internetový protokol verze 6 obsahuje chyby, které umožní třetí osobě účastnit se cizí komunikace, a získat tak například hesla.

4.6. Zákon o kybernetické bezpečnosti v České republice

Protože se kybernetickou bezpečností musí zabývat i každý členský stát, jako příklad konkrétní právní úpravy v oblasti bezpečného kyberprostoru je v této kapitole nastíněna situace v České republice. V roce 2011 bylo zřízeno Národní centrum kybernetické bezpečnosti a Rada pro kybernetickou bezpečnost, přičemž národní autoritou v této sféře byl ustaven Národní bezpečnostní úřad. Tento úřad také zpracoval návrh zákona o kybernetické bezpečnosti, který byl v létě 2014 schválen Parlamentem ČR a je účinný od 1. 1. 2015[105]. Spolu s tímto zákonem také byly přijaty dvě vyhlášky[106]

Zákon mimo jiné definuje pojem kybernetický prostor, ovšem chybí definice pojmu kybernetické bezpečnosti. Definice absentují i ve Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015, která přijetí zákona v podstatě předpokládá. K interpretaci kybernetické bezpečnosti v české právní úpravě lze využít Výkladového slovníku kybernetické bezpečnosti, podle kterého se jí rozumí *souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.*[107] Podle věcného záměru zákona o kybernetické bezpečnosti je nová právní úprava nutná nejen kvůli přeshraniční povaze kybernetických hrozeb a kvůli závislosti kritické infrastruktury na informačních a komunikačních systémech, ale také kvůli absenci centrální regulace řešení kybernetických útoků a nedostatečnému systému prevence a včasného varování.[108] Proto jsou jako obecné cíle vymezeny především zvýšení bezpečnosti kybernetického prostoru a aktivní spolupráce soukromého a veřejného sektoru a v konkrétní podobě se cíle dotýkají například vybudování práv a povinností jednotlivých subjektů, zajištění mechanismu včasného předávání informací či zlepšení bezpečnosti systémů, které jsou součástí kritické komunikační a informační infrastruktury.

---

[105] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. In: *181/2014*. 2014.

[106] Vyhláška o kybernetické bezpečnosti. In: *316/2014*. 2014 a Vyhláška o významných informačních systémech a jejich určujících kritériích. In: *317/2014*. 2014.

[107] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Česká pobočka AFCEA, 2013, s. 57. ISBN 9788072513970.

[108] NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Věcný záměr zákona o kybernetické bezpečnosti: Návrh pro vnější připomínkové řízení*. 2012.

Z důvodu vytvoření nového pojmového aparátu, specifické oblasti regulace a definování nových práv a povinností subjektů v oblasti kybernetického prostoru se jeví jako účelné nepřistoupení k novelizaci některého ze současných právních předpisů (například krizového zákona), ale přijetí nového zákona. Nově účinný zákon se vztahuje na poskytovatele služeb a provozovatele sítí elektronických komunikací, správce informačního a komunikačního systému kritické informační infrastruktury a správce významného informačního systému. Zákon tak respektuje práva uživatelů služeb a sítí, neboť na ně se jeho působnost přímo nevztahuje, nicméně i uživatelé se podílejí na zajištění kybernetické bezpečnosti (negativně mohou participovat například u struktury sítě botnetů, neboli skupiny počítačů kontrolované z jednoho místa[109]) a je otázkou, nakolik by měli i oni aktivně přispět bezpečnějšímu kyberprostoru. Zákon navíc nevymezuje ani povinnosti výrobců softwaru či hardwaru, kteří by mohli účinně přispívat při řešení kybernetických bezpečnostních událostí a incidentů.[110]

Povinnosti, které zákon výše zmíněným subjektům ukládá, se týkají organizačních a technických opatření, například zvládání kybernetických bezpečnostních událostí a incidentů či nástroje pro ověřování identity uživatelů. Dále jsou stanoveny náležitosti a způsob hlášení kybernetických bezpečnostních incidentů, jsou zde popsána opatření k ochraně kybernetického prostoru a stav kybernetického nebezpečí. Právě možnost ředitele Národního bezpečnostního úřadu vyhlásit stav kybernetického nebezpečí představuje další posun v chápání kybernetických hrozeb vůči státu a jeho integritě.

[109] KLUBAL, Martin. *Problematika sítí typu botnet*. Brno, 2013. Diplomová práce. Mendelova univerzita v Brně, Provozně ekonomická fakulta. Vedoucí práce Ing. Jan Přichystal, Ph.D.

[110] BÁRTÍK, František. Analýza Věcného záměru zákona o kybernetické bezpečnosti. In: *Linux EXPRES* [online]. 2012 [cit. 2015-02-21]. Dostupné z: http://www.linuxexpres.cz/analyza-vecneho-zameru-zakona-o-kyberneticke-bezpecnosti.

5. Úmluva o počítačové kriminalitě

Sestavením textu této Úmluvy [111] byl pověřen Výbor expertů pro kriminalitu v kyberprostoru, který působil v letech 1997 až 2000. Výbor ministrů Rady Evropy Úmluvu v listopadu 2001 schválil a od 23. listopadu téhož roku byla Úmluva zpřístupněna k podpisu. [112] Česká republika ji podepsala v roce 2005 a ratifikovala ji o osm let později, v srpnu 2013. I když se nejedná o právní nástroj Unie, Úmluva reprezentuje i její zájmy, což mimo jiné vyplývá i z pracovního dokumentu útvarů Komise (the Commission Staff Working Paper) z února 2001, ve kterém je zdůrazněna nutnost přednosti unijního práva pro členské státy Unie ve věcech, které upravuje jak unijní právo, tak i Úmluva. Tomu tak má být z důvodu zajištění konzistence přijatých národních opatření a z důvodu zabránění fragmentace vnitřního trhu.[113] Navíc období, kdy byla Úmluva připravována, zároveň odpovídá kromě jiného i souběžně vzrůstající význam elektronického obchodu či duševního vlastnictví. [114] Úmluva se věnuje třem základním oblastem, a to harmonizaci trestního práva hmotného, stejně tak i harmonizaci trestního řízení a mezinárodní spolupráci.

5.1. Hmotné právo Úmluvy

V rámci hmotné právní úpravy jsou trestné činy rozděleny do čtyř kategorií. První z nich jsou trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů, jakým je například nezákonný přístup či zasahování do dat. Druhou kategorií jsou trestné činy související s počítačem, tedy například počítačové padělání, kdy neoprávněně došlo k vkládání, pozměnění, vymazání nebo potlačení počítačových dat v úmyslu, aby byla považovaná za pravá. Elektronické padělání není o mnoho složitější

[111] Úmluva o počítačové kriminalitě. In: *104/2013 Sb.m.s.* 2013, 56.
[112] *Kyberkriminalita a právo*. Vyd. 1. Editor Tomáš Gřivna, Radim Polčák. Praha: Auditorium, 2008, s. 104. ISBN 978-809-0378-674.
[113] *"In their mutual relations, Parties which are members of the European Union shall apply the rules of the European Community and the rules laid down or based on Title VI of the Treaty on European Union, and shall therefore not apply the provisions arising from this Convention except insofar as there are no such rules governing the particular subject concerned."* Dostupné z: http://www.statewatch.org/news/2001/mar/18comm315.htm.
[114] SAVIN, Andrej. *EU internet law*. Cheltenham, UK: Edward Elgar, 2013, xix, 266 pages. Hacking, s. 236. ISBN 9781845429379.

než to klasické. Předně proto, že elektronické dokumenty nejsou obvykle zobrazením papírových dokumentů, ale jsou databází, která může být elektronicky přenášena nebo exportována či konvertována do jiných formátů. Schopnost padělat takový záznam pak závisí na pachatelově schopnosti proniknout do systému, což je zároveň trestným činem první kategorie Úmluvy.[115]

Třetí kategorie trestných činů je spojena s obsahem a je zaměřena na dětskou pornografii. Závažnější povaha tohoto protiprávního jednání se projevuje mimo jiné i ve skutečnosti, že je trestná pouhá držba dětské pornografie na počítači nebo jiném nosiči počítačových dat. Při vymezení objektivní stránky Úmluva také rozlišuje pojmy distribuce a přenášení v závislosti na způsobu šíření, který může spočívat buď v aktivním šíření materiálu, nebo jeho zaslání jiné osobě. Poslední, čtvrtá kategorie, vymezuje trestné činy související s porušením autorského práva a práv jemu příbuzných. S ohledem na rozsáhlou mezinárodní právní úpravu v této oblasti Úmluva odkazuje na mezinárodní smlouvy. Smluvní státy jsou tak povinny dbát svých závazků, které převzaly prostřednictvím mimo jiné Bernské Úmluvy o ochraně literárních a uměleckých děl, Dohody o obchodních aspektech práv k duševnímu vlastnictví a Smlouvy Světové organizace duševního vlastnictví o autorském právu.

Sankce za jednotlivé trestné činy Úmluvy mají respektovat princip účinnosti a proporcionality, měly by zároveň mít odrazující charakter a zahrnout i možnost trestu odnětí svobody. Úmluva také vymezuje povinnost zavedení odpovědnosti právnických osob, která však může být nejen trestní, ale i občanskoprávní či správní. Trestní odpovědnost fyzických osob, které čin spáchaly, ovšem tímto zůstává nedotčena.

5.2. Procesní právo Úmluvy

Každý smluvní stát je povinen zavést pravomoci a postupy stanovené Úmluvou za účelem specifického trestního vyšetřování nebo řízení. Ze článku 14 Úmluvy je patrný zájem mezinárodního společenství o harmonizaci procesního práva

[115] SAVIN, Andrej. *EU internet law*. Cheltenham, UK: Edward Elgar, 2013, xix, 266 pages. Hacking, s. 239. ISBN 9781845429379.

vztahujícího se k počítačové trestné činnosti v širší rovině, neboť tyto pravomoci a postupy se mají vztahovat nejen na trestné činy definované v textu Úmluvy, ale i na jiné trestné činy spáchané prostřednictvím počítačového systému i na zajištění důkazů o trestném činu, které jsou v elektronické formě. Všechny používané pravomoci a postupy mají být nejen v souladu s vnitrostátní právní úpravou, ale také s mezinárodními lidskoprávními dokumenty, jakými jsou například Úmluva Rady Evropy na ochranu lidských práv a základních svobod z roku 1950 či Mezinárodní pakt OSN o občanských a politických právech z roku 1966. Další formou záruky je také soudní nebo jiný nezávislý dohled nad výkonem těchto opatření.

Konkrétní procesní instituty v Úmluvě se zaměřují na urychlené uchování uložených počítačových dat (zejména je-li důvodná obava, že tato počítačová data jsou zvláště ohrožená ztrátou nebo pozměněním) a obdobně i na urychlené zachování či zpřístupnění provozních dat. Dále se jedná o formu příkazu k předložení (buď ve vztahu k osobě a jí drženými počítačovými daty nebo ve vztahu k poskytovateli služby a informacích o odběrateli), přičemž význam tohoto ustanovení je zřetelný i z judikatury Spojených států amerických. Společnost the Recording Industry Asscociation of America se úspěšně dožádala informací o identifikaci osob, které neoprávněně sdílely soubory, od provozovatelů internetových serverů. Povinnost poskytnout takové informace totiž tyto subjekty mají z důvodu poskytování služby na daném území, bez ohledu na jejich sídlo. Poskytované informace zahrnují nejen totožnost uživatele a jeho adresu, ale také technické a časové údaje, typ použité komunikační služby či informace ohledně provedených plateb. Je tedy patrné, že široký rozsah trestných činů je také doprovázen rozsáhlým obsahem příkazu k předložení. Protože je však tento institut teprve postupně využíván, ukáže se až v budoucnu jeho skutečný dopad na úspěšnost v boji proti počítačové kriminalitě.[116]

Dalším procesním nástrojem je prohlídka a zajištění uložených počítačových dat (tedy přístup k počítačovému systému i k médiu s počítačovými daty). Nezbytným požadavkem je osoba nacházející se na území smluvního státu nebo poskytovatel služby nabízející služby na tomto území.

[116] SAVIN, Andrej. *EU internet law*. Cheltenham, UK: Edward Elgar, 2013, xix, 266 pages. Hacking, s. 242. ISBN 9781845429379.

Články 20 a 21 Úmluvy upravují shromažďování provozních dat v reálném čase a odposlech obsahových dat, nicméně v obou těchto případech je možné, aby smluvní stát zúžil jejich aplikaci jen na některé trestné činy, pokud mu jeho vnitrostátní právo neumožňuje aplikaci v celém rozsahu. Protože je ovšem zásadnějším zásahem do soukromí osob odposlech obsahových dat, nesmí být omezení shromažďování provozních dat přísnější než omezení odposlechu dat obsahových.[117]

Soudní pravomoc smluvního státu k trestným činům uvedeným v Úmluvě je dána, pokud je čin spáchán na jeho území, na lodi plující pod jeho vlajkou, na palubě letadla registrovaného podle zákonů tohoto státu či jedním z jeho občanů, pokud je tento čin trestný podle trestního práva v místě, kde byl spáchán, nebo se na dané území nevztahuje územní pravomoc žádného státu.

5.3. Mezinárodní spolupráce

Znění Úmluvy výslovně zdůrazňuje nutnost spolupráce v trestních věcech počítačové kriminality smluvních států v nejširší možné míře. Text upravuje především zásady vydávání pachatelů této trestné činnosti mezi státy a zásady týkající se vzájemné pomoci.[118] Úmluva vytváří právní podklad i v situacích, kdy má vydání proběhnout mezi státy, které mezi sebou smlouvu o vydávání neuzavřely. V takovém případě plní funkci této smlouvy Úmluva pro všechny trestné činy v ní uvedené a zařaditelné do kategorie možné extradice.

5.4. Přednosti a nedostatky Úmluvy

Příprava a aplikace Úmluvy představuje pro boj proti počítačové kriminalitě pozitivní posun. Kritika se ovšem objevuje z několika důvodů. Předně některá z jednání nebyla

[117] *Kyberkriminalita a právo*. Vyd. 1. Editor Tomáš Gřivna, Radim Polčák. Praha: Auditorium, 2008, s. 124. ISBN 978-809-0378-674.

[118] Jednou z možných podob vzájemné pomoci je i tzv. spontánní informace, kdy smluvní strana poskytuje bez předchozí žádosti druhé straně informaci, o které se domnívá, že by mohla pomoci této druhé straně s vyšetřováním či řízením související s počítačovou kriminalitou podle Úmluvy. (Článek 26 Úmluvy)

až do této doby považována za škodlivá a stanovením jejich protiprávnosti vznikla rigidní opatření, která nejsou schopna dostatečně rychle reagovat na stále se vyvíjející médium.[119] Například článek 6 Úmluvy stanoví za trestný čin výrobu či zpřístupnění počítačového hesla, přístupového kódu nebo podobných dat, pomocí nichž lze získat přístup do celého počítačového systému nebo do jakékoli jeho části. Ovšem existuje mnoho počítačových programů, které sice neoprávněný přístup umožňují, avšak zároveň je možné je využívat, aniž by došlo k protiprávnímu jednání. Takový stav však znemožňuje jejich další užívání a vývoj. Rovněž sporným ustanovením je příkaz k předložení, zmíněný výše, který umožňuje vyžadování specifikovaných počítačových dat. I když toto procesní ustanovení je nezbytné pro účinný boj proti počítačové kriminalitě, představuje i rizika spojená se zásahy do soukromí.

Naopak jednoznačně pozitivní přínos Úmluvy spočívá kromě jiného v činnosti sítě pro nepřetržité kontakty v oblasti trestné činnosti páchané s využitím špičkové techniky. Členy této sítě je značný počet států, včetně členských států Unie.[120] Praktický přínos spočívá zejména v usnadnění shromažďování důkazů, poskytování právních informací a lokalizování podezřelých osob.[121] V neposlední řadě Úmluva umožňuje sjednocení těch klíčových skutkových podstat trestných činů, které souvisejí s počítačovou kriminalitou, usnadňuje proto mezinárodní postih, a představuje tak převzetí odpovědnosti na mezinárodní úrovni.

5.5. Důsledky Úmluvy a její posuzování po více než deseti letech od ratifikace

Úmluva, která byla zhotovena před více než deseti lety, představuje značný posun ve sjednocování právní úpravy bezpečného kyberprostoru v mezinárodním měřítku. Smluvní státy jsou povinny definovat ve své legislativě určitá jednání za trestné činy, vybavit justici účinnými prostředky procesního práva, například výše zmíněným

[119] SAVIN, Andrej. *EU internet law*. Cheltenham, UK: Edward Elgar, 2013, xix, 266 pages. Hacking, s. 245. ISBN 9781845429379.
[120] *SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ A EVROPSKÉMU VÝBORU REGIONŮ k obecné politice v boji proti počítačové kriminalitě*. 2007. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:CS:HTML.
[121] Článek 35 Úmluvy

urychleným uchováním uložených počítačových dat, a podílet se na efektivní mezinárodní spolupráci v policejní a justiční oblasti. Úmluva byla již v roce 2003 doplněna o Dodatkový protokol o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů[122].

Podle pracovního plánu výboru Úmluvy[123], vytvořeného na období od 1. 1. 2014 do 31. 12. 2015, jsou prioritními cíli podpora ratifikace Úmluvy dalšími státy, což kromě politického dialogu znamená i zajištění potřebné technické podpory, dále dohled nad implementací Úmluvy smluvními státy a v neposlední řadě také zvážení nutnosti dalšího dodatkového protokolu se zaměřením na přeshraniční přístup k počítačovým datům. Nespornými přednostmi Úmluvy je především zapojení států napříč kontinenty do diskuse o bezpečném kybernetickém prostoru, dále tlak na státy, aby novelizovaly své právní normy vztahující se ke kyberzločinům, zdokonalení technické spolupráce na mezinárodní úrovni a přijímání nových procesních institutů. Na druhou stranu v případě některých států se ukázala problematickou skutečnost, že Úmluva byla přijata na poli Rady Evropy, nikoliv Organizací spojených národů, a že se tyto státy neúčastnily přípravy textu Úmluvy.[124] Tuto skutečnost již samozřejmě nelze nijak zpětně napravit, ovšem státy se mohou podílet na dialogu ohledně interpretace jednotlivých ustanovení a přípravě dodatkových protokolů. O něco závažnější se ukazuje otázka tvorby nových mezinárodních úmluv týkajících se kybernetické bezpečnosti či informační společnosti. Úmluva se totiž vztahuje ke kyberzločinům a souvisejícím justičním otázkám, ať již z oblasti hmotného či procesního práva, nicméně státy hovoří o potřebě bezpečného kybernetického prostoru v politicko-vojenském kontextu, a je možné, že tato potřeba vyústí v přípravu nové mezinárodní dohody.[125]

[122] Sdělení Ministerstva zahraničních věcí o sjednání Dodatkového protokolu k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. In: *9/2015*. 2015, roč. 2015, 9.

[123] CYBERCRIME CONVENTION COMMITTEE (T-CY). *T-CY Workplan*. Strasbourg, 2013. Dostupné z: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)24%20workplan%202014-15_v7adopted.pdf.

[124] SEGER. The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is a web. In: *Council of Europe* [online]. 2012 [cit. 2015-01-31]. Dostupné z: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/AS_UNISPAweb_V6_16feb12.pdf.

[125] SEGER. The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is a web. In: *Council of Europe* [online]. 2012 [cit. 2015-01-31]. Dostupné z:

Samostatnou kapitolou je otázka skutečné implementace Úmluvy do právního řádu smluvních států, neboť vymáhání takového pochybení spočívá na mezinárodní spolupráci a není upraveno dostatečně účinně.[126] Rozdíly se projevují také mezi konkrétní podobou procesních nástrojů, například pokud jde o podobu prohlídky a zajištění uložených počítačových dat. Je nicméně samozřejmé, že k zajištění bezpečnějšího kyberprostoru je nezbytná především aktivní role států samotných, větší míra odpovědnosti na straně soukromých subjektů a podpora dalšího technologického pokroku. Úmluva v tomto směru figuruje především jako jednotící prvek a dává prostor dalšímu zdokonalování mezinárodní spolupráce a sjednocování právní úpravy především ve vztahu ke kyberzločinům, ale lze předpokládat, že i ve vztahu bezpečného kybernetického prostoru jako takového.

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/AS_UNISPAweb_V6_16feb12.pdf.

[126] MARION, Nancy. The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation. In: *International journal of cyber criminology*. India: International journal of cyber criminology, 2010, s. 699-712. 4. ISSN 0974-2891.

6. Porovnání strategických dokumentů kybernetické bezpečnosti USA a EU

6.1. Úvod

Hlavní částí této práce je porovnání strategických dokumentů USA a Unie v oblasti kybernetické bezpečnosti a následné porovnání některých právních předpisů navazujících na tyto strategické dokumenty. Za účelem přehlednějšího rozboru jsem zvolila metodu SWOT[127], pomocí které jsem vyzdvihla klíčové znaky jednotlivých dokumentů. Ty jsou jednotlivě popsány, stručně vysvětleny a porovnány se znaky ostatních dokumentů. Následně je pomocí SWOT analýzy rozebrána i Úmluva, která je v závěru porovnána s výše zmíněnými strategickými dokumenty.

6.2. Strategie USA a Evropské unie

K porovnání zpracování strategické úrovně jsem zvolila tři dokumenty, konkrétně Národní strategii ochrany kyberprostoru USA, Mezinárodní strategii pro kyberprostor USA a strategii Evropské unie Otevřený, bezpečný a spolehlivý kybernetický prostor. První z uvedených vychází z následující SWOT analýzy.

[127] Analýza silných a slabých stránek, příležitostí a hrozeb. Zkratka se skládá z počátečních písmen anglických slov *strengths, weaknesses, opportunities, threats*.

Schéma č. 1 Národní strategie ochrany kyberprostoru USA

SILNÉ STRÁNKY	**SLABÉ STRÁNKY**
zaměření na kritickou infrastrukturu	absence vytyčených cílů pro následnou revizi
obsáhnutí pěti základních priorit ke zlepšení kybernetické bezpečnosti	nepřesně definována odpovědnost jednotlivých úřadů
zvýraznění možnosti teroristických útoků na informační sítě USA	absence vypočtení nákladů a potřebných zdrojů pro financování
PŘÍLEŽITOSTI	**HROZBY**
spolupráce veřejného a soukromého sektoru	nedostatek dobrovolného zapojení soukromého sektoru
rozvoj mezinárodní spolupráce	nedostatečné sdílení informací mezi federálními úřady subjekty soukromého sektoru
podpora vzdělávání	nekonkrétnost kroků k odstraňování zranitelnosti systému
propojení s ostatními strategickými dokumenty	

Národní strategie ochrany kyberprostoru se zaměřuje na kybernetické hrozby kritické infrastruktury a zdůrazňuje závislost služeb na kybernetickém prostoru. Poměrně komplexně hned z počátku došlo k vymezení pěti základních pilířů strategie, které odpovídají potřebě v co největším rozsahu redukovat riziko rychlých a anonymních útoků, ať již provedených teroristy, zločinci nebo státy. Ústředním subjektem majícím primární odpovědnost za zajištění kybernetické bezpečnosti (tedy její přiměřené úrovně) je Ministerstvo vnitřní bezpečnosti. Podrobnější informace ale již v tomto ohledu neuvádí a navíc není zcela jasné, zda dohled nad informační bezpečností federální vlády vykonává Ministerstvo vnitřní bezpečnosti nebo Úřad pro řízení a rozpočet, který některé ze svých zákonem svěřených pravomocí převedl na Ministerstvo vnitřní bezpečnosti.[128]

Další zajímavou skutečností je, že i když tato strategie byla vydána již v roce 2003, stále nebyla nahrazena. To mimo jiné dokládá fakt, že strategie konkrétně nevymezuje krátkodobé, střednědobé a dlouhodobé cíle, které by následně v příslušných časových

[128] UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE. *National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*. 2013. Dostupné z: http://www.gao.gov/assets/660/652170.pdf.

intervalech revidovala. Již sama strategie uvádí potřebu národního kybernetického plánu obnovy infrastruktury, ovšem blíže neuvádí právní závaznost dokumentu, jeho obsah či časový horizont vytvoření. V roce 2011 vydala federální agentura pro zvládání krize (FEMA) pokyny[129], jak dosáhnout účinné obnovy po mimořádné události. Poněkud překvapuje, že tento úřad podléhající Ministerstvu vnitřní bezpečnosti ve zmíněných pokynech neobsáhl případ kybernetického útoku a zaměřuje se na revitalizaci zdravotních, sociálních, ekonomických a environmentálních struktur. Je ale zřejmé, že v pokynech vymezené principy, spolupráce mezi zúčastněnými subjekty a rozdělení plánu obnovy na jednotlivé fáze lze vztáhnout i na kybernetické útoky. Domnívám se, že tento uvedený případ deklaruje nedostatečnou návaznost dokumentů v oblasti kybernetické bezpečnosti.

Mezi stále aktuální příležitosti, které dokument obsahuje, patří především rozvoj mezinárodní spolupráce, který koresponduje s požadavkem druhého amerického dokumentu Mezinárodní strategie pro kyberprostor. USA v oblasti kybernetické bezpečnosti implementovaly model účasti všech subjektů (tzv. *multistakeholder goverance model*), tedy jak odpovědnost veřejného sektoru, tak i soukromého, občanské společnosti a akademické obce. Oproti tomu některé státy, například Rusko nebo Čína, by upřednostnily regulaci ze strany jednoho subjektu, například agenturou OSN Mezinárodní telekomunikační unie, a více pravomocí svěřených jednotlivým vládám států. [130] USA by proto měly pravidelně aktualizovat své strategické dokumenty s odkazem na model účasti všech, aby zůstávalo srozumitelné, že tento postoj nebyl změněn.

Spolupráce veřejného a soukromého sektoru v této strategii lze uchopit z hlediska SWOT analýzy jako příležitost i jako hrozbu. Je zřejmé, že podpora výzkumu a vzdělávání ve sféře kybernetické bezpečnosti je velmi pokročilá, což dokládá například činnost pittsburghského střediska NCFTA *(the National Cyber –Forensics*

[129] *National Disaster Recovery Framework: Strengthening Disaster Recovery for the Nation*. 2011. Dostupné z: http://www.fema.gov/media-library-data/20130726-1820-25045-5325/508_ndrf.pdf.

[130] EICHENSEHR, Kristen. The US Needs a New International Strategy for Cyberspace. In: *Just Security* [online]. 2014 [cit. 2015-02-21]. Dostupné z: http://justsecurity.org/17729/time-u-s-international-strategy-cyberspace/.

and Training Alliance)[131], které spolupracuje s bezpečnostními sbory, soukromým sektorem i akademickou obcí. Na druhé straně strategie nevymezuje spolehlivý způsob předávání informací mezi federálními úřady a klíčovými soukromými subjekty (zejména vlastníky prvků kritické infrastruktury), ani způsob varování v případě mimořádné události.

Schéma č. 2 Mezinárodní strategie pro kyberprostor USA

SILNÉ STRÁNKY	**SLABÉ STRÁNKY**
vybudování základních principů	nejasné konkrétní zapojení USA v zajištění spolupráce s ostatními státy
závazek mezinárodní spolupráce	nezdůrazněna potřeba transparentnosti vytvářených norem
PŘÍLEŽITOSTI	**HROZBY**
použití všech přípustných prostředků k zajištění obrany	opuštění modelu zapojení všech subjektů
podpora rozvoje informačních technologií v jiných státech	nedostatečná definice činu agrese
vytváření a rozvoj pravidel chování v kyberprostoru	

Mezinárodní strategie pro kyberprostor USA se opírá o model zapojení všech subjektů do zajišťování bezpečného kyberprostoru, stejně jako uvedená předchozí strategie, a tudíž je i zde platná potřeba časté aktualizace (a protože se jedná o strategii mezinárodní, lze dokonce konstatovat, že je tento požadavek ještě důležitějším). USA se v této strategii zavazují k nalezení konsensu ohledně otázky, jaké právní normy chování v kyberprostoru jsou platné. Strategie uznává platnost mezinárodního práva i v kybernetické sféře, ovšem zároveň vymezuje potřebu je přizpůsobit specifickým znakům síťové technologie. Základem těchto norem je podle strategie řada fundamentálních principů, ať se již jedná o respektování základních lidských práv a svobod, vlastnického práva, ochranu před trestnými činy nebo právo na sebeobranu státu. Zde se zároveň nachází jedna z dosud nevyřešených otázek strategie, neboť v dokumentu se hovoří o právu na sebeobranu státu v případě určitých aktů

[131] The NCFTA: Combining Forces to Fight Cyber Crime. In: *The FBI* [online]. 2011 [cit. 2015-02-21]. Dostupné z: http://www.fbi.gov/news/stories/2011/september/cyber_091611.

agrese v kybernetickém prostoru. Co se těmito akty rozumí, již ale vysvětleno není. Rovněž by bylo příhodné, aby obsah právních norem kybernetického prostoru, které jsou předmětem diplomatických i jiných debat a mají být mezinárodně platné, byl transparentní, a mohl tak být předem probírán i v rámci akademické obce či širší veřejnosti. Obsah těchto norem totiž strategie nevymezuje.[132]

Ve své strategii se USA zavazují pomoci vybudovat pozitivní právo, přispět k bezpečným a otevřeným síťovým technologiím a zajistit společnou, mezi státy sdílenou odpovědnost za bezpečný kyberprostor. K dosažení těchto cílů mají USA využívat především diplomatickou cestu, cestu obrany a rozvoje. Jednou z konkrétních cest, jak dochází k naplňování cílů, je například snaha USA o rozšíření smluvních států Úmluvy, a tím docílení jednotné právní úpravy kyberzločinů. Jednou z největších příležitostí je zřejmě závazek USA přispívat k předávání znalostí, technologií či jiných zdrojů státům, které takovým zázemím nedisponují. Spolupráce se navíc neomezuje pouze na předávání dovedností či výzkumných pokroků, ale též na mezinárodní školení či sdílení nejlepších postupů. Dokladem tohoto závazku bylo například společné cvičení USA a Unie Cyber Atlantic 2011.

Na druhou stranu není zcela zřejmé, jakým způsobem se USA chtějí angažovat v oblasti mezinárodní spolupráce v případě, že některé státy, například Čína, nejsou zatím ochotny v kybernetických otázkách spolupracovat.[133]

[132] EICHENSEHR, Kristen. The US Needs a New International Strategy for Cyberspace. In: *Just Security* [online]. 2014 [cit. 2015-02-21]. Dostupné z: http://justsecurity.org/17729/time-u-s-international-strategy-cyberspace/.

[133] EICHENSEHR, Kristen. The US Needs a New International Strategy for Cyberspace. In: *Just Security* [online]. 2014 [cit. 2015-02-21]. Dostupné z: http://justsecurity.org/17729/time-u-s-international-strategy-cyberspace/.

Schéma č. 3 Strategie EU

SILNÉ STRÁNKY	**SLABÉ STRÁNKY**
návrh příslušné legislativy	absence definic používaných pojmů
naléhání na členské státy za účelem ratifikace a implementace Úmluvy	zaměření na koordinaci na národní úrovni na úkor prohloubení úrovně nadnárodní
komplexní zapojení národních a unijních subjektů	
PŘÍLEŽITOSTI	**HROZBY**
přenesení odpovědnosti za sběr a sdílení informací procesu posuzování rizik jednotlivých členských států na jeden unijní úřad	odlišná či chybějící právní úprava v jednotlivých členských státech
podpora vědy a výzkumu v kybernetickém prostoru	nedostatečné zázemí technologií, závislost na neunijních státech
obnova důvěry občanů v bezpečný kybernetický prostor a rozšiřování povědomí o souvisejících rizicích	

V úvodu Strategie EU jsou vymezeny základní principy kybernetické bezpečnosti, o které se Unie opírá. Jedná se sdílení stejných hodnot a právních norem jak ve fyzickém, tak i ve virtuálním světě, ochranu základních práv a svobod, především pak ochranu svobody projevu a soukromí, a dále o sdílenou odpovědnost za bezpečný kyberprostor. Strategie EU by ovšem také měla hned v úvodu definovat základní pojmy, především pojem kybernetická bezpečnost, protože každý členský stát může pojem interpretovat odlišně a zahrnout pod něj odlišné složky. Někdy může být kladen důraz na informační systémy, jindy například na obranu a krizové řízení. Tato nejednotnost je o to důležitější, že ne všechny členské státy již přijal svoji strategii ke kybernetické bezpečnosti (v současnosti strategii přijalo jen 18 členských států, dále čtyři státy – Irsko, Švédsko, Řecko a Kypr jsou ve fázi přípravy strategie[134]) a právě společná unijní strategie by měla různé právní úpravy sjednocovat.

Jedním z hlavních úkolů Strategie EU je rozvoj legislativy vztahující se ke kyberzločinům. Příkladem může být její odkaz na směrnici Evropského

[134] National Cyber Security Strategies in the World. In: *European Union Agency for Network and Information Security* [online]. 2013 [cit. 2015-02-21]. Dostupné z: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii, jejíž text je v současnosti projednáván v Evropském parlamentu. Dalším zřejmým úkolem je rozšiřování povědomí o rizicích kybernetického prostoru například zapojením univerzitních studentů do soutěží, organizováním měsíce kybernetické bezpečnosti či rozšířením odpovědnosti soukromého sektoru za zajištění této bezpečnosti.

Ve slabých stránkách SWOT analýzy je uvedena primární koordinace na národní úrovni oproti prohlubování nadnárodní úrovně. Odborník na bezpečnostní otázky Evropské unie Dr. Krzysztof Sliwinski v tomto kontextu upozornil na nedostatek panevropské vize. *„Co limituje Evropskou unii nejvíce v kybernetické bezpečnosti, je její mezivládní charakter a odpovídající nedostatek kolektivní vize ze strany členských států.“*[135] Autor upozorňuje na podobu s oblastí spravedlnosti a vnitřních věcí, neboť státy nejsou vždy ochotny sdílet citlivé informace či ponechávat své suverénní pravomoci Unii. Je ovšem zřejmé, že přeshraniční povaha kyberzločinů a potřeba zajistit bezpečný kyberprostor komplexně odůvodňuje potřebu nadnárodního přístupu.

6.3. SWOT analýza Úmluvy

Schéma č. 4 Úmluva

SILNÉ STRÁNKY	**SLABÉ STRÁNKY**
harmonizace trestního práva hmotného	rigidita sporných ustanovení
úprava nových procesních institutů	neúčinnost vymáhání implementace Úmluvy
mezinárodní spolupráce	
PŘÍLEŽITOSTI	**HROZBY**
rozšíření mezinárodní postihu	zásahy do soukromí jednotlivců
ratifikace Úmluvy dalšími státy	nezapojení významných států, z hlediska kybernetické bezpečnosti, do Úmluvy
definování bezpečného kyberprostoru	narušení státní suverenity

[135] Krzysztof Feliks Sliwinski (2014) *Moving beyond the European Union's Weakness as a Cyber-Security Agent*, *Contemporary Security Policy*, 35:3, 480, DOI: 10.1080/13523260.2014.959261 (překlad vlastní)

Význam Úmluvy spočívá v přiblížení k jednotné právní úpravě hmotné i procesní upravující kyberzločiny. Převzetí odpovědnosti za bezpečný kyberprostor jednotlivými státy znamená společný přístup na mezinárodní úrovni, sdílení informací a obecně zdokonalování spolupráce, například v případě předávání pachatelů počítačové trestné činnosti. Úmluva tedy představuje příležitost nejen k zapojení dalších států světa do boje s kyberzločiny, a tím k unifikaci právních řádů států celého světa ohledně trestnosti vymezených jednání, ale také se může rozšířit ve strategicko-politickém kontextu a definovat principy bezpečného kyberprostoru. Úmluva k němu sice bezpochyby přispívá, ovšem primárně sleduje trestní úhel pohledu.

V právní úpravě kyberzločinů je častou otázkou dostatečná aktualizace a sledování pokroku v technologii, což se pochopitelně vztahuje i k textu Úmluvy a například již zmíněné výrobě či zpřístupnění počítačového hesla, přístupového kódu nebo podobných dat, pomocí nichž lze získat přístup do celého počítačového systému nebo do jakékoli jeho části. Smluvních států Úmluvy, které do současné chvíle přijaly její text, je v současné chvíli 44[136]. Mezi nimi ovšem chybí některé ze států, které by mohly významně přispět k problematice kybernetického bezpečí, například Rusko nebo Čína. Mnoho států považuje Úmluvy za dokument spíše regionální povahy a zejména v případě neúčasti na tvorbě podoby textu Úmluvy odmítají její následnou ratifikaci. [137] Zároveň Úmluva negarantuje účinné vymáhání implementace jejích ustanovení do právních řádů členských států, tedy je nutné se opírat především o mezinárodní diplomacii a o činnost výboru Úmluvy, který podle již zmíněného pracovního plánu má dohlížet na přijetí jednotlivých ustanovení. Dále může představovat problém možné narušení soukromí za účelem současné ochrany kyberprostoru, při použití příkazu k zatčení. Balancování mezi těmito právy je typickým problémem dnešní doby a Úmluva jasně odkazuje na ochranu lidských práv a svobod, včetně práva na ochranu soukromí a osobních dat.

[136] Convention on Cybercrime. In: *CETS No.: 185*. 2004. Dostupné z: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG.

[137] CHANG. *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait*. UK: Edward Elgar Publishing, 2012, s. 125. ISBN 9780857936684.

6.4. Závěr vyplývající z porovnání strategických dokumentů

Všechny výše zmíněné strategické dokumenty sdílejí princip odpovědnosti všech subjektů, odkazují na základní principy a ochranu hodnot a pojímají problematiku poměrně komplexně, neboť obsahují jak zlepšování odolnosti kybernetického prostoru a s tím související omezení kyberzločinů, tak podporu technologického výzkumu či spolupráci soukromého a veřejného sektoru. Strategie EU obsahuje poměrně konkrétní úkoly, zadané jednotlivým subjektům (ať již na národní či na unijní úrovni), zatímco Národní strategie ochrany kyberprostoru USA odkazuje primárně na Ministerstvo vnitřní bezpečnosti a rozložení odpovědnosti za splnění cílů není zcela zřejmé, ovšem Strategie EU naopak postrádá celistvý pohled na kybernetickou bezpečnost, když nedefinuje samotný pojem a nedává tak konkrétní obsah pro strategické dokumenty jednotlivým členským státům. Obdoba absence definice se projevuje i u Mezinárodní strategie pro kyberprostor USA, když zmiňuje možné použití prostředků obrany, je-li proveden kybernetický akt agrese, nicméně již dále pojem agrese nevymezuje.

Shoda všech strategických dokumentů je v případě odkazu na Úmluvu a připomenutí závazku přimět ostatní státy k její ratifikaci a implementaci. USA se navíc zavazují k vytváření závazných pravidel chování v kybernetickém prostoru, byť by jejich podoba měla podléhat veřejné diskusi a obsah chystaných norem by měl být více transparentní. Strategie EU na tento závazek USA reaguje požadavkem na Evropskou komisi a vysokého představitele Unie pro zahraniční věci a bezpečnostní politiku, kteří mají ve spolupráci se členskými státy podpořit rozvoj těchto norem, současně ale Unie nepředpokládá potřebu nových mezinárodních právních nástrojů k řešení kybernetických problémů.

O nákladech či zdrojích, které by měly cíle strategií financovat, žádná ze strategií nehovoří. Je pochopitelné, že předběžné vyčíslení nákladů je obtížné, nicméně z důvodu návaznosti na rozpočet a efektivnost plánovaných opatření by bylo žádoucí rozvrhnout předpokládané disponibilní částky klíčovým aktivitám či z jakých zdrojů by mohly být financovány. Pokud jde o konkrétní aktivity, domnívám se, že Strategie EU obsahuje celou řadu konkrétních úkonů, které mají být za účelem

bezpečnějšího kyberprostoru provedeny, a bylo by příhodné, kdyby podrobnější rozpracování obsáhly rovněž uvedené americké strategie, zároveň by tak lépe navazovaly na strategie jiných oblastí. Návaznost na jiné dokumenty na strategické úrovni pokládám za nedostatečnou jak v USA, tak v Unii, neboť zcela chybí výslovné propojení těchto dokumentů pomocí odkazů či stanovení priorit napříč různými oblastmi.

Všechny výše zmíněné dokumenty se důsledně zaměřují na potřebu ochrany kritické infrastruktury, která je vysoce propojená s kybernetickým prostorem, a proto značně ohrožena z hlediska kybernetických útoků. A také všechny tři strategické dokumenty dbají o rozšiřování povědomí soukromého sektoru a občanské společnosti o rizicích kybernetického prostoru.

7. Porovnání vybraných právních předpisů kybernetické bezpečnosti

Tato kapitola se blíže zabývá některými právními předpisy souvisejícími s kybernetickou bezpečností, které byly přijaty na federální úrovni v USA a na nadnárodní úrovni v Evropské unii. Cílem je zhodnotit zaměření těchto závazných právních předpisů a tedy identifikace priorit v kybernetickém prostoru a následné porovnání jednotlivých přístupů.

7.1. Právní předpisy kybernetické bezpečnosti USA

Základním právním předpisem vztahujícím se ke kyberzločinům je CFAA. Tento předpis vymezuje trestná jednání, se kterými jsou spojeny tresty od peněžité pokuty po nepodmíněný trest odnětí svobody. V souvislosti s tímto zákonem se ovšem také ukazuje problém absence definice pojmů *přístup* a *neoprávněný*, a ani judikatura dosud pojmy přesně nevymezila.[138] Například termín *neoprávněný* vyvolal akademickou polemiku v trestním řízení proti Lori Drewové.[139] Drewová šikanovala třináctiletou dívku prostřednictvím falešného účtu na sociální síti MySpace, dívka se po sérii útočných zpráv oběsila. Drewová byla obviněna z porušení zákazu přístupu k počítači bez oprávnění (překročení mezí oprávnění), kterého se dopustila v úmyslu získávat osobní informace o oběti a následně je využívat k citovému týrání. Porota shledala Drewovou vinnou, nicméně soudce Wu vyhověl žádosti obviněné a viny ji zprostil. Své rozhodnutí zdůvodnil tak, že je nepřípustné vztáhnout trestní odpovědnost i na porušení smluvních podmínek webové stránky, neboť takový posun by zjednal CFAA příliš vágním a tedy neplatným. Vytvoření falešného účtu představuje porušení smluvních podmínek sociální sítě (jednalo se o neoprávněné užití služby), nicméně běžný občan nemůže předpokládat, že tak může být vystaven i trestnímu stíhání. Navíc by

[138] HERNACKO, Andrew. A Vague Law in i Smartphone World: Limiting the Scope of Unauthorized Access under the Computer Fraud and Abuse Act. In: *American University Law Review*. 61, no. 5, 2012, s. 1543-1584.
[139] U.S. v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009)

připuštěním této cesty byla nezákonně dána pravomoc vlastníku webové stránky přesně určit, které jednání je trestným.

Podobnou situaci řešilo americké právo v jiném případě.[140] David Nosal, zaměstnanec soukromé společnosti zaměřené na vyhledávání nových zaměstnanců, byl obviněný z porušení ustanovení CFAA, protože před ukončením svého pracovního poměru stáhl z počítače zaměstnavatele celou řadu kontaktních údajů a tímto jednáním porušil pravidla společnosti. Nosal upozornil, že CFAA míří především na počítačové pachatele, a navíc tvrdil, že ani nemohl jednat bez oprávnění nebo přesáhnout své oprávnění, protože jako zaměstnanec společnosti byl oprávněn těmito údaji disponovat. Soud v daném případě dospěl k závěru, že přesah oprávněného přístupu podle CFAA lze uplatnit, neboť obviněný porušil omezení zaměstnavatele v přístupu k údajům. Taková interpretace ovšem není ve shodě s předchozím judikátem, což vyplývá i ze stanoviska disentující soudkyně Campbell. Podle ní daný rozsudek zjednává CFAA příliš vágním. Rozhodnutí je velmi diskutabilní, protože vznik trestně právní odpovědnosti za porušení pravidel obchodní společnosti představuje značné rozšíření pravomocí zaměstnavatele při tvorbě vlastních pravidel.

V prosinci 2014 americký Kongres schválil hned celou řadu zákonů směřujících k ochraně kybernetické bezpečnosti. Jeden z nich, zákon o ochraně národní kybernetické bezpečnosti, se mimo jiné také zabývá sdílením informací, což bylo svěřeno jako jeden z hlavních úkolů centru NCCIC. Zákon již ovšem nepamatuje na právní ochranu společností, které informace vládnímu sektoru poskytují. Tyto informace jsou mnohdy citlivé, součástí obchodního tajemství, nebo se společnosti v souvislosti s těmito informacemi mohou obávat narušení důvěryhodnosti ve svůj informační systém. Navíc původní návrh zákona obsahoval přímý odkaz na zákon o bezpečnosti[141], který poskytuje právní ochranu prostřednictvím Ministerstva vnitřní bezpečnosti antiteroristickým technologiím, nicméně tento odkaz již ve schváleném znění zákona není.[142] Zůstává tedy otázkou, nakolik úspěšné bude sdílení informací v této oblasti mezi soukromým a veřejným sektorem.

[140] U.S. v. Nosal, 642 F.3d 781 (9th Cir. 2011)
[141] *Safety Act*
[142] Congress Takes Action on Stalled Cybersecurity Legislation in Final Days of the 113th Congress. In: *Hunton & Williams LLP* [online]. 2014 [cit. 2015-02-22]. Dostupné

Další z nově přijatých zákonů, zákon o posílení kybernetické bezpečnosti, zvýrazňuje vliv Národního institutu standardů a technologie, neboť i když je pro soukromé společnosti stále jen dobrovolné převzetí jeho požadavků, lze předpokládat, že v brzké době se tak stane běžnou součástí postupu každého subjektu, tedy nejen v případě vlastníků prvků kritické infrastruktury. Tento předpoklad lze také podpořit nabídnutou možností soudům opřít svá argumentační tvrzení právě o standardy tohoto institutu. I tak se ale podle mého názoru jeví jako účelné přeměnit institut v regulační orgán, jehož výchozí normy by byly závazné pro soukromý i veřejný sektor. Při přijetí série nových zákonů došlo ke zrušení povinnosti správních úřadů každoročně vyplňovat kontrolní zprávu, která dokládá, jaké konkrétní kroky byly přijaty k zajištění vyšší úrovně jejich systémů informační technologie. Nyní je tímto přezkumem pověřeno Ministerstvo vnitřní bezpečnosti, které má rovněž ostatním úřadům pomoci zmírňovat rizika kybernetických hrozeb. Vysoce pozitivní trend spatřuji v činnosti Národního počítačového soudního institutu, který proškoluje členy justice a policie a také v obecném nárůstu expertů zaměřujících se na kybernetické hrozby.

7.2. Právní předpisy kybernetické bezpečnosti EU

I když je nesporné, že problematika bezpečného kyberprostoru se v unijním právu stala jednou z priorit, stále vzbuzuje celou řadu otázek. Hned zpočátku je nutné připomenout citlivé spojení trestních věcí se suverenitou členských států, které představuje částečnou překážku pro harmonizaci jednotlivých právních úprav. Lisabonská smlouva přesto hovoří o sbližování trestního práva, což se projevuje stanovením minimálních pravidel v přijatých směrnicích. Nutnost jednotného přístupu a užší vztah mezi vnitrostátním a unijním právem přiznal i SDEU. Kromě toho tuto shodnou právní úpravu vyžaduje také řešení některých otázek společného trhu, nadnárodní spolupráce v trestních věcech a přeshraniční povaha kybernetického prostoru.

---

z:http://www.hunton.com/files/News/20c17d1d-fe88-445e-b7ef-3c27d6386271/Presentation/NewsAttachment/1afcfadb-7589-4b45-b956-3dd4b847c10f/congress-passes-four-cybersecurity-bills.pdf.

Konkrétními unijními nástroji jsou dnes směrnice o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii a směrnice o útocích proti informačním systémům. Podle posledně zmíněné směrnice jsou členské státy povinny stanovit za trestný čin úmyslný neoprávněný přístup k informačnímu systému, pokud tím bylo porušeno bezpečnostní opatření a zároveň se nejedná o méně závažný případ. Interpretace pojmu *méně závažný* je ponechána na úvaze každého státu. Směrnice pamatuje i na nové metody, které jsou při kybernetických útocích využívány, například vytváření a používání botnetů, nicméně samotná schopnost softwaru vytvářet botnety nesmí být kriminalizována, neboť i takový nástroj může sloužit zákonným účelům. Směrnice stanovuje minimální tresty ke čtyřem kategoriím jednání, a to za neoprávněný přístup k informačním systémům, neoprávněné zasahování do informačních systémů, neoprávněné zasahování do údajů a neoprávněné sledování údajů. Zároveň zdůrazňuje potřebu spolupráce soukromého a veřejného sektoru, zejména pokud jde o identifikaci pachatelů a zachování fungování informačních systémů.

Nedostatečné zajištění spolupráce napříč sektory a nejasné dělení odpovědnosti za bezpečný kyberprostor však nadále zůstává předmětem kritiky. S tím souvisí i stále neuspokojivá úroveň vzdělání občanské společnosti, ale i zástupců policejních složek či justice v oblasti kyberzločinů. Jedním z kroků, který by opět posunul stávající situaci, by mohlo být přijetí navrhované směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii[143]. Důraz by tak byl kladen na odolnost informačních systémů nejen pro případy úmyslných bezpečnostních incidentů, a to včetně teroristických útoků, ale také pro případy přírodních pohrom či lidských chyb. Směrnice také zdůrazňuje význam výměny informací (a za tímto účelem by mělo být zřízeno pouze jedno vnitrostátní kontaktní místo), podpory výzkumu a zhotovení národních strategií pro bezpečnost sítí a informací.

Závěrem je nutné připomenout i prioritu ochrany lidských práv a svobod, zejména pokud jde o ochranu osobních údajů, která je v unijních předpisech zcela zřejmá.

[143] Legislativní usnesení Evropského parlamentu ze dne 13. března 2014 o návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii. In: *2013/0027(COD)*. 2014. Dostupné z: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0244&language=CS&ring=A7-2014-0103.

Přesto se dostala do problematické situace, a to kvůli směrnici Evropského parlamentu a Rady 2006/24/ES [144], která se týkala otázky uchovávání údajů o elektronických komunikacích. SDEU svým rozhodnutím ze dne 8. 4. 2014 učinil tuto směrnici neplatnou.[145] Ve svém zdůvodnění upozornil na dopad směrnice na každou osobu, každý prostředek elektronické komunikace a na všechny provozní údaje, aniž by byly stanoveny odlišné podmínky, omezení nebo výjimky. Problematickým bodem je především absence požadavku souvislosti mezi uchovanými údaji a ohrožením veřejné bezpečnosti, absence objektivního kritéria přístupu úřadů k údajům a absence objektivních kritérií pro určení doby uchovávání údajů. Ochrana soukromí je bezesporu výsadním právem každého člověka, nicméně vývoj informačních technologií a přibývající kybernetické hrozby rovněž znamenají větší míru odpovědnosti států (ale i každého jednotlivého subjektu) a tedy i potřebu o něco rozsáhlejší regulace a podrobnější trestní hmotněprávní i procesní úpravy.

7.3. Závěr vyplývající z porovnání právních předpisů USA a EU

Při porovnání právních dokumentů USA a Unie je nutné mít na paměti rozdílnou podobu těchto dvou celků. V případě USA, tedy konkrétně tamní federální úrovně, lze poukázat na razantní zaměření na kybernetickou oblast v závěru roku 2014. Právě tato legislativní reforma značí upřednostnění kybernetických otázek, a i když nevytváří nové kybernetické nástroje pro boj proti kyberzločinům, poměrně komplexně sjednocuje standardy informačních systémů subjektů soukromého i veřejného sektoru a otázku sdílení informací. Obdobný posun, i když v menším měřítku, lze pozorovat i v uznání potřeby unijní harmonizace právních řádů v trestních otázkách kyberprostoru a v přijetí výše zmíněných směrnic. Úroveň bezpečnosti informačních systémů členských států se ale stále značně liší a připravenost států na kybernetické hrozby není rovnocenná. Spolupráce v postihu kyberzločinů je sice rozvíjena mimo jiné

[144] 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 (Úřední věstník EU č. L 105 z 13. 4. 2006).

[145] Rozsudek Soudního dvora (velkého senátu) 8. dubna 2014, ve spojených věcech C-293/12 a C-594/12

i prostřednictvím nově zřízeného Evropského kybernetického centra, ovšem úroveň povědomí občanské společnosti a odborné znalosti příslušníků veřejné správy, zástupců justice a bezpečnostních sborů neodpovídá rozsahu kybernetických hrozeb a jejich aktuálnosti. Domnívám se, že by jako určitý vzor mohl posloužit Národní počítačový soudní institut USA. Zatím nejasné zůstává stanovení hranice ochrany osobních údajů a zájmy státu na postihu trestného jednání. V tomto kontextu lze předpokládat, že bude přijata nová směrnice nahrazující již neplatnou směrnici 2006/24/ES, která bude respektovat požadavky SDEU a nebude obsahovat předchozí příliš obecná ustanovení.

8. Pracovní skupina EU-USA pro kybernetickou bezpečnost a kyberkriminalitu

Na listopadovém summitu Unie a USA roku 2010, konaném v Lisabonu, došlo k vytvoření pracovní skupiny, zaměřené primárně na oblast kybernetické bezpečnosti a kyberkriminality. Skupina se skládá ze čtyř týmů, přičemž každý z týmů se specializuje na konkrétní oblast. Jedná se o management kybernetických mimořádných událostí (*cyber incident management*), o spolupráci veřejného a soukromého sektoru (*public-private partnership*), o zvyšování povědomí v dané oblasti (*awareness raising*) a o kyberzločiny (*cybercrimes*).[146] Experti pracovní skupiny transatlantickou vazbu skutečně posílili. V roce 2011 proběhlo cvičení Cyber Atlantic, které bylo touto skupinou iniciováno, a které si kladlo především za cíl zjistit, na jaké oblasti kybernetického prostoru by se měla spolupráce Unie a USA zaměřit. Pracovní skupina také zorganizovala celou řadu seminářů pro soukromý a veřejný sektor, které se orientovaly především na řídicí systémy, inteligentní sítě a na zapojení dalších subjektů do zvyšování povědomí v rámci kybernetického prostoru. Je třeba podotknout, že celá řada americko-evropských seminářů proběhla ještě před vznikem této pracovní skupiny, například v roce 2007 se ve státě Illinois v USA konal seminář s účastí čtyřiceti zástupců z USA a Unie na téma závislosti systémů na kybernetickém prostoru a problematiky jeho bezpečnosti[147], ovšem tato forma spolupráce byla spíše neformální, nestálá a méně intenzivní.

Dalšími úspěchy této skupiny se staly podpis deklarace zakládající Globální alianci proti zneužívání dětí na internetu a kontinuální práce na zvyšování úrovně bezpečnosti doménových jmen a IP adres. Současný důraz je kladen na skupinu zabývající se zvyšováním povědomí o kybernetickém prostoru, dále na stanovení norem řízení rizik, správu útoků formou botnetů a na podporu Úmluvy. Navíc je tento pracovní orgán zprostředkovatelem transatlantického dialogu, koordinuje další setkání, semináře

[146] MANN, Michael. EU-US cooperation on cyber security and cyberspace. In: *Evropská služba pro vnější činnost* [online]. Brussels, 2014 [cit. 2015-02-21]. Dostupné z: http://www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf.

[147] CLARKE, Jim a Thomas SKORDAS. Second EU-US Workshop on Secure, Dependable and Trusted ICT Infrastructures. In: *ERCIM NEWS* [online]. 2007 [cit. 2015-02-22]. Dostupné z: http://ercim-news.ercim.eu/en70/european-scene/second-eu-us-workshop-on-secure-dependable-and-trusted-ict-infrastructures.

a konference a podílí se na vytváření pravidel pro on-line sledování za obchodními účely. Součástí činnosti je také spolupráce s celou řadou dalších orgánů, z nichž klíčové místo zaujímají americké bezpečnostní sbory a Evropské kybernetické centrum EC3.

8.1. Dialog mezi USA a Evropskou unií

26. března 2014 bylo na bruselském summitu přijato rozhodnutí o posílení spolupráce mezi Evropskou unií a USA v různých otázkách kybernetické bezpečnosti, v oblasti mezinárodního vývoje této oblasti a v příslušných otázkách mezinárodní politiky. Toto rozhodnutí bylo přijato nikoliv proto, že by předtím scházela dostatečná forma spolupráce, ale proto, že tato setkání probíhala neformálně a byla součástí politických záležitostí zahraničních a bezpečnostních jako takových. Výsledkem summitu se stala každoroční schůze vysokých představitelů Unie a USA, která má představovat prostor pro diskuse a strategické plánování ve čtyřech základních oblastech. První z nich je mezinárodní kybernetický vývoj, druhou podpora a ochrana lidských práv online, třetí sférou jsou otázky související s politicko-vojenskou problematikou a s mezinárodní bezpečností a poslední, čtvrtou oblastí je budování kybernetické bezpečnosti ve třetích státech.

Potřeba dialogu vyvstala rovněž v oblasti politiky a správy informačních a komunikačních technologií, včetně Internetu. Odborníci, kteří se zaměřují na tuto problematiku, se scházejí přibližně jedenkrát ročně a zabývají se otázkami souvisejícími například se sdílením hardwarových a softwarových prostředků pomocí sítě (*cloud computing*)[148] či s elektronickým zdravotnictvím (*eHealth*). Tyto otázky jsou kromě toho také řešeny například v Transatlantické ekonomické radě.[149] Právě tato rada

[148] *Cloud computing* [online]. 2010 [cit. 2015-02-22]. Dostupné z: http://www.cloudcomputing.cz/.
[149] MANN, Michael. EU-US cooperation on cyber security and cyberspace. In: *Evropská služba pro vnější činnost* [online]. Brussels, 2014 [cit. 2015-02-21]. Dostupné z: http://www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf.

významnou měrou posiluje ekonomickou integraci a ve své sekci Inovace a technologie se zaměřuje právě na elektronické zdravotnictví.[150]

8.2. Cvičení Cyber Atlantic

Dne 3. listopadu 2011 proběhlo v Bruselu první společné cvičení Evropské unie a USA Cyber Atlantic 2011 zaměřené na počítačovou bezpečnost. O rok dříve proběhlo celoevropské cvičení Cyber Europe 2010 v rámci ochrany evropské kritické informační infrastruktury, bylo možné tak navázat na předchozí zkušenosti. Cvičení Cyber Atlantic se zúčastnilo přes dvacet členských států Unie, každý byl zastoupen třemi odborníky, z nichž vždy jeden byl nominován jako moderátor. Každá skupina obdržela nezbytné informace o problému (formou novinových článků, dopisů ze strany vládních představitelů apod.). Cvičení probíhalo jeden den a skládalo se ze dvou různých situací. V té první skupina hackerů provedla cílený počítačový útok (tzv. *Advanced Persistent Threat*) na tajné informace bezpečnostních agentur členských států Unie, které následně byly zveřejněny, a USA byly požádány o spolupráci v řešení této krizové situace. Některé kybernetické agentury již skupinu sledovaly, a to téměř rok, tudíž předávaly informace dalším členským státům a USA. V druhé situaci museli počítačoví odborníci řešit narušení systému dohledu, řízení a získávání údajů v elektrárenských zařízeních (tzv. *Supervisory Control and Data Acquisition).*[151] V přípravě na cvičení se podílely především Evropská agentura pro bezpečnost sítí a informací a americké Ministerstvo vnitřní bezpečnosti. Cvičení bylo v podstatě výzkumné povahy, neboť odborníci měli během něj sami prozkoumat a určit zásadní body, jak zlepšit pomoc členských států Unie v případě kybernetického útoku v USA a naopak, a také byla předpokládána bezprostřední výměna znalostí a dovedností na mezinárodní úrovni.

[150] EU-USA - Transatlantic Economic Council. In: *European Commission* [online]. 2013 [cit. 2015-02-22]. Dostupné z: http://ec.europa.eu/enterprise/policies/international/cooperating-governments/usa/transatlantic-economic-council/index_en.htm.

[151] V Bruselu proběhlo první společné cvičení EU a USA v oblasti počítačové bezpečnosti Cyber Atlantic 2. In: *CSIRT.CZ* [online]. 2011 [cit. 2015-02-22]. Dostupné z: https://www.csirt.cz/page/959/v-bruselu-probehlo-prvni-spolecne-cviceni-eu-a-usa-v-oblasti-pocitacove-bezpecnosti-cyber-atlantic-2/.

Výsledkem cvičení bylo konstatování, že při řešení počítačových útoků nadnárodní povahy je nezbytné využití dostupných moderních technologií a komunikačních prostředků a je potřeba zajistit, aby všechny státy měly povědomí o těchto možnostech. Dále byl podtržen značný význam hlubšího zapojení ze strany odborné (tedy IT odborníků), ze strany policejních služeb a jiných bezpečnostních sborů a také ze strany politické. Dalším důležitým zjištěním byla možnost usnadnění spolupráce mezi Unií a USA, pokud by bylo v Unii vytvořeno jedno centrální kontaktní místo. Účastníci i pozorovatelé shledali cvičení jako jednoznačně užitečné (na škále od 1 do 4, kde 1 znamenala *zcela neužitečné* a 4 znamenala *rozhodně užitečné,* ohodnotili hráči i moderátoři cvičení známkou 3,7 a pozorovatelé dokonce známkou 4[152]). Obecně lze konstatovat, že realizace těchto či podobných cvičení je velmi potřebná.

Ředitelka Agentury pro výzkum pokročilých obranných projektů Regina Dugan po realizaci cvičení sdělila, že armáda potřebuje větší množství moderních informačních prostředků, aby byla schopna čelit kybernetickým hrozbám ohrožujícím celou řadu průmyslových oblastí, včetně automobilového průmyslu. Podle ní moderní vedení války vyžaduje účinné použití kybernetických zbraní, kinetických zbraní i jejich kombinace. Kybernetické útoky totiž mohou poškodit nejen počítačový, ale také fyzický, hmotný systém, včetně vojenského.[153]

8.3. Spolupráce s Evropskou agenturou pro bezpečnost sítí a informací

Vznik Evropské agentury pro bezpečnost sítí a informací (dále „ENISA“) a její činnost jsou upraveny nařízeními Evropského parlamentu a Rady č. 460/2000 a 526/2013. Jejím účelem je předcházení a řešení problémů souvisejících s bezpečností sítí a informací. Její činnost zahrnuje zapojení Unie jako celku, jednotlivých členských států i spolupráci soukromého a veřejného sektoru. ENISA organizuje celoevropská cvičení, stejně

[152] CYBER ATLANTIC 2011: 1 st joint EU-US Cyber Exercise. In: *Building International Cooperation for Trustworthy ICT* [online]. 2011 [cit. 2015-02-22]. Dostupné z: http://www.bic-trust.eu/files/2011/12/slides15.pdf.

[153] EU and US conduct cyber attack response exercise. In: *Regulatory Cyber Security: The FISMA Focus IPD* [online]. 2011 [cit. 2015-02-22]. Dostupné z: http://www.thecre.com/fisma/?p=769.

jako se podílela na přípravě cvičení Cyber Atlantic 2011. Také připravila dvě mezinárodní konference zaměřené na spolupráci při kybernetických krizích, v roce 2012 v Paříži a v roce 2013 v Athénách. Na těch se kromě jiného probíraly případové studie, technické aspekty kybernetických cvičení či spolupráce v rámci krizového managementu.

Spolu s USA ENISA dále zorganizovala otevřený seminář k posílení transatlantické spolupráci v oblasti kybernetické bezpečnosti řídicích systémů, který se konal 15. října 2012. Účastníci semináře reprezentovali například Ministerstvo vnitřní bezpečnosti USA, Evropskou Komisi, společnost Microsoft, Honeywell či Siemens. Tento seminář také posloužil jako zázemí v přípravě Strategie a Akčního plánu kybernetické bezpečnosti řídicích systémů a inteligentních sítí, který vytvářely Evropská Komise a americké Ministerstvo vnitřní bezpečnosti za podpory agentury ENISA a jednotlivých členských států Unie. Tyto semináře pomáhají rozvíjet nejlepší způsoby ochrany kritické infrastruktury za současného snižování počtu zranitelných míst a umožňují výbornou platformu pro sdílení informací a zkušeností v přípravě na kybernetické útoky. Nespornou výhodou těchto akcí je také zapojení subjektů ze soukromého sektoru a akademické obce.

8.4. Globální aliance proti zneužívání dětí na internetu

Jedním ze zvláště citlivých témat, která se objevují ve spojitosti s kyberzločiny, je pohlavní zneužívání dětí na internetu. Rozhodla jsem se ve své práci zmínit právě tuto oblast, neboť aliance států bojující proti těmto trestným činům vznikla na základě společné iniciativy USA a Evropské unie. Států účastnící se této aliance je v současnosti padesát čtyři. Jedním z hlavních závazků, které jsou její součástí, je zaměření se na identifikaci obětí a zajištění potřebné pomoci a ochrany a také zvýšené úsilí v odhalování těchto případů a odhalení pachatelů. Vznik aliance je datován k prosinci 2012, kdy byly též zveřejněny konkrétní závazky států. Na pozvání Komisařky Evropské unie pro vnitřní záležitosti Cecilie Malmströmové a ministra spravedlnosti USA Erica Holdera se konala v září 2014 ministerská konference, na které byly posuzovány dosavadní výsledky aliance a navrženy postupy do budoucna. Jedním

z nich je například zákonná úprava umožňující snazší získání elektronických informací a důkazů ze strany poskytovatelů internetového připojení či z jiných zdrojů, dále je také možné zmínit usnadnění rychlé a komplexní výměny informací vztahujících se k přeshraničním trestným činům, k obětem či skupině pachatelů mezi bezpečnostními sbory.

8.5. Summity 2014 dotýkající se problematiky kyberzločinů

Dne 26. března 2014 se v Bruselu konal summit USA – EU. Cílem tohoto setkání bylo potvrzení silné spolupráce mezi těmito celky. USA i Evropská unie sdílejí stejné hodnoty, jakými jsou demokracie, lidská práva a svobody či vláda práva. Transatlantická spolupráce byla připomenuta v celé řadě oblastí, například v otázce územní integrity Ukrajiny či v ekonomické a obchodní sféře, stejně jako v oblasti kybernetického prostoru. Na summitu byla zdůrazněna potřeba otevřeného, bezpečného a spolehlivého internetu a rovněž byla potvrzena skutečnost, že lidská práva jsou platná nejen v běžném světě, ale i v prostředí online. Dále bylo poukázáno na expertní spolupráci mezi USA a Unií, a to především skrze Pracovní skupinu EU-USA pro kybernetickou bezpečnost a kyberkriminalitu a její politický úspěch, jakým je vytvoření Globální aliance proti zneužívání dětí na internetu.

Tento summit také zdůraznil potřebu ratifikace a implementace Úmluvy a potřebu zesílení spolupráce Unie a NATO právě v oblasti kybernetické bezpečnosti.[154] Pokud jde o spolupráci Unie a NATO, lze zmínit například i bruselskou konferenci ze září 2014. Je nutné ovšem podotknout, že i přes nesporné úspěchy Pracovní skupiny EU-USA pro kybernetickou bezpečnost a kyberkriminalitu, podobné cíle se objevily i na předcházejícím summitu, konaném ve Washingtonu v roce 2011, především pokud jde o požadavek ratifikace Úmluvy. Je pochopitelné, že summit se dotýká celé řady různých problematik a nemůže stavět podrobné požadavky, přesto se domnívám, že by na této strategické úrovni bylo vhodné vymezit konkrétní požadavky v oblasti kybernetické bezpečnosti.

[154] U.S.-EU Summit in Brussels. In: *United States Mission to the European Union* [online]. 2014 [cit. 2015-02-22]. Dostupné z: http://useu.usmission.gov/useu_summit_brussels_032614.htm.

Dne 3. listopadu 2014 v německém Bonnu proběhl transatlantický summit zaměřený na kybernetickou bezpečnost. Primárně se zabýval otázkami ochrany kritické infrastruktury a střetu práv na soukromí s potřebou zpravodajských služeb a prevence kyberzločinů. Tohoto summitu se kromě Unie a USA zúčastnili také zástupci NATO či soukromých společností, například společnosti Siemens. Výsledky summitu ukazují, že nic takového jako absolutní bezpečí v rámci Internetu neexistuje, nicméně je třeba učinit pravidla bezpečného chování v oblasti kyberprostoru stejně známými a běžnými jako je tomu například u pravidel řízení vozidel na pozemních komunikacích. Také byla zdůrazněna potřeba výměny informací o bezpečnostních mimořádných událostech mezi společnostmi navzdory skutečnosti, že žádná z nich nechce připustit, že se stala obětí kybernetického útoku. Důležitá je dostatečná transparentnost, větší ochota riskovat a financování rizikovým kapitálem. Zajímavé výsledky měla čtvrtá pracovní skupina summitu.[155] Podle ní trvá společnostem průměrně více než sedm měsíců zjištění kybernetického útoku na jejich informační systém, přičemž software, podle závěrečné zprávy, v průměru obsahuje pět chyb. Primárním cílem by tak neměla být blokace hackerů, ale identifikace slabin a zjišťování, kdo již narušil jejich systémy. Zařízeními, do kterých se hackeři nejsnáze dostanou, jsou podle Rika Fergusona, reprezentanta společnosti Trend Micro, chytré telefony. S přihlédnutím k faktu, že hackeři se vystavují jen minimálním rizikům a jsou zástupci v dnešní době lukrativního podnikání, je boj proti kyberzločinům velmi obtížný. Jedním z příspěvků k řešení by mohlo být například častější využívání kódování, které je stále málo rozšířené.[156]

[155] Cyber Security Summit 2014 – Documentation of the working groups. In: *CyberSecurity Summit* [online]. 2014 [cit. 2015-02-22]. Dostupné z: http://cybersecuritysummit.de/downloads/CSS_2014_Ergebnisse_Arbeitsgruppe_4_englisch.pdf.

[156] Cyber Security Summit 2014 – Documentation of the working groups. In: *CyberSecurity Summit* [online]. 2014 [cit. 2015-02-22]. Dostupné z: http://cybersecuritysummit.de/downloads/CSS_2014_Ergebnisse_Arbeitsgruppe_4_englisch.pdf.

9. Závěr

Tato práce předkládá ucelenější pohled na programové dokumenty kybernetického prostoru a na ně navazující právní předpisy USA a Unie. Není možné podat úplný výčet související právní úpravy, ale bylo nutné zaměřit se na klíčové texty, jejichž podstatou je předcházet a postihovat kyberzločiny. Tyto vybrané dokumenty jsou posouzeny jak v politickém kontextu, tak s ohledem na judikaturu a transatlantickou spolupráci. Je totiž zřejmé, že rozvíjející se spolupráce se bude zásadněji podílet na tvorbě a novelizaci těchto dokumentů. Razantní vývoj kybernetického prostoru vybízí k časté opětovné revizi již platných předpisů, a proto tato práce poukazuje na přednosti a nedostatky dané právní úpravy obou porovnávaných celků, i s ohledem na Úmluvu o počítačové kriminalitě jako mezinárodní pramen práva.

Strategické dokumenty USA a Unie, které se vztahují k problematice kyberzločinů a zajištění bezpečného kybernetického prostoru, zdůrazňují potřebu ratifikace a implementace Úmluvy. Význam Úmluvy spatřuji především v postupném sjednocování trestněprávní úpravy hmotné i procesní a postupu mezinárodní spolupráce jak formou výměny informací, tak i skrze postih pachatelů kyberzločinů. Zůstává ovšem otázkou, zda-li pojetí Úmluvy bude vyhovovat i požadavkům politického pojetí kybernetického prostoru, který Úmluva jako takový nedefinuje a primárně jej ani neřeší, neboť se orientuje především na trestní pohled. Současně s touto otázkou také vyvstává potřeba aktualizace některých bodů, například v podobě zmíněného dodatkového protokolu, který by se blíže věnoval přeshraničnímu přístupu k počítačovým datům. Právě forma dodatkových protokolů umožňuje zapojení celého mezinárodního společenství, a touto cestou, nikoliv tvorbou nových dokumentů pro ochranu kyberprostoru, by mohla být odstraněna výtka některých států, že se nepodílely na tvorbě textu Úmluvy.

Základní dokumenty, které byly předmětem studia v této diplomové práci, jsou stále značně nejednotné v terminologii. Některé pojmy definovány nejsou zcela, například v případě Strategie EU a pojmu kybernetická bezpečnost, což z důvodu rozsáhlé abstraktnosti pojmu znamená odlišnou interpretaci dalšími subjekty. Toto, stejně jako vágní určení odpovědnosti za zajištění bezpečného kyberprostoru, považuji za zásadní

nedostatek dokumentů. I když je nepochybné, že přístup USA i Unie se opírá o model odpovědnosti a zapojení všech subjektů, který klade důraz na spolupráci veřejného a soukromého sektoru, není zřejmé, jakou konkrétní podobu má tento model mít. Zatímco USA odkazují na Ministerstvo vnitřní bezpečnosti, Unie se zaměřuje především na národní úroveň (a odkazuje na odpovědnost států), zatímco nadnárodní je spíše upozaděna. Předpokládám, že postupná celosvětová ratifikace Úmluvy ukazuje mimo jiné současnou potřebu sdílení bezpečného kyberprostoru, mezinárodní spolupráce a jednotné politiky. Navíc se domnívám, že Lisabonská smlouva i judikatura SDEU předpokládá užší vztah vnitrostátního a unijního práva v oblasti kyberzločinů a postupné přijímání směrnic a jejich implementace v členských státech dokládá postupné sbližování právní úpravy.

Nedávné přijetí konkrétních právních předpisů v USA upravující otázky kybernetického prostoru dokládá vysoce aktivní přístup ze strany státu a uchopení problematiky z více úhlů pohledu, mimo jiné i ze strany snazšího sdílení informací. Právě na odpovídající sdílení informací se zaměřuje i evropská právní úprava, nicméně ani v jedné není dostatečně garantováno aktivní zapojení soukromých subjektů, které se při hlášení kybernetických incidentů mohou cítit svázány obavou o svá obchodní tajemství či narušení své důvěryhodnosti. Bližší právní úprava by také mohla více vymezit povinnosti konkrétních zapojených subjektů, včetně například softwarových a hardwarových výrobců.

S ohledem na aktuálnost problémů souvisejících s ochranou kybernetického prostoru zdůrazňuje právní úprava Unie i USA potřebu zajištění vysoké úrovně bezpečnosti informačních systémů, znalostí zaměstnanců veřejné správy i soukromého sektoru a dostatečnou informovanost občanské společnosti. Již zmíněný Národní počítačový soudní institut v USA je příkladem vzdělávání policistů, státních zástupců či soudců v otázkách kyberzločinů a kybernetické bezpečnosti. Stejně tak je klíčové i zvyšování povědomí o kybernetických rizicích u všech fyzických i právnických osob. Právě zde také vyvstává otázka ochrany osobních údajů a přílišná intervence ze strany veřejné moci. Je samozřejmé, že nalezení rovnováhy mezi zájmem na bezpečný kybernetický prostor a postih kyberzločinů a zájmem na respektování základních lidských práv

a svobod není jednoduché, nicméně je nutné si uvědomit, že bez garance určité úrovně bezpečného kyberprostoru nemůže stát zajistit ani respektování osobních svobod.

Nepochybným pozitivním přínosem je posilování spolupráce Unie a USA, zejména prostřednictvím Pracovní skupiny EU-USA pro kybernetickou bezpečnost a kyberkriminalitu. Mezi úspěchy této pracovní skupiny patří mimo jiné cvičení Cyber Atlantic z roku 2011, které pomohlo určit další zaměření euroatlantické spolupráce, dále vytvoření Globální aliance proti zneužívání dětí na internetu a také organizování každoročních schůzek nejen odborníků na kybernetické otázky, ale také vysokých představitelů USA i Unie. Úzká spolupráce byla potvrzena i na summitech konaných v uplynulém roce 2014, neboť USA i Unie sdílejí stejné hodnoty a snaží se přispět jak otevřenému, bezpečnému a spolehlivému internetu, tak ochraně lidských práv. Spolupráce by nicméně mohla být o něco užší, zejména pokud jde o tvorbu společných dokumentů, a bylo by žádoucí realizovat více seminářů či cvičení za účelem sdílení informací, technologií a zkušeností. Z předchozího porovnání právních norem je zřejmé, že byly dosaženy značné výsledky v oblasti kybernetické bezpečnosti a prevence kyberzločinů, ale vzhledem k mimořádně rychlému rozvoji technologií a potřebě komplexního řešení se ukazuje jako nezbytná nutnost užší spolupráce při efektivním zdokonalování právních textů.

Bibliografie

Knižní zdroje

Kyberkriminalita a právo. Vyd. 1. Editor Tomáš Gřivna, Radim Polčák. Praha: Auditorium, 2008. ISBN 978-809-0378-674.

BUCKLAND, Michael Keeble. *Information and information systems: fundamentality, diversity and unification*. New York: Praeger, 1991, xv. World Scientific series in information studies. ISBN 02-759-3851-4.

BUONO, Laviero. Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (EC3). In: *New journal of European criminal law*. 2012. ISSN 2032-2844.

BURGIN, Mark. *Theory of information: fundamentality, diversity and unification*. Hackensack, N.J.: World Scientific, 2010, xvi. ISBN 9789812835499.

HERNACKO, Andrew. A Vague Law in i Smartphone World: Limiting the Scope of Unauthorized Access under the Computer Fraud and Abuse Act. In: *American University Law Review*. 61, no. 5, 2012, s. 1543-1584.

CHANG. *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait*. UK: Edward Elgar Publishing, 2012. ISBN 9780857936684.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Česká pobočka AFCEA, 2013. ISBN 9788072513970.

JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007. Hacking. ISBN 978-802-4715-612.

KLUBAL, Martin. Problematika sítí typu botnet. Brno, 2013. Diplomová práce. Mendelova univerzita v Brně, Provozně ekonomická fakulta. Vedoucí práce Ing. Jan Přichystal, Ph.D.

MARION, Nancy. The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation. In: International journal of cyber criminology. India: International journal of cyber criminology, 2010, s. 699-712. 4. ISSN 0974-2891.

PLOUG, Thomas. *Ethics in cyberspace how cyberspace may influence interpersonal interaction*. Dordrecht: Springer, 2009. ISBN 978-904-8123-704.

ROSS, Jeffrey Ian. *Cybercrime*. New York: Chelsea House, 2010. ISBN 978-143-8117-980.

SAVIN, Andrej. *EU internet law: the transformation of crime in the information age*. Reprint. Cambridge: Polity, 2007. ISBN 9781781006016.

TICHÝ, Luboš. *Evropské právo*. 5., přeprac. vyd. V Praze: C.H. Beck, 2014, xlii, 756 s. Academia iuris (C.H. Beck). ISBN 978-80-7400-546-6.

WALL, David S. *Cybercrime: the transformation of crime in the information age*. Reprint. Cambridge: Polity. ISBN 978-074-5627-359.

Právní předpisy

Legislativní usnesení Evropského parlamentu ze dne 13. března 2014 o návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii. In: 2013/0027(COD). 2014. Dostupné z: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0244&language=CS&ring=A7-2014-0103.

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. Věcný záměr zákona o kybernetické bezpečnosti: Návrh pro vnější připomínkové řízení. 2012.

Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii. In:2013/0027/COD. 2013. Dostupné z: http://eur-lex.europa.eu/procedure/EN/202368.

Rámcové rozhodnutí Rady 2005/222/SVV o útocích proti informačním systémům. (Úřední věstník EU č. L 69 z 16. 3. 2005).

Sdělení Ministerstva zahraničních věcí o sjednání Dodatkového protokolu k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. In: *9/2015*. 2015, roč. 2015, 9.

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 (Úřední věstník EU č. L 105 z 13. 4. 2006).

Směrnice Evropského parlamentu a Rady 2013/40/EU o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV. (Úřední věstník EU č. L 218/8 z 12. 8. 2013).

Smlouva o Evropské unii; Smlouva o fungování Evropské unie

Strategie pro oblast kybernetické bezpečnosti ČR a období 2012-2015.

Úmluva o počítačové kriminalitě. In: *104/2013 Sb.m.s.* 2013, 56.

USA. Cybersecurity Enhancement Act of 2014. In: S. 1353 (113th). 2014.

USA. Cybersecurity Workforce Assessment Act. In: H.R. 2952 (113th). 2014.

USA. National Cybersecurity Protection Act of 2014. In: S. 2519 (113th). 2014.

Usnesení Evropského parlamentu ze dne 22. listopadu 2012 o kybernetické bezpečnosti a ochraně.

Vyhláška o kybernetické bezpečnosti. In: 316/2014. 2014.

Vyhláška o významných informačních systémech a jejich určujících kritériích. In: 317/2014. 2014.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. In: 181/2014. 2014.

Soudní judikatura

Rozsudek Soudního dvora ze dne 11. listopadu 1981, trestní řízení proti Guerrinu Casatiovi, C- 203/80.

Rozsudek Soudního dvora ze dne 16. června 1998, trestní řízení proti Johannovi Martinovi Lemmensovi, C – 226/97.

Rozsudek Soudního dvora ze dne 16. června 2005, trestní řízení proti Marii Pupino, C – 105/03.

Rozsudek Soudního dvora ze dne 13. září 2005, Komise Evropských společenství proti Radě Evropské unie, C – 176/03.

Rozsudek Soudního dvora (velkého senátu) 8. dubna 2014, ve spojených věcech C-293/12 a C-594/12.

Rozsudek U.S. v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009)

Rozsudek U.S. v. Nosal, 642 F.3d 781 (9th Cir. 2011)

Internetové zdroje

Annual Report 2013. In: *European Defence Agency* [online]. 2014 [cit. 2015-02-15]. Dostupné z: http://www.eda.europa.eu/info-hub/publications/publication-details/pub/annual-report-2013.

BÁRTÍK, František. Analýza Věcného záměru zákona o kybernetické bezpečnosti. In: *Linux EXPRES* [online]. 2012 [cit. 2015-02-21]. Dostupné z: http://www.linuxexpres.cz/analyza-vecneho-zameru-zakona-o-kyberneticke-bezpecnosti.

CLARKE, Jim a Thomas SKORDAS. Second EU-US Workshop on Secure, Dependable and Trusted ICT Infrastructures. In: *ERCIM NEWS* [online]. 2007 [cit. 2015-02-22]. Dostupné z: http://ercim-news.ercim.eu/en70/european-scene/second-eu-us-workshop-on-secure-dependable-and-trusted-ict-infrastructures.

Congress Takes Action on Stalled Cybersecurity Legislation in Final Days of the 113th Congress. In: *Hunton & Williams LLP* [online]. 2014 [cit. 2015-02-22]. Dostupné z: http://www.hunton.com/files/News/20c17d1d-fe88-445e-b7ef-3c27d6386271/Presentation/NewsAttachment/1afcfadb-7589-4b45-b956-3dd4b847c10f/congress-passes-four-cybersecurity-bills.pdf.

Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime. In: Official website of the European Union [online]. 2000 [cit. 2014-03-16]. Dostupné z:http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193b_en.htm.

CYBER ATLANTIC 2011: 1 st joint EU-US Cyber Exercise. In: *Building International Cooperation for Trustworthy ICT* [online]. 2011 [cit. 2015-02-22]. Dostupné z: http://www.bic-trust.eu/files/2011/12/slides15.pdf.

CYBERCRIME CONVENTION COMMITTEE (T-CY). *T-CY Workplan*. Strasbourg, 2013. Dostupné z: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)24%20workplan%202014-15_v7adopted.pdf.

Cybersecurity. In: *The White House* [online]. 2015 [cit. 2015-01-24]. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

Cyber Security Summit 2014 – Documentation of the working groups. In: *CyberSecurity Summit* [online]. 2014 [cit. 2015-02-22]. Dostupné z: http://cybersecuritysummit.de/downloads/CSS_2014_Ergebnisse_Arbeitsgruppe_4_englisch.pdf.

Cybersecurity Results. In: *The Department of Homeland Security* [online]. 2013 [cit. 2015-01-24]. Dostupné z: http://www.dhs.gov/cybersecurity-results.

DAHL, Matt. Understanding the New Federal Cyber Laws. In: *Security Magazine* [online]. 2015 [cit. 2015-01-26]. Dostupné z: http://www.securitymagazine.com/articles/86057-understanding-the-new-federal-cyber-laws.

Digitální program pro Evropu. In: *Oficiální webové stránky Evropské unie* [online]. 2010 [cit. 2015-01-24]. Dostupné z: http://europa.eu/legislation_summaries/information_society/strategies/si0016_cs.htm.

EICHENSEHR, Kristen. The US Needs a New International Strategy for Cyberspace. In: *Just Security* [online]. 2014 [cit. 2015-02-21]. Dostupné z: http://justsecurity.org/17729/time-u-s-international-strategy-cyberspace/.

EU approach to cyber-security. In: *Evropský parlament*[online]. 2014 [cit. 2015-01-25]. Dostupné z: http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140775/LDM_BRI%282014%29140775_REV1_EN.pdf.

EU-USA - Transatlantic Economic Council. In: *European Commission* [online]. 2013 [cit. 2015-02-22]. Dostupné z: http://ec.europa.eu/enterprise/policies/international/cooperating-governments/usa/transatlantic-economic-council/index_en.htm.

EUROPEAN COMMISSION. *European Cybercrime Centre – one year on*. Brussels, 2014 [cit. 2015-01-25]. Dostupné z: http://europa.eu/rapid/press-release_IP-14-129_en.htm.

EUROPEAN PARLIAMENT - DIRECTORATE- GENERAL FOR INTERNAL POLICIES.*Developing a Criminal Justice Area in the European Union*. Brussels, 2014.

HABIB, Jessica. Cyber Crime and Punishment: Filtering Out Internet Felons. *Fordham*

Intellectual Property, Media and Entertainment Law Journa. 2004, Volume XIV, Book 4. Dostupné z: http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1290&context=iplj.

HRONEK, Jiří. *Informační systémy* [online]. Olomouc, 2007 [cit. 2015-01-24]. Dostupné z: http://phoenix.inf.upol.cz/esf/ucebni/infoSys.pdf. Učební text. Univerzita Palackého.

Johnson, David R. and Post, David G., Law and Borders - The Rise of Law in Cyberspace. Stanford Law Review, Vol. 48, 1996, s. 1370-1371. Dostupné z SSRN: http://ssrn.com/abstract=535 or http://dx.doi.org/10.2139/ssrn.535.

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. In: 2013. Dostupné z: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

KLIMEK, Libor. Combating Attacks against Information Systems: EU Legislation and its Development. *Masaryk University Journal of Law and Technology*. 2012, č. 1. Dostupné z: http://mujlt.law.muni.cz/view.php?cisloclanku=2012070007.

Krzysztof Feliks Sliwinski (2014) *Moving beyond the European Union's Weakness as a Cyber-Security Agent, Contemporary Security Policy*, 35:3, 480, DOI: 10.1080/13523260.2014.959261 (překlad vlastní)

LEVIN, Avner a Daria ILKINA. *International Comparison of Cyber Crime*. Toronto, Canada, 2013. Dostupné z: http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf. Ryerson University.

MALMSTRÖM, Cecilia. Next step in the EU - US cooperation on Cyber security and Cybercrime. In:*European Commission* [online]. 2013 [cit. 2015-01-24]. Dostupné z: http://europa.eu/rapid/press-release_SPEECH-13-380_en.htm.

MANN, Michael. EU-US cooperation on cyber security and cyberspace. In: *Evropská služba pro vnější činnost* [online]. Brussels, 2014 [cit. 2015-02-21]. Dostupné z: http://www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf.

MAY, Maxim. Federal Computer Crime Laws. *SANS Institute* [online]. 2004, s. 2-4 [cit. 2015-01-24]. Dostupné z: http://www.sans.org/reading-room/whitepapers/legal/federal-computer-crime-laws-1446?show=federal-computer-crime-laws-1446&cat=legal.

MEADE, Catlin a Susan CASSIDY. FISMA Updated and Modernized. In: *Covington's Government Contracts* [online]. 2014 [cit. 2015-01-24]. Dostupné z: http://www.insidegovernmentcontracts.com/2014/12/fisma-updated-and-modernized/.

MINISTERSTVO OBRANY USA. *Department of Defense Strategy for Operating in Cyberspace*. 2011. Dostupné z: http://www.defense.gov/news/d20110714cyber.pdf.

National Cyber Security Strategies in the World. In: *European Union Agency for Network and Information Security* [online]. 2013 [cit. 2015-02-21]. Dostupné z: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

National Disaster Recovery Framework: Strengthening Disaster Recovery for the Nation. 2011. Dostupné z: http://www.fema.gov/media-library-data/20130726-1820-25045-5325/508_ndrf.pdf.

Network and Information Security: Proposal for a European Policy Approach. 2001. Dostupné z: http://www.steptoe.com/assets/attachments/811.pdf.

ROUSE, Margaret. Ethical hacker. *Search Security* [online]. 2014 [cit. 2015-02-15]. Dostupné z: http://searchsecurity.techtarget.com/definition/ethical-hacker.

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ A EVROPSKÉMU VÝBORU REGIONŮ k obecné politice v boji proti počítačové kriminalitě. 2007. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:CS:HTML.

SEGER. The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is a web. In: *Council of Europe* [online]. 2012 [cit. 2015-01-31]. Dostupné z: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/AS_UNISPAweb_V6_16feb12.pdf.

THE COUNCIL OF THE EUROPEAN UNION. *Council conclusions on setting the EU's priorities for the fight against serious and organised crime between 2014 and 2017*. Luxembourg, 2013. Dostupné z: http://www.eurojust.europa.eu/Practitioners/operational/THB/Documents/JHA-2013-06-06_137401_EN.pdf.

THE DEPARTMENT OF JUSTICE USA. *Cyber Crime* [online]. 2014 [cit. 2015-01-24]. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

The NCFTA: Combining Forces to Fight Cyber Crime. In: *The FBI* [online]. 2011 [cit. 2015-02-21]. Dostupné z: http://www.fbi.gov/news/stories/2011/september/cyber_091611.

The Internet Organised Crime Threat Assessment. In: *Europol* [online]. 2014 [cit. 2015-01-25]. Dostupné z: https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta.

THE WHITE HOUSE, Washington, President Bush. *The National Strategy to Secure Cyberspace*. 2003. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

THE WHITE HOUSE, Washington, President Obama. *International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World*. 2011. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

United States Computer Emergency Readiness Team. *The National Strategy to Secure Cyberspace* [online]. 2003 [cit. 2014-03-16]. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE. *National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*. 2013. Dostupné z: http://www.gao.gov/assets/660/652170.pdf.

U.S.-EU Summit in Brussels. In: *United States Mission to the European Union* [online]. 2014 [cit. 2015-02-22]. Dostupné z: http://useu.usmission.gov/useu_summit_brussels_032614.htm.

U.S. DEPARTMENT OF STATE. *Secretary Clinton on U.S. International Strategy for Cyberspace*. 2011. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

VASAGAR, Jeevan. Google could face ´cyber courts´ in Germany over privacy rights. *Financial Times* [online]. 2014 [cit. 2015-02-15]. Dostupné z: http://www.ft.com/cms/s/0/a7580826-e59d-11e3-8b90-00144feabdc0.html.

WHITE VANCE, Joyce. Forensics: Secret Service Computer Forensics Training Facility. In: *The Department of Justice USA* [online]. 2014 [cit. 2015-01-24]. Dostupné z: http://www.justice.gov/usao/priority-areas/cyber-crime/forensics.

Resumé

Název práce: Evropská právní úprava kyberzločinů s porovnáním právní úpravy kyberzločinů ve Spojených státech amerických

Diplomová práce se zabývá právní úpravou kyberzločinů a kybernetické bezpečnosti Spojených států amerických a Evropské unie. V úvodu vymezuje základní pojmy a významné momenty historie související právní úpravy a popisuje klíčové strategické dokumenty přijaté v transatlantickém prostoru. Dále představuje politiku obou uvedených celků v této oblasti a jejich klíčové právní předpisy a popisuje mezinárodní Úmluvu o počítačové kriminalitě. Vybrané dokumenty jsou následně porovnány a zhodnoceny v kontextu právní terminologie, technologického vývoje i aplikace předpisů v praxi. Práci uzavírá uvedení základních kroků transatlantické spolupráce v otázkách kybernetické bezpečnosti. Závěr práce shrnuje poznatky získané porovnáním dokumentů, především mezinárodní akcent na ratifikaci Úmluvy o počítačové kriminalitě a zajištění dostatečné úrovně informovanosti o kybernetickém prostoru, a upozorňuje na některé terminologické nepřesnosti.

Klíčová slova

Kybernetické hrozby * kybernetická bezpečnost * kyberzločin* mezinárodní spolupráce * strategické dokumenty

Abstract

Thesis title: European legal regulation of cybercrimes in a comparison with the legal regulation of cybercrimes in the USA

The diploma thesis deals with the legislation of cybercrime and cyber security of the United States of America and the European Union. The introduction defines the basic concepts and important moments of history of related legislation and discusses key policy documents adopted in the transatlantic area. It also presents the politics of these two units and their key legislation and describes the international Convention on Cybercrime. Selected documents are subsequently compared and evaluated in the context of legal terminology, technological development and application of regulations in practice. The thesis is concluded by the basic steps of transatlantic cooperation on issues of cyber security. The conclusion summarizes the lessons learned by comparing documents, particularly international emphasis on ratification of the Convention on Cybercrime and adequate levels of awareness of cyber space, and highlights some terminological inaccuracies.

Keywords

Cyber threats * cyber security * cybercrime * international cooperation * strategic documents