Západočeská univerzity v Plzni
Fakulta právnická

Diplomová práce

Cybercrime a směřování jeho právní úpravy v mezinárodním právu a právu Evropské unie

Vypracoval: Vojtěch Toman
Plzeň 2015

Autor by zde velice rád poděkoval vedoucí této diplomové práce, JUDr. Monice Forejtové, Ph.D. za odborné vedení a přívětivý přístup, dále pak také své rodině a přátelům za pochopení a vytvoření podmínek k tomu, aby tato práce vůbec mohla vzniknout.

Zároveň autor prohlašuje, že diplomovou práci na téma *„Cybercrime a směřování jeho právní úpravy v mezinárodním právu a právu Evropské Unie“* zpracoval samostatně, studiem dané problematiky, uvedl veškeré použité prameny a použité cizí myšlenky řádně dle povahy této práce označil.

_____

Vojtěch Toman v. r.

Abstrakt

Tato práce na téma „Cybercrime a směřování jeho právní úpravy v mezinárodním právu a právu Evropské unie“ pojednává o aspektech a specifikách kyberkriminality a ochrany před ní. Snaží se zachytit současnou právní úpravu dané problematiky a nastínit její možný, předpokládaný či zamýšlený vývoj v blízké budoucnosti. Vychází z povahy právní limitace lidského chování v protikladu k přirozené svobodě lidských jedinců a jejich právu na sebeurčení, v tomto případě informačnímu. Nutná je zprvu shoda na definici kyberkriminality a kyberbezpečnosti, tedy přesné vymezení vlastního předmětu právní úpravy, s přihlédnutím k odlišnostem ve vývoji právní kultury v jednotlivých státech a možnostem, které mají na poli informačních a komunikačních technologií.

Klíčová slova: kyberkriminalita, kybernetická bezpečnost, informační technologie a systémy, právo EU, kritická informační infrastruktura, mezinárodní spolupráce v oblasti IT.

Thesis on „Cybercrime and direction of its legal regulations in the area of international law and the law of European Union.“ deals with aspects and specifics of cybercrime and defence against it. It tries to chronicle recent enactment and outline its possible, expected or intended developement in a near future. It sequents on a nature of law limitation of mankind‘s behavior and its collision with a human being’s natural freedom and its privilege for informational self-determination. First are needed a consensual definitions of cybercrime and cybersecurity, therefore exact delimitation of very subject matter of legal regulations, with regard to varyings in developement of law culture in particular states and theirs potential on the field of ICT.

Keywords: cybercrime, cybersecurity, information technologies and systems, EU law, critical information infrastructure , international cooperation on the field of ICT.

Motto

„Umění knihtisku je faktem, od něhož se datuje druhý díl světa a umění, který se od prvního zcela liší.“

Johann Wolfgang Goethe 1749–1832

Obsah

Úvod

Snad každý v dnešní době využívá výdobytky vědy k usnadnění svého bytí na Zemi, často aniž by nahlédl pod roušku jejich tajemství. Není zajisté v lidských silách vědět vše o všem, rozumět všemu, důležitá je však snaha k tomuto dospět; významná je tedy cesta, nikoliv cíl. Jen takovýto přístup může posouvat jedince a koneckonců i celou společnost kupředu. Realitou dnešních dnů je však fakt, že čím více, čím častěji něco používáme, tím méně si uvědomujeme principy, na kterých to či ono funguje. Hektický shon, „multitasking“, hodnotová disbalance a turbulentní změny způsobují zevšednění jinak přelomových a fascinujících vynálezů. Právě toto zevšednění zapříčiňuje náš neodůvodněný pocit znalosti, familiárnosti k těmto věcem. Aniž bychom si něčeho všimli či to dokonce ocenili, informační a komunikační technologie tak nějak proklouzly do našich životů a postupně s nimi začaly splývat. Jsou našimi pomocníky, průvodci, společníky, sbližují nás lidi dohromady a zároveň nás na hony vzdalují. Nemusíme si připouštět závislost, dokonce ani závislí být nemusíme, pravdou však zůstává, že při dnešní sociální interakci před nimi neutečeme, téměř nikam se neschováme. Čekají nás doma, pronásledují na ulici, na nákupech, okupují naše přátele, vyvolávají nás v čekárnách - na úřadech a v nemocnicích, zajišťují nám dopravu, vodu, teplo i světlo; postupně obrůstají společnost tak, jako břečťan obrůstá letitý kamenný dům kdesi v Provence. Jejich využívání však nepřináší pouze výhody, skýtá i mnohá nebezpečí, za něž musíme nést odpovědnost, za která musíme takříkajíc zaplatit danou cenu A o to bolestivěji nás zraní, o to vyšší ona cena bude, pokud k těmto nebezpečenstvím a úskalím zůstaneme nadále slepí.

Téma této práce jsem si vybral proto, že jsem fascinován, jakého až symbiotického vztahu je společnost schopna dosáhnout s něčím tak mladým, inovativním a nadále se prudce vyvíjejícím, jako je virtuální svět informačních technologií. Téměř se už stírají hranice, kdo vlastně stvořil, či spíše objevil, koho. Rád bych v této práci tedy prozkoumal systematiku i dynamiku tohoto vztahu a pátral po příčinách chyb, kterých se v něm dopouštíme.

Plzeň, březen 2015.

Vojtěch Toman v. r.

Užité zkratky

ICT (IT) – Information and Communication Technologies, informační a telekomunikační technologie
IoT – Internet of Things, internet věcí
NATO – North Atlantic Treaty Organization, Severoatlantická aliance
CCD COE – NATO Cooperative Cyber Defence Centre of Excellence, alianční Centrum pro kyberobranu
UN (OSN) – United Nations, Organizace spojených národů
EC3 – European Cybercrime Centre, Evropské centrum pro boj proti kybernetické kriminalitě
GPS – Global Positioning System, Globální polohový systém
C4E – Czech CyberCrime Centre of Excellence, České centrum excelence pro kybernetickou kriminalitu
ISEC – Prevention of and Fight against Crime Programme, Program prevence a boje proti kriminalitě
CSIRT – Computer Security Incident Response Team, Tým pro koordinaci řešení bezpečnostních incidentů v počítačových sítích
CERT – Computer Emergency Response Team, Tým pro řešení situací nastalých za počítačové nouze
BBS – Bulletin Board Systém, forma on-line služeb, dostupných prostřednictvím veřejné telefonní sítě
MIT – Massachusetts Institut of Technology, Massachusettský technologický institut, založený Williamem Bartonem Rogersem v roce 1861
H4H – Hackers for Hire, námezdní hackeři.
EFF – Electronic Frontier Foundation, mezinárodní nezisková právní organizace zabývající se ochranou práv a svobody slova v digitálním prostředí
TRMC – Tech Model Railroad Club, studentská organizace na MIT, založená Johnem Fitzallenem Moorem and Walterem Marvinem roku 1946
NCSC – National Cyber Security Centre, Národní centrum kybernetické bezpečnosti
USD – Kód amerického dolaru podle ISO 4217
TČ – Trestný čin
BSI – Britský standardizační institut
NIST – National Institute of Standards and Technology, Národní institut pro standardy a technologie Spojených států amerických
DoS (DDoS) – Denial of Service nebo Distributed Denial of Service, odmítnutí služby
DNS – Domain Name Systém, hierarchický systém doménových jmen
MHP – Mezinárodní humanitární právo
ITU – International Telecommunication Union, Mezinárodní telekomunikační unie
UNIDIR – United Nations Institute for Disarmament Research, Výzkumný institut OSN pro otázky odzbrojení
CTITF – Counter-Terrorism Implementation Task Force, Zvláštní jednotka pro implementaci protiteroristické strategie OSN
GCA – Global Cybersecurity Agenda, agenda pro mezinárodní spolupráci v oblasti kybernetické bezpečnosti
IMPACT – International Multilateral Partnership Against Cyber-Threats, Mezinárodní mnohostranné partnerství proti kybernetickým hrozbám
ECOSOC – Economic and Social Council, Ekonomická a sociální rada OSN
UNODC – United Nations Office on Drugs and Crime, Úřad OSN pro drogy a kriminalitu
UNICRI – United Nations Interregional Crime and Justice Research Institute, Meziregionální výzkumný institut OSN pro kriminalitu a spravedlnost
OECD – Organisation for Economic Co-operation and Development, Organizace pro hospodářskou spolupráci a rozvoj

G8 – Group of Eight, sdružení ekonomicky nejvyspělejších států světa - Francie, Itálie, Japonsko, Kanada, Německo, Spojené království a USA (Rusku bylo 18. března 2014 pozastaveno členství jako reakce na anexi Krymu)

WPISP – OECD Working Party on Information Security and Privacy, Pracovní skupina pro informační bezpečnost a ochranu soukromí

HLEG – High Level Experts Group, Skupina expertů vysoké úrovně

ICSPA – International Cyber Security Protection Alliance, Mezinárodní kyberbezpečnostní ochranná aliance

APEC – Asia-Pacific Economic Cooperation, Asijsko-pacifické hospodářské společenství

SPAM – nevyžádané reklamní sdělení masově šířené internetem, zkratky UBE/UCE (Unsolicited Bulk/Commercial Email)

CERT-CC – Computer Emergency Response Team - Coordination Center, Centrální koordinační centrum pro reakci na počítačový bezpečnostní incident

SEI – Software Engineering Institute, Institut softwarového inženýrství na Univerzitě Carnegie Mellon (CMU)

GCLD – Global Cyber Law Database, Globální databáze zákonů o kyberprostoru

T-CY – The Cybercrime Convention Committee, Výbor Úmluvy o kyberkriminalitě

EU – European Union, Evropská unie

SZBP – Společná zahraniční a bezpečnostní politika Evropské unie

ISA – Interoperability Solutions for European Public Administrations, Řešení interoperability pro evropské orgány veřejné správy

ICT- PSP – ICT Policy Support Programme, Program podpory politiky v oblasti IT, součást programu CIP

ESRAB – European Security Research Advisory Board, Poradní platforma pro evropský bezpečnostní výzkum

PASR – Preparatory Action for Security Research, Přípravná akce pro bezpečnostní výzkum

CIP – Competitiveness and Innovation framework Programme, Rámcový program pro konkurenceschopnost a inovace

ENISA - European Union Agency for Network and Information Security, Evropská agentura pro bezpečnost sítí a informací

EUROPOL – European Police Office, Evropský policejní úřad

CSV4 – Cyber Security in the V4: Preparing the Region for a New Reality, Kyberbezpečnost pro Visegrádskou skupinu: Příprava regionu na novou realitu

FIRST – Forum for Incident Response and Security Teams, Fórum pro bezpečnostní a reakční týmy

EGC – European Government CERTs group, Sdružení národních vládních CERT

AFCEA – Armed Forces Communications & Electronics Association, Asociace rozvoje informačních a komunikačních technologií ozbrojených sil

CCRA – Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, Dohoda o společných kritériích pro hodnocení bezpečnosti informačních technologií

VUT – Vysoké učení technické v Brně

NIS – Network and Information Security, Síťová a informační bezpečnost

1. Důvody vzniku kyberkriminality

Člověk je ze své podstaty, ze své lidskosti, tvorem tvořivým a bádavým. Neustále touží něco objevovat, vytvářet a přizpůsobovat si vše kolem sebe. K uspokojení jeho touhy mu však přestaly stačit hlubiny oceánů, výšky hor i vzdálené oblasti vesmíru. Při hledání dokonalého ideálu člověk stvořil svět nový, ve kterém je téměř vše dovoleno, neexistují zde téměř žádné limity a svoboda se zdá být nekonečnou – virtuální svět. Limity kyberprostoru jsou nastaveny pouze kódem, tedy sledem logických instrukcí, vytvářejícím virtuální realitu. Jeho původcem je sice člověk a kód vytváří jakési kauzální omezení kyberprostoru, avšak ve zpětné vazbě normativně omezuje uživatelovo chování v rámci tohoto systému. (Mnohým se možná vybaví legendární Tron a jeho virtuální prostor, ve kterém člověk-uživatel mohl vytvořit vše, co si jen dovedl představit, důležitá byla jen znalost kódu, jehož změny sebou nesly kýžené výsledky.)

Je nasnadě ptát se, zda by Goethe, stále živ, byl fascinován virtuálním světem stejně tak, jako kdysi býval fascinován vynálezem a technologií knihtisku a jeho přínosem civilizaci. Stejně jako on tehdy i my můžeme dnes přikládat, spíše než vytvoření, lze říci objevu kyberprostoru zlomový, revoluční potenciál. Kyberprostor[1] je prakticky ta část virtuálního světa, která ony chladné strojové končiny nekonečných řad jedniček a nul obohacuje o živý substrát, o uživatele. Lidstvu se tak otevřely možnosti dříve nepředstavitelné, postupem času proměňovaly společnost, přetvářely ji na společnost závislou na informacích, datech, více než kdy dříve. Z několika vyvolených se počet „návštěvníků“ kyberprostoru rozrostl na téměř každého druhého obyvatele planety. Lidé přenášejí své životy do virtuální reality čím dál z větší části, v kyberprostoru spolu komunikují, hledají zábavu, nakupují, obchodují, seznamují se, žádají o půjčky, odevzdávají své kvalifikační práce či jen tak volně prezentují své pocity a myšlenky. Stávají se tak součástí virtuálních sociálních sítí či obecně informačních sítí, jsou schopni téměř okamžitě přenést obrovské množství informací a obstarat či spravovat tak velké množství svých záležitostí na libovolnou vzdálenost v malém časovém horizontu. Plní i jiné role než tradiční,

[1] *Ve slovníku lze najít definici kybernetického prostoru coby digitálního prostředí umožňujícího vznik, zpracování a výměnu informací, tvořeného informačními systémy a službami a sítěmi elektronických komunikací.*

JIRÁSEK, P. NOVÁK, L. POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Druhé aktualizované vydání. Policejní akademie ČR & Česká pobočka AFCEA, 2013. str. 59.

připsané jim v běžném denním životě, mohou se projevovat víceméně anonymně, což opět rozvolňuje svázaný kruh společenské kontroly a společenského odsouzení. Jednotlivé střípky dat a informací, které každý emituje do kyberprostoru při jednotlivých úkonech, jež v něm činí, pak utvářejí jeho virtuální já, obraz, skrze který ho ostatní uživatelé při vzájemné interakci poznávají. U jedince – uživatele, pak dochází k jakémusi rozpolcení, je reálně existující osobou z masa a kostí a zároveň virtuální bytostí, jde o dichotomii toho, jakým člověk je a jakým se jeví ostatním, možnost participace v kyberprostoru tuto dichotomii pak jen značně umocňuje.

Usnadnění, která tento koncept s sebou přináší, jsou nesporná, je však třeba si uvědomovat i nebezpečí s tím spojená. Neexistuje žádný systém hodnocení relevance informací kolujících kyberprostorem či punc jejich pravosti, vše je založeno na určité reflexi stran ostatních uživatelů. Pravdivost tedy předurčuje informační kvalitu, která jako jediná je schopna zvyšovat míru organizovanosti. V opačném případě může, při racionálním přístupu, působit entropicky, v určitých případech emocionální percepce informace však toto neplatí.[2] *„Přijmeme-li Humovu systematiku[3], alespoň jako metodologické východisko, můžeme rozlišit informace na dva základní typy – na takové, které popisují skutečnost (tedy to, co je) a pak na instrukce, tedy informace o tom, co být má. Informace o skutečnosti nazýváme výroky a přiřazujeme jim hodnotu pravdivosti. Pokud vztáhneme kategorii pravdivosti k pojmu informace a budeme vycházet z výše uvedené Wienerovy definice,[4] docházíme k závěru, že pravdivost je nutným předpokladem toho, abychom nějaké sdělení mohli označit za informaci. Jen pravdivá informace je totiž způsobilá snižovat míru entropie příslušného systému. Dostane-li tedy adresát pravdivou informaci, zvyšuje se jeho schopnost reagovat na okolní prostředí a naopak se snižuje pravděpodobnost chybného*

[2] Více o pravdivosti informací a jejich vlivu na organizovanost viz POLČÁK, R.. *Internet a proměny práva*. Praha: Auditorium, 2012. ISBN 978-80-87284-22-3. str. 26 a násl.

[3] Citovaný autor má na mysli Humovu tezi dělící svět na doménu bytí (is) a mětí (ought). K základní distinkci mezi bytím a mětím srov. HUME, D. *A Treatise on Human Nature.* Project Gutenberg, 2003. Volně ke stažení na adrese www.gutenberg.org/etext/4705.

[4] *„Právě tak, jako entropie je mírou dezorganizace a neuspořádanosti, informace je mírou organizace, uspořádanosti, a že informaci tedy lze chápat jako zápornou entropii; a že stroj, obdobně jako živý organismus nebo informacemi řádně řízené lidské společenství, je zařízení, jež bojuje proti obecné tendenci k vzrůstu entropie."* Viz Wiener, N. *Cybernetics: Or the Control and Communication in the Animal and the Machine.* Cambridge: MIT Press, 1961, str. 11.

rozhodnutí."[5] Problém je i s informací samou, její pojem je velice mnohoznačný, obecný, vyznačuje se mnohostí druhů i mnohostí důsledků, které může ten který druh informace vyvolat. Pokud tedy přijmeme fakt, že tato společnost je pro svou současnou životaschopnost a svůj další rozvoj téměř zcela odkázána na informace, na jejich vytváření, na jejich přenos a sdílení, jejich další zpracování a zhodnocování, dojdeme pak k závěru, že není možné chránit veškeré informace a že je taková snaha i neúčelná. Absolutní kontrola a ochrana by vlastně dementovaly samotný smysl a náplň kyberprostoru jako prostředku zcela nového způsobu lidské socializace a projevu hodnot starých i nově vytvářených.

Tato práce si tedy klade za cíl popis a poznání vzniku a vývoje ochranných mechanismů v kyberprostoru, které jsou zcela novým a svébytným fenoménem, ať už jsou součástí autoritativní rozhodovací činnosti orgánů veřejného sektoru, nebo pouze výplodem svépomoci osob soukromé sféry ve chvílích selhání či nedostatku ochrany jiné; popis systémů profesionálně vyvíjených i vzniklých stylem pokus a omyl v raných fázích vývoje kyberprostoru; poznání důvodů, které vedly k potřebě a vzniku těchto mechanismů a také poznání důsledků a dopadů na běžný život uživatele či obecněji člověka, jež volba toho kterého mechanismu může s sebou nést. Je nutné zde připomenout, že kyberprostor, respektive jeho vliv na každodenní chod společnosti je tak značný, že se stal esenciální potřebou civilizace ať už v zemích rozvinutých či rozvojových. A contrario k tomuto se přes svou kruciální důležitost problém řádné a efektivní ochrany kyberprostoru stále pohybuje v marginálních oblastech zájmu uživatelů, poskytovatelů i států. Nutno je však podotknout, že s narůstající mírou osvěty a ICT gramotnosti vzrůstají postupně i snahy hledat cesty k dosažení opravdu účelného a zároveň vyváženého řešení ochrany slabin, jejichž zneužití může ohrožovat dnes již stovky milionů lidí po celém světě.

1.1. Informační společnost

Na začátku jsme zmínili prudký rozvoj společnosti na základě rozmachu ICT technologií a jejich postupnou a stále větší integraci do každodenního života jedince. Pohonem tohoto procesu bylo volání po stále větší úrovni informovanosti. Informace v digitální podobě proudily stále větší rychlostí při stále narůstajícím objemu dat. Je ovšem chybou tvrdit, že změna paradigmatu při tomto přechodu

[5] POLČÁK, R. *Právo a evropská informační společnost.* Brno: Masarykova univerzita, 2009. ISBN 978-80-210-4885-0. str. 16.

spočívala v užívání informací samotných. V celé historii lidstva byla informace jako taková nositelem určité hodnoty, její získávání a přenos byly náplní soustavné lidské činnosti při snaze o lepší organizovanost společnosti jako celku.[6] Zde lze vzpomenout na příklad Haralda I., přídomkem Bluetooth, dánského a norského krále, který oplýval značnými diplomatickými a komunikačními schopnostmi. Nechal zřídit síť jakýchsi prvních poštovních stanic, které měly usnadnit komunikaci mezi jednotlivými částmi skandinávského poloostrova. Následně můžeme sledovat vývoj od objevu knihtisku, telegrafu, telefonu, faxu, televizoru po osobní počítač, internet, poštovní služby urychlila letecká doprava atd. Veškeré tyto prostředky sloužily jedinému cíli, přenosu informací. *„Pojem informační společnosti je tedy ve své podstatě obecný a do značné míry zbytečný. Každou společnost, respektive každé společenství totiž můžeme považovat za informační, neboť je to právě informace, co je drží pohromadě a zajišťuje mu přežití a rozvoj. Pravý význam pojmu informační společnost, respektive význam, v němž se tento pojem aktuálně používá, však není obecným synonymem pro organizovanou nebo organizace chtivou společnost. Jedná se o pojem označující společnost, která si postupně uvědomuje důležitost informací a která ke zvýšení své informovanosti využívá možností daných moderními informačními a komunikačními technologiemi.“*[7]

Pokud tedy máme pátrat po vzniku a významu pojmu kyberkriminality, musíme se v počátku věnovat popisu hlavních znaků, které definují informační společnost,[8] rozdílu v kvantitativním i kvalitativním přístupu k využívání informací, proměnám, kterých doznává na poli ekonomickém, pracovním, sociálním, komunikačním, kulturním a také jejímu vlivu na sektory, které s postupnou informatizací[9] primárně nesouvisejí.

---

[6] Srov. WIENER, N. *Cybernetics: Or the Control and Communication in the Animal and the Machine.* Cambridge: MIT Press, 1961, str. 11.

[7] POLČÁK, R.. *Internet a proměny práva.* Praha: Auditorium, 2012, ISBN 978-80-87284-22-3. str. 275.

[8] *Informační (kybernetickou) společnost definuje výkladový slovník kybernetické bezpečnosti jako společnost schopnou využívat a využívající informační a komunikační technologie. Základem je neustálá výměna znalostí a informací a práce s nimi za předpokladu schopnosti jim rozumět. Tato společnost pokládá vytváření, šíření a manipulaci s informacemi za nejvýznamnější ekonomické a kulturní aktivity.*
JIRÁSEK, P. NOVÁK, L. POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Druhé aktualizované vydání. Policejní akademie ČR & Česká pobočka AFCEA, 2013. ISBN 978–80–7251–397–0 , str. 45.

[9] *Informatizace společnosti je proces prosazování nové gramotnosti ve společnosti založené na zvládnutí nových metod práce s počítačem, s informacemi a informačními technologiemi.* Tamtéž, str. 46.

Informační společnost se tedy profiluje jako společnost, která využívá přenosu velkého množství digitalizovaných dat při současném masivním přístupu k informačním a komunikačním technologiím za současného snižování jejich cen (kvantitativní stránka).[10] Proměna užití informací potom představuje stránku kvalitativní, kdy společnost vědomě využívá těchto informací k navýšení organizovanosti, přičemž dostupnost, změna způsobu šíření a snadná možnost duplikace informací vede k celospolečenským změnám zasahujícím do každého aspektu lidské činnosti.[11] I v rámci informační společnosti pak dochází k určité genezi, kdy uživatelé přecházejí od pasivního příjmu a zpracování informací k aktivnímu utváření obsahu kyberprostoru, ne však jeho architektury. Lidé jednoduše přenáší obsah své sociální interakce z reálného do virtuálního světa, což mění aspekty takovéto interakce. *„Druhou centrální hodnotou informační společnosti je vzájemnost (solidarita). Její implicitní přítomnost je dána per se skutečností, že základní komoditou informační společnosti jsou informace. Člověk má v rámci svého společenského fungování přirozenou tendenci k tomu, informace nejen přijímat a zpracovávat, ale též šířit. Jsou to pak právě svoboda a tendence ke vzájemné informační výměně, co nejvýrazněji táhne společenský i technologický rozvoj informačních sítí.“*[12] Zjednodušeně řečeno, tendence k co nejaktivnějšímu přístupu a co nejsvobodnějšímu prostoru sloužícímu mezilidské výměně informací nadále exponenciálně urychluje další rozvoj informační společnosti.

O změnách v ekonomickém, kulturním, pracovním a dalším prostředí jsme se již zmínili, je však třeba uvést změny, které se dějí v chápání a využívání prostoru. Hranice nemají takovou důležitost, vzdálenost se marginalizuje, komunikace se přesouvá postupnou virtualizací na naprosto jinou úroveň, kyberprostor se globalizuje a stává se supranacionálním. Takovéto přiblížení a současné odtělesnění uživatelů přináší nové výzvy pro lidskou psychiku, proměňuje podstatu mezilidských vztahů a často mění zavedené vzorce lidského

[10] *Slovník informační a komunikační technologií (ICT) rozumí veškerou techniku, která se zabývá zpracováním a přenosem informací, tj. zejména výpočetní a komunikační technika a její programové vybavení.*

Tamtéž, str. 46.

[11] Viz. WEBSTER, F. *Theories of the Information Society.* 3. vydání. New York: Routledge, str. 21.

Srov. POLČÁK, R.. *Internet a proměny práva.* Praha: Auditorium, 2012, ISBN 978-80-87284-22-3, str. 277 – 281.

[12] POLČÁK, R. *Internet a proměny práva.* Praha: Auditorium, 2012, ISBN 978-80-87284-22-3. str. 286.

chování. Je téměř indiferentní, vstupujete-li v kyberprostor prostřednictvím internetové či podnikové sítě, kvalitativní změny v lidské psychice a lidské interakci se pak mohou projevovat naprosto stejně. Problém spočívá ve fyzické delokalizaci, která nabourává distančnost takovéto komunikace a interakce, jinými slovy řečeno, je jedno kde se nacházíte, omezení nevyplývají z umístění, ale z typu, formy použité komunikace a technického zabezpečení. To může narušovat právní chápání a řešení tzv. distančních deliktů a nastoluje zcela nový pohled na tento druh vztahů. *„Pro trestní právo tento přeshraniční prvek dává vzniknout situaci, kdy delikvent může jednoduše manipulovat informace skrze datový přenos, přičemž efekt takové manipulace se téměř okamžitě projeví na druhé straně planety… Vzniká nová nezávislá jurisdikce, „Kyberprostor", ovlivňující mnoho rozdílných právních systémů zároveň. Je tedy možné mluvit o jisté „deteritorializaci práva" uvnitř Internetu."*[13] Vzhledem k takto postavenému systému je velké množství informací, jejich shromažďování i nakládání s nimi fakticky vzdáleno místním orgánům a jejich jurisdikci, nutná je tedy v takovémto případě mezinárodní spolupráce.[14]

Informační společnost vzniká ve své podstatě spontánně, vzdaluje se vlivu autorit, tvoří živý celek, stále více se vymyká oficiální kontrole, zdrojem její organizovanosti je informace, nikoli autoritativní vnucená organizace, je v ní obsažena dokonce i možnost seberegulace[15] v případě určité „přeinformovanosti", deregulace a reflektivního hodnocení pravdivosti sdílených informací. Nicméně je zde velice důležitá podpora vědomého rozvoje, komplexní a soustavné snahy o zachování kyberprostoru jako svobodného kosmopolitního území pro sdělování, přenos a šíření informací, bez níž by i takovýto systém organizovaného sdílení informací nakonec pohltil sám sebe, už jen z premisy, že vyrovnaného ideálu kvantity a kvality nelze dosáhnout. Klíčovým pojmem této činnosti tedy musí být rovnováha. Nadměrná regulace by mohla poškodit fungování kyberprostoru stejně tak vážně, jako regulace nulová s naprostým a volným šířením chaosu a to pro nemožnost jednotlivce zabezpečit svá fundamentální informační práva. Při nadměrné regulaci za účelem ochrany těchto práv by však naopak docházelo

[13] SIEBER, U. LEDERMAN, E. Conceptualizing Informational Law. In Law, Information and Information Technology. The Hague: Kluwer Law International, 2001. s. 17. Překlad je neoficiální, autorův.

[14] Viz. POLČÁK, R.. Internet a proměny práva. Praha: Auditorium, 2012. ISBN 978-80-87284-22-3, str. 102.

[15] Viz POLČÁK, R. *Autoritativní regulace kyberprostoru a legitimita trestního práva. In Kyberkriminalita a právo*. Praha: AUDITORIUM, 2008. s. 12-24, 13. ISBN 978-80-903786-7-4.

k zásahům do práv jiných a naprostému znehybnění svobodného informačního toku. *„Z uvedeného vyplývá poněkud pompézní přesto však racionální závěr, že nechat jednotlivce volně komunikovat znamená mimo jiné dát prostor k rozvoji základním hodnotám lidské společnosti.“*[16] Z tohoto důvodu je pak také obtížnější vytvářet limitující pravidla ve státech s totalitní minulostí, kdy i specificky cílená, ale citlivá úprava může zvednout vlnu nevole jak jednotlivců, tak i interesovaných nevládních organizací.[17]

Další změnou, kterou prodělal vývoj informační společnosti je, a to by se zdálo jako opětovné, připojení neživého substrátu do informačních sítí, postupný vznik toho, co odborníci nazývají Internet of Things (IoT). Jedná se o uvedení věcí, které slouží lidským potřebám, do prostředí uživatelů, aby byla umožněna vzájemná komunikace. Tento směr vývoje má neuvěřitelně rozsáhlé možnosti dalšího postupu, s nedozírným dopadem na společnost jako celek i na život jednotlivce v rámci společnosti. *„Mezinárodní expert nového centra kybernetické kriminality (EC3) založeného v rámci Europolu v Haagu Jaroslav Jakubček řekl, že Evropa se v budoucnu stane cílem masivních kybernetických útoků, souvisejících s připojením obyvatel rozvojových zemí k internetu, které nastane během pěti až deseti let… Útokem přitom podle něj nebudou ohroženy jen počítače a přenosné telefony, jež budou i nadále hrát podstatnou roli, ale i různé přístroje, které dříve internetové připojení neměly, ale nyní už tuto funkci mít budou – televizory, ledničky, toastery nebo třeba termostaty. Právě u podobných zařízení podle něj v budoucnu kyberkriminality výrazně přibude.*“[18] Představme si situaci: odjíždíme z práce, nasedáme do automobilu, na palubním GPS modulu zvolíme možnost „domů“. Automobil začne komunikovat s domácností - zapne vytápění, chlazení, praní, otevře okna na větrání atp. Jaké výhody ve zkvalitnění komfortu života, v ekonomickém i environmentálním aspektu a mnohých dalších toto přináší, je jednoznačné. Jaké fatální dopady by nastaly při ovládnutí, kontrole, změně či poškození těchto přenášených informací, je zneklidňující. Zvláště při představě, že dnes jsou na některou z informačních sítí připojeny výrobní linky, řízení provozu a dopravy, jaderné elektrárny, armádní sítě,

[16] POLČÁK, R. *Internet a proměny práva.* Praha: Auditorium, 2012. ISBN 978-80-87284-22-3, str. 282.

[17] Srov. HARAŠTA, J. Cyber security in young democracies. In Jurisprudence, Mykolas Romeris University, 2013, ISSN 2029–2058 str. 1460 a násl.

[18] Česká justice, *Případů kyberútoků prý přibude, terčem budou třeba ledničky nebo toastery*, 21. 9. 2014, © 2014 Česká justice (online), dostupné z: http://www.ceska-justice.cz/2014/09/pripadu-kyberutoku-pry-pribude-tercem-budou-treba-lednicky-nebo-toastery/

rozvodové infrastruktury - zásobování elektřinou, vodou, plynem, servery médií, letištní dispečinky i řízení kontroly vesmírných letů a stovky dalších…

„Každá naše činnost bude nadále stále více ovlivňována fenoménem Internetu věcí, skrývajícím se pod zkratkou IoT. Nejen lidské bytosti vybavené komunikační technikou, ale i „věci", jako jsou vozidla, produkty spotřební i průmyslové elektroniky, lékařské přístroje, vzdálené senzory monitorující parametry životního prostředí a další zařízení, budou připojeny do sítí a jejich prostřednictvím k Internetu. Tento vývoj dalekosáhle ovlivní ekonomiku a stane se výzvou pro budoucí koncepci kybernetické bezpečnosti a její implementaci do sítí IoT, výzvou pro obchodní operace a partnerské ekosystémy. Internet věcí se tak stává stimulem obrovské „demokratizace", kdy data jsou v reálném čase sdílena v takovém rozsahu, jako dosud nikdy. Paradoxně tato zásadní přednost, tj. potenciál okamžitě sdílet data s kýmkoli a s čímkoli, vytváří obrovskou kyberbezpečnostní hrozbu. IoT tak bude vyžadovat nové kolo revize strategií rizikového managementu, nové nástroje pro vyhodnocení bezpečnosti sítě a revizi obchodních modelů. Jako všechny významné změny v komerčním prostředí, také rozvoj Internetu věcí bude vytvářet výzvy, ale i příležitosti pro firmy, které budou mít možnost profitovat z nových požadavků na kyberbezpečnost."[19]

1.2. Informační sebeurčení

Regulace kyberprostoru je tedy buď nadbytečná a poškozuje práva jiná, či je nedostatečná a nezabezpečuje práva informační, dotkli jsme se tedy problematiky kyberbezpečnosti. Mnohé teorie ji označují za bezpečnost informací, nakolik je tato definice nepřesná, si uvedeme dále. Bezpečnost obecně se nejčastěji definuje jako stav ochrany před vznikem škody. Pokud užíváme pojmu ochrana, musíme se nutně ptát čeho? Předmětem kyberbezpečnosti[20] je ochrana práva na informační sebeurčení; je to neodmyslitelná součást informační společnosti. Jako takové je toto právo celým katalogem dílčích distributivních

[19] Sdělovací technika červen 2014. *Úvodník: Kyberbezpečnost v Internetu věcí* (online) © 2015 Sdělovací technika, dostupné z: http://www.stech.cz/e-casopis/nahled/2014/6.aspx

[20] *Dle slovníku je kybernetickou bezpečností míněn souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru. Slovník pak dále rozlišuje bezpečnost dat, informací, informačních systémů, internetu a komunikací, které jsou pouze jednotlivými složkami kyberbezpečnosti.* JIRÁSEK, P. NOVÁK, L. POŽÁR, J. Výkladový slovník kybernetické bezpečnosti. Druhé aktualizované vydání. Policejní akademie ČR & Česká pobočka AFCEA, 2013. str. 18-19, 57.

práv. Ochrana informací a dat je tedy pouze prostředkem kyberbezpečnosti k zajištění práva na informační sebeurčení, které jí propůjčuje jednak opodstatnění a legitimitu, ale zároveň nastavuje určité limity jejího uplatňování. Právo však může chápat kyberbezpečnost v užším významu, než jak ji posuzujeme z tohoto pohledu. Z právního pohledu je totiž nutno odlišovat ochranu kybernetické bezpečnosti státu od dalších forem informační bezpečnosti, tj. od ochrany dat a informací včetně osobních údajů, ochrany obchodního tajemství, ochrany před běžnou trestnou činností zaměřenou k informacím (před informační kriminalitou) apod.[21] Takto chápaná kyberbezpečnost má ovšem i mnohem užší pole působnosti, její účelnost a legitimita pramení už ze samé existence státu, jeho snahy o sebezachování a je prostředkem k udržení schopnosti státu plnit své základní funkce při službě občanům, což by mu postižení určitých kritických systémů ztěžovalo či zcela znemožňovalo. *„Z konkrétních elementů hodnotového základu informační společnosti je na prvním místě třeba jmenovat svobodu. Holländer tuto základní hodnotu lidské společnosti staví do kontrapozice se státní mocí a zajištěním reprodukce.[22]Svoboda jednotlivce je totiž vždy omezitelná (omezená) státní mocí tam, kde by její bezmezná realizace mohla vést k narušení sociální konzistence a tím k ohrožení reprodukčního potenciálu společnosti.“*[23] Avšak s nárůstem hodnoty a stále větší role informací narůstá i význam práva na informační sebeurčení a vymezení jednotlivých základních práv, které pod tuto svobodu spadají. S rozvojem informačních a komunikačních technologií se rozšiřuje jednak katalog těchto práv, resp. institutů, zároveň však i limity, které tato práva současně omezují. Dnes jsou nejdůležitějšími instituty chránícími informace: svoboda projevu a svoboda vědeckého bádání; ochrana soukromí včetně ochrany osobnosti a práva na soukromý život; právo na vzdělání; ochrana osobních údajů; právo na informace veřejného sektoru včetně práva na jejich další užití; práva duševního vlastnictví; know-how; obchodní tajemství; nezapsaná označení; utajované informace.[24] Velice často diskutovaným právem je potom také právo přístupu, tedy jakési právo na Internet, právo moci být online. Jedná se o jednu z nejdůležitějších a v současnosti velice diskutovanou složku

[21] Viz. SMEJKAL, V. a kol. *Právo informačních a telekomunikačních systémů*. Praha: C. H. Beck, 2001, ISBN 80-7179-552-6, str. 479 a násl.

[22] Viz. HOLLÄNDER, P. *Filosofie práva*. Plzeň: Aleš Čeněk, 2006, str. 102 a násl.

[23] POLČÁK, R.. *Internet a proměny práva.* Praha: Auditorium, 2012. ISBN 978-80-87284-22-3, str. 284.

[24] Srov. POLČÁK, R.. *Internet a proměny práva*. Praha: Auditorium, 2012. ISBN 978-80-87284-22-3, str. 302.

informačního sebeurčení, která může zabránit svévolnému omezování přístupu k Internetu a filtrování jeho obsahu ze strany státní moci. Celosvětově první zákon garantující připojení byl přijat ve Finsku v roce 2010. Již rok na to vyšla pod OSN zpráva Rady pro lidská práva[25], kterou vypracoval zvláštní zpravodaj Frank La Rue, pověřený monitoringem nových médií a jejich vlivu na lidská práva a svobody. Ve zprávě připomíná zásadní postavení Internetu pro vývoj informační společnosti celosvětově a odsuzuje nepatřičné státní vměšování, jelikož právo na přístup k Internetu dle něho spadá pod čl. 19 Všeobecné deklarace lidských práv[26], dále rozvedeno v Mezinárodním paktu o občanských a politických právech[27]; tedy by mělo k omezení tohoto práva docházet pouze rozhodnutím nezávislého orgánu a to pouze při kumulativním splnění tří podmínek:

- omezení musí vyplývat pouze ze zákona,
- musí chránit práva či reputaci ostatních, chránit národní bezpečnost nebo veřejný pořádek nebo chránit zdraví či morálku,
- omezení musí být prokazatelně nevyhnutelné, musí to být nejmenší možné omezení, nutné k dosažení cíle.

Jak je patrné, právo přístupu k Internetu je v současnosti nejstěžejnějším právem informační společnosti, jehož zajištění a nerušený výkon teprve umožní plný výkon zmíněných práv ostatních. Tedy řečeno zcela obhrouble, je vcelku jedno, že máte právo svobodně šířit a sdílet informace Internetem, když Vám k němu někdo zamezuje byť jen přístup.

Právě tedy ochranou všech těchto institutů zajišťuje kyberbezpečnost fundamentální, informační práva. Jestliže zmíníme základní hodnoty informační společnosti, tedy svobodu a solidaritu, na výstupu dostaneme, že se jedná o právo svobodně informace tvořit, získávat, zpracovávat, mít k dispozici a dále je svobodně sdílet, šířit. Pokud zde však vzpomeneme výrok Ovidia Nasa *„Často nejistě stojí a neví, kam by měl jíti poutník, jenž volnou má cestu do všech čtyř světových stran.“*, můžeme dobře vidět, že ani absolutní svoboda nemusí být plodná a konstruktivní, zvláště vezmeme-li v potaz, že stejně tak, jako se lidé

[25] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 16. 5. 2011, dostupné z: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[26] *Všeobecné deklarace lidských práv,* 10. 12. 1948, dostupné z http://www.osn.cz/dokumenty-osn/soubory/vseobecna-deklarace-lidskych-prav.pdf

[27] *Mezinárodní pakt o občanských a politických právech.* New York, 19. 12. 1966, dostupné z: http://www.osn.cz/dokumenty-osn/soubory/mezinar.pakt-obc.a.polit.prava.pdf

snaží využívat informace ve svém celospolečenském tažení proti entropii, stejně tak mohou mít tendence informace zneužívat, měnit a překrucovat, uvádět je v nepravdu, a tím k entropii vlastně přispívat. Přijmeme-li pak tezi, že svoboda jednoho končí tam, kde začíná svoboda druhého, tedy že ani informační práva nemohou mít absolutní povahu, jelikož se uplatňují v organizovaném společenském systému a narážejí na stejná informační či jiná práva ostatních jednotlivců, pak nám vyjde legitimita kyberbezpečnosti coby regulativního omezení informačních práv za účelem zajištění jejich nedistributivního a rovného práva na ochranu pro každého, a zároveň i částečně ochrany jedince před sebou samým. Poslání kyberbezpečnosti se ovšem nesmí posuzovat pouze v tomto uzavřeném prostoru, samo musí být limitováno s ohledem na ostatní okolnosti, v širších souvislostech celého právního řádu pro zachování kontinuity právní jistoty a atributů právního státu i v takto rychle se měnícím světě a v proměnlivých potřebách informační společnosti. Že tento úkol není snadno dosažitelným cílem, ukazuje už jen princip, že stát, resp. jeho orgány, mohou jen to, co jim právo umožňuje, přičemž efektivní ochrana kyberprostoru vyžaduje velice flexibilní reakce na příslušné útoky či jejich hrozby. Pokud by však právní rámec kompetence nadmíru rozvolnil, mohlo by docházet k příliš neadekvátním zásahům do distributivních informačních práv, které jsou pro účinnou obranu nutné. Turbulentní rychlost, se kterou přicházejí nové formy hrozeb, pak jednoznačně předstihuje legislativní proces a zanechává stát téměř neakceschopný. Uvedený stav pak může vést k debatám či obecnému a celkovému popření platnosti práva v kyberprostoru. Příkladem takového popření je Deklarace nezávislosti kyberprostoru (dále jen Deklarace):

- *Vlády průmyslového světa, vy strhaní obři z masa a oceli, přicházím z Kyberprostoru, nového domova mysli. Ve jménu budoucnosti žádám vás, kteří jste minuli, abyste nás nechali na pokoji. Nejste mezi námi vítáni. Nemáte svrchovanost nad místy, kde se scházíme.*
- *Nemáme volenou vládu, ani ji nejspíš mít nebudeme, takže vás neoslovuji s větší autoritou, než se kterou vždy mluvívá svoboda sama. Prohlašuji za přirozené, že globální společenský prostor, který jsme vytvořili, nemá nic společného s tyranidou, do které se nás snažíte uvalit. Na panování nad námi nemáte ani morální právo, ani donucovací prostředky, kterých by mělo smysl se bát.*

- *Vlády odvozují svoji oprávněnou moc ze souhlasu ovládaných. O ten náš jste ani nepožádaly, ani jste ho neobdržely. Nepozvali jsme vás. Neznáte nás, ani náš svět. Kyberprostor neleží uvnitř vašich hranic. Nemyslete si, že ho můžete postavit, jako by to byl veřejný stavební projekt. Nemůžete. Projevuje se v něm přirozenost a roste sám díky našemu společnému jednání.*
- *Naší skvělé a sbližující konverzace jste se ani neúčastnili, ani jste nevytvořili bohatství našich tržišť. Neznáte naši kulturu, naši etiku nebo nepsaná pravidla, která naší společnosti už teď přinášejí pevnější řád, než jaký by vaše tresty vůbec mohly zajistit.*
- *Tvrdíte, že jsou u nás problémy, které potřebujete vyřešit. Využíváte svého tvrzení k ospravedlnění invaze do naší zóny. Řada z těchto problémů vůbec neexistuje. Skutečné konflikty, v nichž se páchají křivdy, poznáme a zaměřujeme na ně své prostředky. Ustavujeme svou vlastní Společenskou smlouvu. A tato vláda vznikne podle podmínek našeho světa, ne vašeho. Náš svět je jiný.*
- *Kyberprostor sestává jen z transakcí, vztahů a myšlenek, které svým uspořádáním připomínají stojatou vlnu na síti naší komunikace. Náš svět, který je zároveň všude i nikde, určitě není tam, kde žijí naše těla.*
- *Vytváříme svět, do něhož smí vstoupit každý bez ohledu na přednosti či předsudky založené na rase, hospodářské síle, vojenské moci nebo místě původu.*
- *Vytváříme svět, kde může každý vyjadřovat svou víru, kde chce. Bez ohledu na to, jak je výstřední, se nemusí bát, že bude umlčován nebo tlačen většinou k souhlasu.*
- *Vaše právní pojmy pro majetek, vyjadřování, identitu, hnutí a souvislosti se na nás nevztahují. Jsou založeny na hmotě. Tady žádná hmota není.*[28]

Již z tohoto výňatku je patrné, že se tento pamflet snaží působit až revolučním dojmem, jeho iniciaci způsobil v Kongresu schválený Zákon o reformě telekomunikací, který de facto zaváděl do médií po celých USA cenzuru pod hrozbou pokuty vcelku značné sumy až 250,000$. Autoři této deklarace, níže uvedení, dokonce tento akt chápali jako vyhlášení války kyberprostoru ze strany *„starých struktur“*. Proč bylo nutné tyto počáteční

[28]BARLOW, J. P. *Deklarace nezávislosti Kyberprostoru.* Davos, 1996. Electronic Frontier Foundation, (překlad Jakub Friedl), dostupné z: http://svetylko.blog.cz/1206/deklarace-nezavislosti-kyberprostoru

odstavce Deklarace citovat, nejen na Deklaraci, volně dostupnou online odkázat, je nasnadě. Veškeré zachycené stížnosti se vážou k hodnotám, k atributům a tedy i k problémům, se kterými se kyberprostor potýká téměř od samého začátku. Dále pak budeme mít možnost srovnat Deklarací hlásané hodnoty s Levyho „hackerskou etikou" a s prohlášeními a postoji dalšího následovníka liberálně alternativního proudu v kyberprostoru, a to hnutí Open Source Code.

Tuto Deklaraci vytvořila organizace Electronic Frontier Foundation (EFF) která „*byla založena v roce 1990 trojicí amerických občanů, kteří nebyli spokojeni s přístupem státních orgánů k tzv. digitálním svobodám, v té době ještě pro většinovou populaci šlo o nezajímavou záležitost. Zakladateli byli John Gilmore, John Perry Barlow a Mitch Kapor*".[29] Tato organizace tedy virtuální prostor Internetu považuje za zcela nově objevený prostor, který nespadá pod žádnou jinou jurisdikci, její členové nepřipadají ke kontraktualistům, tzn. nevzdali se společenskou smlouvou své suverenity ve prospěch nikoho. Jejich nedostatek vůle k uzavření takovéto smlouvy pramení z jejich přesvědčení o vlastní soběstačnosti, tedy z nedostatku odůvodněnosti a tedy i legitimity státních či jiných vnějších zásahů do problémů této komunity, pramenících také právě z jakési delokované a:supranacionální povahy téměř každého kyberprostoru. Stát by však v takovém případě nemohl zasáhnout ani při nesplnění první podmínky, tedy soběstačnosti. Pouhá potřeba ochrany by pak nahrazovala vůli k uzavření takovéto společenské smlouvy vůči suverénnímu státu. Empiricky pak lze dovodit, že taková potřeba ochrany existuje, už jen kvůli existenci chaotizujícího chování, leckdy kriminalizovaného, které komunita sama nemá zájem či obsáhlejší schopnosti řešit a eliminovat.

„Vypořádání se s třetím argumentem ohledně fakticity působící praktickou nevynutitelnost práva však je v porovnání s prvními dvěma nesrovnatelně složitější a za stávající právní situace v řadě ohledů dokonce prakticky nemožné."[30] První dva argumenty, jistá nemohoucnost státu, mají určité řešení ve spolupráci s institucemi, které nepodléhají obdobným omezením jako stát a mohou být aktivně zapojeny do systému ochrany kyberprostoru, kde nedojde jejich svázání zákonem, tedy mohou činit vše, co jim právo výslovně nezakazuje.

[29] BOŘÁNEK, R. *Electronic Frontier Foundation: neziskovka, která jde po krku NSA*. F. 4. 7. 2014, © 1998 – 2015 Root.cz (online) ISSN 1212-8309, dostupné z: http://www.root.cz/clanky/electronic-frontier-foundation-neziskovka-ktera-jde-po-krku-nsa/

[30] POLČÁK, R.. *Internet a proměny práva*. Praha: Auditorium, 2012. ISBN 978-80-87284-22-3, str. 101.

Takovéto propojení za aktivní účasti státu formou podpory a finanční motivace může být velice přínosné, otázka faktické nevymahatelnosti práva může být řešena pouze mezinárodní spoluprací[31] a zapojením soukromého sektoru, v obojím ovšem naráží v určitých úsecích na zatím neřešitelné či těžko odstranitelné problémy.[32]

Pokud tedy narážíme na normativitu a kauzalitu v kyberprostoru, dostáváme se zpět do úvodu, kde jsme se zmínili o kódu. Teorii Kódu formuloval Lawrence Lessig ve své knize Code and Other Laws of Cyberspace[33], kde uvedl výčet regulativů lidského chování, tedy práva, sociálních norem a etických regulativů, samoregulační mechanismy, pravidla ekonomiky a kód. Kód se v jeho očích vymyká běžnému pochopení, je normou sui generis, jde o definiční normu, tedy v sobě slučuje kauzalitu s normativitou, je projevem chtění, tedy toho co má být, zároveň však kauzálně nastavuje uživatelům mantinely jejich působení. „*Definiční normy je třeba, jak již bylo naznačeno, považovat za normy sui genesis. Důvodem jejich vzniku je, podobně jako u ostatních typů norem, chtění specifické definiční autority. Jejich charakter však způsobuje, že spíše než normativita je pro většinu jejich adresátů, tj. pro běžné uživatele, důsledkem jejich existence kauzalita.*“[34]

Dalo by se říci, že kód v informačním prostředí nahrazuje přírodní zákony či Boží vůli, nejedná se o pouhý program, ale jde o vícevrstvý, víceúrovňový komplex systémů, proto je jeho případná změna velice náročná. Kdo však vládne takovými prostředky, tedy diskrecí, zda kód následovat či nikoliv, protože ho dokáže obejít či změnit, má v informačním prostředí faktickou možnost měnit kauzalitu daného prostředí ostatním běžným uživatelům, kteří nedosáhnou hranic definičních norem, nenarazí na bariéry možného, které jsou kódem stanoveny. Ti pak považují informační prostředí regulované kódem za přirozené a jaksi intuitivní. „*Využití definiční normy či kódu k regulaci chování je tedy možné srovnat s využitím přírodního zákona. Kód však, na rozdíl od přírodního zákona, není kauzálním pravidlem světa bytí, ale normou. Existuje zde tedy transparentní a v porovnání s Bohem i relativně dobře dosažitelná autorita, která kód vlastním*

[31] Srov. SIEBER, U. LEDERMAN, E. *Conceptualizing Informational Law. In Law, Information and Information Technology.* The Hague: Kluwer Law International, 2001. str. 17-18.

[32] Viz. POLČÁK, R.. *Internet a proměny práva.* Praha: Auditorium, 2012. ISBN 978-80-87284-22-3, str. 95 a násl. a str. 347 a násl.

[33] Viz LESSIG, L. *Code V. 2.* New York: Basic Books, 2006, str. 234.

[34] POLČÁK, R. *Právo a evropská informační společnost.* Brno: Masarykova Univerzita, 2009. ISBN 978-80-210-4885-0. str. 147.

chtěním vytváří a implementuje. Na rozdíl od přírodních zákonů tedy můžeme kódu nejen využít, ale můžeme jím chování i přímo regulovat tak, aby odpovídalo chtění příslušné autority.“[35] Pokud tedy přijmeme existenci definičních norem schopných měnit kauzalitu informačního prostředí, můžeme pak dovodit povinnost autorit zabezpečit ochranu takovýchto norem před poškozujícími zásahy, tedy dovodit nejen ochranu distributivních informačních práv, ale i nedistributivní právo na elementární kybernetickou bezpečnost. Jak jsme uvedli výše, definiční normy jsou projevem chtění autorit a naplňují ve své podstatě systém kauzalitou, platnou ale jen pro ty, kteří této kauzalitě utéci nemohou z důvodu nízké úrovně technologické zdatnosti. Pokud tedy takováto norma není sama o sobě schopna zajistit svoji vymahatelnost a stálost a narušení takové normy by znamenalo ohrožení všech, kteří jsou svázáni jí vytvořenou kauzalitou, je nutný nástup vnějších forem regulace k ochraně právě těchto atributů, tedy nástup vnějšího, právního normativního systému, je nutné zajištění kyberbezpečnosti státní či nadstátní regulací; skrze existenci definičních norem tedy dovodíme potřebu a současně i legitimitu takovéto regulace.[36]

Ovšem otázka, v jaké míře právně regulovat informace, je samostatnou kapitolou. Sice mohou být chráněny klasickými instituty práva, jako jsou utajované skutečnosti, osobní údaje, obchodní tajemství či duševní vlastnictví, nicméně zvláště s rozvojem ICT informace nabývají několik specifik. V takovémto případě jde právě o snadnou dostupnost (tedy je lze i snadněji odcizit, zfalšovat či znehodnotit), ale jedná se právě i o určitou novost a překotný vývoj fyzických nosičů, s nimiž jsou informace nerozlučně spojeny. Toto velmi ztěžuje legislativní proces již v jeho počátku. Zákonodárce má velice málo vzorů, zkušeností či jen pouhých představ o tom, co regulace té či oné informační oblasti přinese. Jak už jsme uváděli výše, informace a její výměna se váže k lidstvu od nepaměti, z toho důvodu je její regulace a ochrana obsažena snad v každém právním oboru. To na co je však třeba reagovat, je právě onen nový prostor, přinášející naprosto nové způsoby přenosu informací, nové možnosti jejich zneužívání, a tedy i nové výzvy pro právní regulaci. Klade nároky současně na jednoznačnost a zároveň na dostatečnou nadčasovou obecnost.

---

[35] POLČÁK, R. *Právo a evropská informační společnost.* Brno: Masarykova Univerzita, 2009. ISBN 978-80-210-4885-0, str. 148 – 149.

[36] Srov. SIEBER, U. LEDERMAN, E. *Conceptualizing Informational Law. In Law, Information and Information Technology.* The Hague: Kluwer Law International, 2001. str. 32 a násl.

1.3. Kyberkriminalita a kyberbezpečnost

1.3.1. Kyberkriminalita

Pokud se tedy máme dobrat původu kyberkriminality, je nutné se vrátit téměř na samotný začátek. Rozvoj ICT započal již v polovině 20. století, docházelo k miniaturizaci a tím i rozšíření, v souvislosti s tím bylo sestaveno několik prvních programovacích jazyků. Za kolébku rozvoje jsou považovány Spojené státy americké, především pak soukromá univerzita MIT, kde se soustředila skupina, která je označována za první hackery. *„Studetská organizace TRMC (Tech Model Railroad Club) byla založena v roce 1946 Johnem Fitzallenem Moorem a Waltrem Marvinem. Klub se věnoval, jak název napovídá, budování modelové železnice v rozměru H0; tzv. Signals and Power Subcommittee byla podskupina zkoumající, jak vytvořit systémy a sehnat vybavení (relé, spínače a prvky z telefonních ústředen), s nimiž by bylo možné modelovou železnici automaticky řídit; právě tato skupina vytvořila na sklonku padesátých let velmi specifickou subkulturu prvních hackerů.“*[37] Hacker je tedy *„člověk, kterého baví zkoumat detaily programovatelných systémů a způsoby jak maximálně využít jejich schopností, na rozdíl od běžných uživatelů, kteří většinou dávají přednost pouze nezbytnému minimu znalostí.“*[38]

Přeci jen však, vzhledem k úrovni tehdejšího technologického pokroku, nedosáhl hacking značnějšího rozšíření. Toho se mu dostalo až později, sestavením integrovaného obvodu, avšak stále nízká dostupnost ICT omezila hacking na využití telefonu – zde vzniká tzv. phreaking, proslavený především případem Johna Drapera, který pomocí dětské píšťalky dosahoval tónu o určité frekvenci, nutné k získání bezplatného hovoru. Píšťalka byla běžnou součástí balení cereálií Captain Crunch. Zabezpečení telefonních ústředen provozovateli poté vedlo ke vzniku Blue Boxu. Technologické zneužití telefonu však nebylo jediným možným způsobem, doplňovalo ho ještě sociální inženýrství, tedy způsob, při kterém se klame lidský substrát. Tato metoda se dodnes uplatňuje v mnohých druzích hackingu. Její úspěch spočívá ve využití psychologických poznatků, lži a klamu na jedné straně, při současné neostražitosti, naivitě

[37] ERBEN, L. *Příchod hackerů* – TMRC: hackeři modelových železnic 20. 8. 2013, © 1998 – 2015 Root.cz (online) ISSN 1212-8309, dostupné z: http://www.root.cz/clanky/prichod-hackeru-tmrc-hackeri-modelovych-zeleznic/

[38] KOŠATA, B. *Hacker? Kdo to je?* 1. 11. 2000, © 1998 – 2015 Root.cz (online) ISSN 1212-8309, dostupné z: http://www.root.cz/clanky/hacker-kdo-to-je/

a momentu překvapení na straně druhé. Vzrůstající společenská nevole nakonec vyústila ve vyšetřování a následné odsouzení několika phreakerů (John Draper byl mezi nimi), což způsobilo nezvratný úpadek phreakingu jako takového.

Hackingu však v tuto dobu nastávaly zlaté časy. Uvedení prvního osobního počítače na trh a jeho rychlé zdokonalování od té doby zpřístupnilo ICT širší veřejnosti; tento rozvoj pak samosebou znamenal i velký rozkvět hackingu. Vedle klasického hackingu se rozvíjel i tzv. *„hardwarový hacking“,* tedy pokusy o spojování jednotlivých komponent do sítí či o stavbu vlastních počítačů. Před příchodem internetu spolu hackeři komunikovali pomocí BBS, pořádali hackerské meetingy, zakládali kluby, ve kterých si vzájemně radili, spolupracovali, sdělovali informace. Je tedy jasné, že naprosto zásadní význam pro pokrok ICT a jejich přiblížení širokým masám měli téměř výlučně hackeři. Jejich zájem o ICT, jejich smysl pro čest, pro hackerskou etiku, ideály a hodnoty, které mezi sebou vytvořili a uznávali, je skutečně postavila do čela lidského pokroku v tomto směru.

Zlom ovšem nastal ve chvíli přesunu komerčního zájmu do sféry kyberprostoru. ICT přestávaly být výlučně akademicko-vědeckou záležitostí několika fanoušků tohoto oboru, ale přesouvaly své těžiště do soukromého sektoru, setkávaly se s komerčním využitím a značným úspěchem. Hackerská skupina se rozštěpila na dva proudy. První pokračoval ve svém dosavadním zaměření, z druhého postupem času vznikla právě kyberkriminalita. Hackeři se od této doby (polovina 80. let 20. století) dělí na *„Briliant hackers“* – ti tvoří skutečný výkvět, dále pak na *„White hat hackers“, kteří se* hackerské aktivity snaží udržet v mezích etiky a legitimity. Tito hackeři nebojují ani tak proti kyberbezpečnosti, argumentují pouze ohledně její extenzity a intenzity, v rámci ideologie freeshare jsou pro ně přijatelná pouze minimální bezpečnostní opatření, zajišťující pouze bezpečný provoz základních páteřních schopností informačního systému, tedy udržení formy, nikoli kontrola obsahu. Tato skupina se často díky svým schopnostem pro odhalování bezpečnostních rizik nechává zaměstnávat jako vývojáři nových bezpečnostních softwarů. Jakousi skupinou mezi jsou *„Gray hat hackers“,* nejbližší původní vlně, stále lpící na hackerských hodnotách a hackerské etice. Jejich pokusy v rámci kyberprostoru nejsou zcela legitimní, nicméně slouží právě jen k sebezdokonalení; jejich motivací není zisk a primárně ani působení škod. Průnik do systému je jim sám sobě odměnou, další akce převážně nevedou k poškozování datových toků. Poslední skupinou, která se zcela vydělila z hackerské komunity, jsou *„Black hat hackers“,* u nich je rozdíl oproti

předchozí skupině patrný, své schopnosti využívají pro vlastní zisk či za účelem poškozování cizí strany, páchají plošnou viktimizaci na ostatních uživatelích systému. Spadají sem především crackeři, můžeme sem řadit kyberterorismus nebo spíše hacktivismus, součástí jsou také H4H, námezdní hackeři nabízející své schopnosti právě terorismu, k špionáži, či organizovanému zločinu. (Takovou platformou pak může být i na oko legální portál jako například Hackers List apod.)[39] Právě Black hat hackers měli největší podíl na démonizaci hackerské kultury napříč společností, což zapříčinilo exil hackerů na okraj společnosti.[40]

V roce 1984 americký novinář Steven Levy ve své knize *Hackers: Heroes of the Computer Revolution*[41] uvádí šest bodů hackerské etiky:

1. *Přístup k počítačům a čemukoliv, co tě může naučit něco o tom, jak svět funguje, by měl být neomezený a absolutní. Vždy respektuj pravidlo osobní zkušenosti (Hands-on imperative).*
2. *Veškeré informace by měly být dostupné bezplatně.*
3. *Nevěř autoritám, podporuj decentralizaci.*
4. *Hackeři by měli být souzeni podle svých činů a nikoliv podle scestných kritérií jako jsou akademické tituly, věk, rasa nebo pracovní zařazení.*
5. *Na počítači můžeš vytvářet umění i krásu.*
6. *Počítače mohou změnit tvůj život k lepšímu.*

Jedná se jak o etický kodex, tak o jakási základní práva hackera, dodnes jsou tato pravidla veskrze uznávána. Jejich výklad se samozřejmě liší, nicméně existují skupiny, kterými hackeři kvůli neúctě k těmto zásadám vyloženě opovrhují. Jsou jimi především tvůrci virů, jejichž „hack value“ je minimální, díky nedostatku intelektuální hodnoty; napsat vir není až tak složitým procesem, co se tvůrčích vloh týče. Další takovou skupinou jsou zloději, využívající hacking jen jako nástroj. Jejich schopnosti jsou limitované, motivací je především finanční zisk. Poslední opovrhovanou skupinou jsou tzv. *„Insideři“*, odpadlíci od White hat hackerů, kteří často působí jako rádci a pomahači, podporu při uskutečnění útoku si zpětně nechají finančně ohodnotit. Jejich motivací často bývá msta na zaměstnavateli, což povětšinou bývají společnosti zabývající se kybernetickou bezpečností a vývojem softwaru.

[39]Find a professional hacker. © 2015 Hacker's List, dostupné z: https://hackerslist.com/

[40]Viz. HOLT, T. J. SCHELL, B. H. *Hackers and Hacking: A Reference Handbook (Contemporary World Issues)* California, USA, 2013, ABC-CLIO, LLC. ISBN-13: 978-1610692762. 354 s.

[41] LEVY, S. *Hackers: Heroes of the Computer Revolution* 1. vyd. Sebastopol, CA: O'Reilly Media. ISBN 978-1449388393. Překlad je neoficiální, autorův.

Hackerská etika tedy stojí na dvou základních principech: *„Víra, že sdílení informací je správné a dobré a že je etickou povinností hackerů dělit se o své poznatky psaním open-source a usnadňováním přístupu k informacím a počítačovým zdrojům v maximální možné míře; a víra, že „nabourávání" do systémů pro pobavení a získání zkušeností je eticky v pořádku, dokud však nedojde k vandalismu, zcizení informací či porušení jejich utajení."*[42] Oba tyto předpoklady vůbec podmiňují fungování jakýchkoli pravidel šířících se napříč touto subkulturou, jsou však stále mezi hackery široce, i když nikoli všeobecně, přijímány. Většina hackerů, přestože neuznává šest Levyho pravidel, se nadále drží alespoň těchto principů a naplňuje jejich význam vytvářením open-source softwaru. Někteří jsou však přesvědčeni, že by všechny informace měly být volně dostupné. Až takový radikální liberalismus, řekněme téměř utopismus, je však těžko představitelný v praxi.

Jak je patrné, hackerská subkultura má vcelku bohatou historii, svá nepsaná pravidla, vnitřní členění i svůj nezanedbatelný přínos pro rozvoj ICT. Ovšem právě naprostá neinformovanost, mediální očernění, vnímání hackingu pouze v počítačové sféře, sociální konstrukt hackera jako narušeného jedince, ať už psychicky či sociálně; to vše vedlo k celospolečenskému odsouzení hackingu jako původce kyberkriminality. Kyberkriminalitu však musíme rozdělit do dvou základních skupin: za prvé tradiční delikty, páchané online – tam o trestnosti není pochyb, jedná se o trestním právem kriminalizované delikty, které jsou nyní pouze páchány za pomoci ICT; za druhé delikty nové, které lze spáchat právě jen díky ICT. Pokud se hacker dopustí deliktu z první skupiny, nenastává vcelku žádný problém[43], s druhou skupinou je to ovšem podstatně těžší. Jak jsme již uvedli, hackerská subkultura vyrostla na samých základech při vzniku ICT a značně napomohla jejich rozšíření a pochopení. Dlouho byli právě jen hackeři jedinými, kdo se dokázal v kyberprostoru orientovat, spravovat ho. Až teprve ekonomické zájmy určitých skupin a tlak z jejich strany na komerční využití kyberprostoru způsobily rozštěp hackerské formace a zapříčinily formování kyberkriminality jako zcela nové formy poškozování informačních a komunikačních systémů a informací samotných. Činy, které byly původně

[42] KOŠATA, B. *Hacker? Kdo to je?* 1. 11. 2000, © 1998 – 2015 Root.cz (online) ISSN 1212-8309, dostupné z: http://www.root.cz/clanky/hacker-kdo-to-je/

[43] *Míněno ideologicky, o jiných problémech trestání takovýchto deliktů v kyberprostoru už jsme se zmiňovali výše v této práci.*

inicializovány hackery a postupně kriminalizovány za současného očernění celé hackerské komunity, byly vlastně jen prostředkem ideologického boje; boje proti kapitalistickému smýšlení při komercializaci kyberprostoru, ICT obecně.

Kyberprostor dodnes zůstává díky svému nehmotnému charakteru, rozsáhlosti a nemožnosti absolutní kontroly bitevním polem o lidské právo na svobodu a soukromí. Hackerská subkultura stále usiluje o prosazení hodnot rovnosti, svobody a sdílení v rámci kyberprostoru, nerovnováha sil je však jednoznačně patrná. Kapitalistický prvek získává značnou převahu jak přístupem k masmédiím, tak ovlivňováním kontrolních mechanismů, právních řádů, konečně i nesouměřitelně většími finančními prostředky a lidskými zdroji. S postupnou kriminalizací veškerých hackerských aktivit a jejich sledováním se velká většina hackerů uchýlila ke kyberterorismu či hacktivismu.

O kyberterorismu bude řeč dále, hacktivismus spočívá ve spojení politicko-mocenských záměrů a technologických prostředků hackingu za účelem dosahování určitých sledovaných cílů[44], může se jednat jak o pouhou proklamaci, upozornění či pohrůžku, tak o skutečný nátlak. Odděluje se již značně od původních myšlenek hackingu, nicméně zůstává nástrojem k prosazení liberálních antiglobalistických a antikapitalistických projevů v kyberprostoru. Tím se přibližuje právě takovému směřování kyberprostoru, jaké zamýšleli už původní hackeři, jeho pojetí jako otevřeného systému volného a svobodného šíření informací, jejich využití a navrácení, ovládané teorií daru a návratu. Jakousi reflexi tohoto paradigmatu dnes přináší hnutí Open Source Code, založené stále na kultuře daru; celá koncepce funguje na principu volně dostupného softwaru, přičemž uživatelé jsou vyzváni k volnému vylepšování tohoto softwaru, čímž se technologický pokrok posouvá opět kupředu při minimální finanční investici. Jak už jsme uvedli dříve, tato myšlenka prosycuje většinu alternativních subkultur napříč kyberprostorem, s požadavkem na její neomezenost, což vyúsťuje ve střety s organizacemi, majícími na šíření informací a výrobě softwaru finanční zájem.

Právo, právní řády, se tedy potýkají s nelehkým úkolem stanovit, co kyberkriminalitou je a nese s sebou určitou společenskou škodlivost, a co naopak spadá právě do rámce výkonu základních práv informační společnosti či boje za ně.

[44] Srov. POLČÁK, R. GŘIVNA, T. *Kyberkriminalita a právo.* Praha: Auditorium, 2008. Auditorium. ISBN 978-80-903786-7-4. str. 47.

1.3.2. Definice kyberkriminality a absence konsensu

Je třeba si uvědomit, že – a zvláště z pohledu práva- je kyberkriminalita stále velice málo poznaným fenoménem, pokusy o její definování se velice různí dle toho, v jakém diskursu se právě pohybujeme. Absence dlouhodobějších zkušeností, překotný vývoj a minimální sbližující legislativa na mezinárodní úrovni zapříčiňuje definiční roztříštění. Pod pojmem kyberkriminalita můžeme navíc rozumět nespočetný počet druhů škodlivé činnosti, zasahující do téměř všech oblastí lidského života a bádání.

Historicky jsou pojmy jak virtuální realita, tak kyberprostor literárními počiny. Pojem virtuální realita použil francouzský divadelní teoretik, herec a básník Antonin Artaud ve své knize Divadlo a jeho dvojník (Théâtre et son double) roku 1938, termín kyberprostor vymyslel americko-kanadský spisovatel science fiction William Gibson, považovaný za zakladatele kyberpunku. Použil tento pojem ve své povídce Jak vypálit Chrome (Burning Chrome), publikované v časopise Omnia roku 1982. Avšak až ve svém románu Neuromancer z roku 1984 jej definoval jako *„sdílenou halucinaci*“.[45] Pojem kyberkultury je tedy naprosto legitimní, její antisociální motivy a spojení s moderními technologiemi k osvobození jedince ze společenské represe regulativů ostatně v kyberprostoru přetrvávají dodnes.[46]

Ohledně kyberkriminality však už takové jednoduché řešení nenalezneme. Její prvotní označení za kriminalitu počítačovou je již dnes obsoletní. Rozmach ICT technologií zapříčinil, že se tento druh kyberkriminality již nemusí nutně vztahovat pouze na počítače a jejich vzájemnou interakci, ať již jsou nástrojem či předmětem útoku; dnešní záběr je mnohem větší a jako prostředek i cíl může zahrnovat desítky různých zařízení či systémů, které jsou připojeny na nějaký druh informační sítě. Přílišná úzkost pojmu počítačové kriminality by měla být tedy nahrazena rozsáhlejším termínem informační kriminality, resp. kriminality vztahující se k ICT (čistě pojem informační kriminalita by byl přespříliš široký, obsahoval by i činy, které prvek ICT vůbec neobsahují). Někdy se užívá pojmu „high-tech“ kriminalita, avšak ten nezahrnuje pouze obor ICT, ale znamenal by vztažení takové kriminality do všech oborů lidského pokroku, například robotiky, biomedicíny apod. Název kyberkriminalita tedy není právě nejlogičtějším

[45]GIBSON, W. *Neuromancer*, (přeložil Josef Rauvolf) Laser-books, 2010, ISBN 978-80-7193-318-2.

[46] Nadřevo.cz. *Život ve virtualitě* (online) © 2012. Nadřevo.cz, dostupné z: http://nadrevo.blogspot.cz/2010/01/zivot-ve-virtualite.html

vývodem, s přihlédnutím k trestněprávní systematice, kdy se jednotlivé trestné činy označují spíše dle druhu chráněného zájmu, tedy dle objektu, by měl pojem znít asi takto: *„informační trestné činy spojené se zneužitím či poškozováním ICT.“* Jedná se vlastně o výčet možných TČ obsažených v názvu, tedy o činy, jejichž jsou ICT cílem, dále o činy, jejichž jsou ICT prostředkem a nakonec o činy, které se zaměřují na obsah informačního prostředí.[47] Autor však zvolil pojem kyberkriminalita z důvodu jeho masového rozšíření jak mezi laickou veřejností, tak v právním prostředí.

Jako taková je kyberkriminalita relativně nově vzniklým druhem kriminality, bývá též označována jako počítačová či, ještě obecněji, informační kriminalita; její zrod souvisí s kriminalizací chování v prostředí informační společnosti. Z pohledu historického její vznik nepředstavuje nic převratného, pouze kriminalita následovala evoluci lidské společnosti, osvojila si nové prostředky a přizpůsobila se novému prostředí. Z pohledu kriminalistického a sociálního představuje problém kvůli vysoké míře nebezpečnosti a latentnosti, právě díky schopnosti napadnout páteřní systémy, na které je společnost ve svém fungování dnes už téměř odkázána. Kyberkriminalita se pohybuje ve sférách, které jsou jen těžko monitorovatelné, což je dáno zčásti jejich rozsáhlostí, zčásti také inovativností. Díky pokroku, který se pohybuje na hraně zítřka, nabízí toto prostředí pachatelům stále nové a nové možnosti, které mohou částečně objevovat i sami. Otázka prevence sice tvoří účinnou ochranu, z tohoto pohledu ji však musíme chápat zcela jinak, než jak používáme tento pojem běžně. Navíc jeho deteritorializace a supranacionální charakter jej téměř vymyká kontrole ze strany státu. *„Hlavním důvodem, proč má přeshraniční přenos informací dramatický dopad na proměnu práva je to, že datový přenos není nadále možné podrobovat kontrole ze strany státu. Neschopnost řádné kontroly takovéhoto přenosu - pramenící z velkého objemu dat přenášených v reálném čase – je jednoznačně prokázána na případě kódovaných dat a komunikace například přes satelity. Mimoto, extenzivní kontrola takto přenášených informací není ani žádoucí, znamenala by nemístné vměšování státu do soukromých záležitostí. Nicméně tato*

[47]POLČÁK, R. GŘIVNA, T. *Kyberkriminalita a právo.* Praha: Auditorium, 2008. Auditorium. ISBN 978-80-903786-7-4, str. 23 a násl.

neschopnost kontroly vede k „erozi státní suverenity“ a ke „ztrátě moci klasických národních států.“[48]

Pokud tedy mluvíme o kyberkriminalitě jako o obecné informační kriminalitě, nemůžeme náš rozhled omezit pouze na síť, Internet. Ten je sice svým výsostným postavením, masovostí a snadnou dostupností velmi úrodným podhoubím pro raketový růst kyberkriminality, není však jediným prostředím, kde se vyskytuje. Ačkoliv se objevují názory, že kyberkriminalita je pouze virtuální obdobou kriminality obecné, má určité charakteristiky, které ji významně odlišují a tak volají po zavedení jiných institutů prevence, ochrany a stíhání kyberkriminality, než oněch klasických. Na druhou stranu je dobré připomenout, že kyberkriminalita svou pestrostí a škálou možných druhů útoků i cílů rozhodně nepředstavuje uzavřený svět a každý jednotlivý segment vyžaduje svůj unikátní přístup k danému problému. Pravdou je tady potom jakási střední cesta, kdy pojem kyberkriminalita v sobě zahrnuje jak „staré“ kriminální činy, známé klasickému trestnímu právu, kterým rozvoj informačních technologií pouze poskytl nové možnosti, tak objev zcela nových specifických kriminálních činů, umožněných právě až tímto rozvojem.[49]

Nebezpečnost kyberkriminality pak pramení ještě z jednoho aspektu, napadá totiž společnost v jejím nejzranitelnějším, nejchoulostivějším místě. Informační společnost sice zažila nečekaný a závratný boom, nepředstavitelné před dvaceti lety je dnes nudnou všední rutinou a samozřejmou součástí našich životů, statistiky prodeje a rozšíření zařízení, která umožňují přístup do kyberprostoru, se pohybují v astronomických položkách, informační technologie a přístup k informacím jsou dnes esenciální součástí života. Pokud nahlédneme do statistik, zjistíme, že je kolem tří miliard uživatelů Internetu celosvětově, ročně se prodá 350 milionů počítačů a kolem 5 milionů mobilních telefonů za jediný den. Denně pak uživatelé pošlou zhruba 203 bilionů e-mailových zpráv, aktualizují 4 miliony blogů, napíšou 700 milionů tweetů a provedou 4 miliardy hledání ve vyhledávači Google. Zarážející je přitom porovnání s mírou počítačové gramotnosti, která celosvětově dosahuje necelých 40 procent![50]

---

[48] SIEBER, U. LEDERMAN, E. *Conceptualizing Informational Law. In Law, Information and Information Technology*. The Hague: Kluwer Law International, 2001. str. 17. Překlad je neoficiální, autorův.

[49] Srov. BAINBRIDGE,D. *Introduction to Computer Law*, 4. vydání, Harlow: Pearson Education Limited, 2000, s. 285

[50] Data získána z © Worldometers.info (online), dostupné z: http://www.worldometers.info/

Pozorujeme pak přímou úměru stoupající nebezpečnosti v závislosti na tom, jak silně proces informatizace probíhá. Čím vyšší míru organizovanosti nám vyšší míra informovanosti přináší, tím hlubší a rozsáhlejší chaos může být způsoben, kybernetické útoky jsou schopny páchat čím dál větší, cílenější a více ochromující poškození; jak vidíme už jen na příkladu IoT, o kterém jsme mluvili v předchozí kapitole. Denně se stane obětí kybernetických útoků přes 556 milionů uživatelů, tedy šestina všech připojených, přičemž se jen Internetem šíří v každém jednom okamžiku na 150 tisíc různých škodlivých kódů. Přes tento bouřlivý rozvoj kyberkriminality a alarmující škody, jaké může její dopad napáchat na celé společnosti, se prevenci před kyberkriminalitou a boji s ní věnuje stále jen okrajový zájem a prostředky investované do tohoto sektoru jsou v porovnání s jiným financováním stále ještě minimální. (Jen v evropském prostředí roční škody dle nejvyšších odhadů dosahují až neuvěřitelných 388 miliard USD[51], přičemž objem financování programů kyberbezpečnosti v období mezi lety 2013 až 2020 představuje v Evropské unii pouhých 400 milionů eur).

Opětovně je třeba připomenout, že to, co se nazývá kybernetická, počítačová či informační kriminalita, se dá shrnout pod pojem kriminalita související s pokročilými technologiemi. Tedy tento pojem zahrnuje případy, kdy se informace, informační a komunikační technologie či systémy stávají nástrojem, cílem nebo prostředím kriminálního chování. Jak už jsme ovšem naznačili, stále je mezi odbornou veřejností tendence za kyberkriminalitu označovat v úzkém pojetí jen takové jednání proti informačním technologiím, které nemůže být spácháno žádným jiným způsobem.

Je také nutné neplést dohromady veškerou činnost, která se zaměřuje na informace v moderním pojetí a zneužívá je či poškozuje. Kyberkriminalita sice patří do skupiny, jejímž definičním znakem je narušení kvantitativní či kvalitativní úrovně informací, což v důsledku vede ke snižování datové základny informační společnosti a může dospět až k její hypertrofii; nicméně rozdělujícími znaky jsou nikoliv forma či způsob provedení, ale cíl a motiv. Ke kyberkriminalitě se tak řadí ještě kyberterorismus, kybernetická špionáž, kybernetická válka a hacktivismus. Zkoumání těchto druhů možného škodlivého chování v kyberprostoru není účelem této práce, je však třeba si uvědomit, že pro

[51]Evropská komise. *Nové Evropské centrum pro boj proti kyberkriminalitě bude potírat internetový zločin a chránit spotřebitele* (online) © Evropská unie, 1995–2015, dostupné z: http://ec.europa.eu/ceskarepublika/press/press_releases/12_317_cs.htm

potřeby kyberbezpečnosti a její právní úpravy v celém spektru je důležitý způsob narušení a způsobený účinek, nikoliv motiv a cíl narušitele. Jakékoliv poškozování přirozeného informačního toku musí být minimalizováno, motiv či cíl mohou být pouze vodítkem pro předpoklad dalšího průběhu narušení.

Uveďme si tedy jen krátkou charakteristiku těchto pojmů pro zběžné pochopení rozdílu mezi nimi. Kyberterorismus je *„konvergencí terorismu a kyberprostoru, obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu nebo obyvatele k podporování sociálních nebo politických cílů."*[52] Realitou dnešních dnů jsou však cílenější útoky, které narušují fungování určité služby, aniž by směřovaly proti konkrétní společnosti nebo vládě s konkrétním účelem. Kyberteror jako takový zatím nebyl pozorován, teroristické buňky a skupiny se soustředí spíše na logistickou výhodu kyberprostoru, rekrutují členy, sdílejí informace, domlouvají další postup, prezentují se apod. Přesto je hrozba kyberterorismu reálná. Ač zatím k ničemu podobnému nedošlo, kyberteroristický útok na vitální systémy by v důsledku mohl mít na svědomí i lidské životy. *„Obrana před kyber útoky je nyní zmiňována stejně často jako protiraketová obrana a energetická bezpečnost, prohlásil Sulejman Anil, který má na starosti ochranu Severoatlantické aliance před počítačovými útoky. Viděli jsme již mnoho počítačových útoků a myslíme si, že tento problém jen tak rychle nezmizí. Pokud by se proti tomuto nezavedla celosvětová opatření, mohly by se kyber útoky stát globálním problémem,* dodal Anil. *Anil varoval před státy, které by mohly sponzorovat internetové útoky na členské země NATO. Mezi největší hrozby kyber terorismu patří útoky na internetové komunikační sítě nebo útoky na servery oficiálních institucí.“*[53]Na příkladu kyberterorismu můžeme demonstrovat, jak tenká hranice ve vytyčení dotčených pojmů je. Citovaná definice Denningové tak může pouze při záměně slova popsat všechny čtyři uvedené pojmy. Všechny se totiž vyznačují téměř shodnými znaky, jak druhem útoků, tak způsoby provedení, sledovaný cíl je jediné, co je odlišuje. Jde také o neletálnost, tedy nesmrtící účinek těchto útoků.

[52] DENNING, D. E. *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.* (online), dostupné z: http://130.154.3.14/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

[53] Natoaktual.cz. NATO: Kyber terorismus je celosvětovou hrozbou.(online) 6. 3. 2008. © Jagello 2000, dostupné z: http://www.natoaktual.cz/nato-kyber-terorismus-je-celosvetovou-hrozbou-frv-/na_media.aspx?c=A080306_155324_na_media_m00

Většinová společnost, ač konfrontována s následky reálných činů, nepociťuje tak intenzivně dopad kyberútoků, což může vést k banalizování hrozby, jakou představují. Toto rozdělování je tedy vesměs právní a nese s sebou právě rozdílné právní následky. Vezměme kupříkladu fiktivní hackerskou skupinu, pokud by její útoky napadaly systémy čistě v jejím zištném zájmu, jednalo by se o „ obyčejnou“ kyberkriminalitu; pokud by takové útoky byly motivovány finančně, na objednávku nějaké společnosti, jednalo by se o kybernetickou špionáž, jejímž cílem je získání určitého tajemství; motivovány politicky, v zájmu nějakého vyššího uskupení, by znamenaly projev hacktivismu, jenž se právě velice těžko odděluje od kyberterorismu; zde mohou být původcem skupiny organizovaného zločinu či teroristické buňky. Pokud by se ukázalo, že tato hackerská skupina je vojenským útvarem, přičitatelným určitému státu či uznané válčící straně, přesunuli bychom se na úroveň kybernetické války či vojenské kyberšpionáže. Ve všech případech se však může jednat o jeden a ten samý druh kyberútoku, důležité je tedy, ke kterému subjektu je původce útoku vázán, tedy rozlišení se děje na základě toho, kdo *„stojí v pozadí“*, právě na základě motivace.

Kvůli přesycení trhu s běžnými daty, jako jsou přihlašovací údaje, informace o účtech apod. se dnešní útočníci stále více zaměřují na cíle vyšší. Přestože kolem dvou třetin cílů stále leží v soukromé hospodářské sféře, začínají se množit útoky napadající kritickou infrastrukturu, vitální páteřní systémy či útoky zaměřené na hospodářskou špionáž obchodních tajemství. Je přitom až s podivem, jak jsou společnosti v této sféře málo chráněny i proti vcelku amatérským útokům. Cílenému, promyšlenému a chirurgicky přesnému útoku však neodolají bezpečnostní systémy ani na státní úrovni či systémy společností vedoucích pokrok ve vývoji právě těchto systémů, natož aby měl šanci zabezpečit svou osobní zónu a všechna svá zařízení proti případným hrozbám běžný uživatel.

1.3.3. Vztah kyberbezpečnosti ke kyberkriminalitě

„Kybernetickou bezpečnost tedy právo vnímá jako ochranu národního kyberprostoru před bezpečnostními hrozbami. Jednotlivé bezpečnostní incidenty samozřejmě mohou dosáhnout takové intenzity, že se negativně projeví v národním měřítku, tj. dojde například k výpadku páteřní sítě. Většina běžně se vyskytujících incidentů však nedosahuje takové závažnosti, aby bylo nutno se jimi na úrovni národní kybernetické bezpečnosti zabývat – s takovými jevy se pak právo vypořádává za užití standardních ochranných institutů trestního, správního

a civilního práva. Typickým příkladem může být únik osobních údajů nebo průnik do firemního informačního systému.“[54] Jak lépe uvést kapitolu o vztahu kyberbezpečnosti a kyberkriminality než právě těmito slovy pana docenta Polčáka. Vztah těchto dvou pojmů je velice problematický a postrádá ostré a jasné hranice. V širším pojetí je kyberbezpečnost ochranou před jakoukoli hrozbou, jak však dodává citovaný text, z právního pojetí je kyberbezpečností pouze ochrana vitálních systémů, přičemž ponechává širokou oblast pro regulaci jinými instituty a soukromou sféru téměř „na holičkách“, o běžném uživateli nemluvě. Na druhou stranu z tohoto nedostatku potom vznikají zajímavé kooperační projekty a soukromé iniciativy, které se snaží nastalou situaci řešit. Taktéž vznikají centra na státní úrovni, která mají na starosti poskytování informací, řízení takové kooperace, osvětu a pomoc subjektům, které o téma kyberbezpečnosti projeví zájem. Tato centra posléze komunikují na nadstátní úrovni. Jsou jakýmsi mostem právě mezi striktním chápáním kyberbezpečnosti z právního pohledu a onou šedou zónou, do které spadá veškerá ostatní agenda, týkající se kyberbezpečnosti v širším pojetí. Jak poznáme dále, existují i případy, kdy kyberútoky jako takové jsou právem dovoleny, jedná se například o činnosti, které se vztahují k preventivnímu útoku či sebeobraně v rámci válečného konfliktu. Některé jsou zase právně i finančně irelevantní. Jiné jsou pak zcela žádoucí, pokud jsou prováděny k výzkumným účelům pracovníky či hackery, najatými bezpečnostními společnostmi za účelem odhalení bezpečnostních mezer v ochranných systémech. Takovéto pevné a jasné vymezení je proto esenciální pro další právní otázky ohledně kyberbezpečnosti. Je potom velice složité takováto vymezení a pravidla prosadit s mezinárodní platností, to způsobuje, že je právní úprava celosvětově, přes značný pokrok, stále ještě značně neostrá a roztříštěná. Navíc pohled na to, co je kyberkriminalitou a co ne, se liší diskurs od diskursu. Například „*nizozemský poskytovatel webového prostoru CyberBunker prohlásil, že bude hostit všechno, jen v případě dětské pornografie a materiálů spojených s terorismem si vyhrazuje právo využít všech prostředků a takového uživatele odpojit.“*[55] Je to tedy úhel pohledu z druhé strany, který v rámci hackerské etiky nevidí na sdílení nic špatného, naopak dětskou pornografii a terorismus označuje

[54]POLČÁK, R. *Legislativa v České republice.* (online) *Pracovní příručka bezpečnostního manažera*, ISBN: 978-80-7251-364-2. © 2010 - 2015,CyberSecurity.cz, dostupné z: http://www.cybersecurity.cz/law.html

[55] CyberBunker. *Privacy Policy* (online) ©2000-2015 CyberBunker.com, dostupné z: http://www.cyberbunker.com/web/privacy-policy.php

za něco, co už je *„přes čáru“*. Zásah ze strany neziskové organizace Spamhaus pomáhající e-mailovým servisům blokovat spamy, které spočíval v zablokování serverů, pak považoval Cyberbunker za omezení svých informačních práv a spustil kampaň DDoS útoků, které ve svém důsledku dokonce zpomalují Internet. Útoky jsou sice cílené, ale vzhledem k napojení napadených serverů na DNS by se efekt mohl rozšířit i na další internetovou infrastrukturu. Dalším takovým případem byl malware s názvem Flame, jehož původ je zatím neověřen, byl odhalen pracovníky ruské společnosti Kaspersky Labs, kteří ho popsali jako jednu z nejkomplexnějších dosud objevených hrozeb. *„Flame nezpůsobuje hmotné škody, avšak shromažďuje obrovské množství citlivých informací, jinými slovy - krade. Do vyšetřování okolností kyberútoku se zapojila Mezinárodní telekomunikační unie OSN. Komplikovanost viru napovídá, že nejde o dílo nezávislých kyberzločinců, ale některého dosud neznámého státu.“*[56] Všechny tyto zprávy jen ukazují, jak vzrůstá potřeba mezinárodní spolupráce a jednoznačně přijímané a uznané mezinárodněprávní úpravy na poli kyberbezpečnosti.

O kyberbezpečnosti a jejím předmětu jsme se již zmínili výše, nutno připomenout, že pojem kyberbezpečnosti není zcela vyčerpán pojmem kyberkriminality, nejedná se o zcela shodné, synonymní výrazy. Předně, kyberbezpečnost chrání informace před jakýmkoliv poškozením largo sensu (ve smyslu ztráty, odcizení, změny či poškození stricto sensu), zaobírá se tedy ochranou informací při úmyslném, neúmyslném či jiném poškození systému – například při živelných pohromách, pádech systémů z hardwarových či softwarových příčin atd. Nicméně úmyslné útoky nyní tvoří většinu případů, které musí bezpečnostní systémy a týmy kybernetické bezpečnosti řešit. Jak jsme si uvedli v předchozí kapitole, je tedy téměř irelevantní, kdo a proč na nás útočí, důležitá je včasnost- jak odhalení, tak případné reakce a nápravy.

Pokud tedy budeme pátrat po obsahu pojmu kyberbezpečnost a jeho vztahu ke kyberkriminalitě, musíme nahlížet situaci ze širších souvislostí, zahrnout jak nejnovější trendy, právní regulaci a především tento pojem rozložit na dvě části; o původu slova kyber už jsme psali výše v této práci, zbývá nám tedy rozklíčovat, co se rozumí pod pojmem bezpečnost. Je jasné, že náš náhled se zaměří především na právní určení pojmu. Jeho definice bude pak posledním

[56]EuroZprávy.cz. *Experti odhalili největší kyberútok v dějinách, virus řádil 5 let*. © 2009–2015 Active Solutions s.r.o. ISSN 2336-257X, dostupné z: http://zahranicni.eurozpravy.cz/evropa/50239-experti-odhalili-nejvetsi-kyberutok-v-dejinach-virus-radil-5-let/

stupněm, který nám umožní analýzu právního stavu regulujícího kyberprostor ať už v tuzemsku, či v zahraničí.

Bezpečnost v intencích právního řádu může mít spoustu výkladů; od jaderné bezpečnosti, přes bezpečnost práce po bezpečnost potravin, vše má svůj výklad v oboru, v němž se používá. Stránky ministerstva vnitra České republiky v sekci pojmy mluví taktéž o několika druzích bezpečnosti:

- *Bezpečnost*

Stav, kdy je systém schopen odolávat známým a předvídatelným vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí. Je to tedy míra stability systému a jeho primární a sekundární adaptace.
Pro vymezení systému na podmínky státu je obsah bezpečnosti uveden v ústavním zákoně č. 110/1998 Sb., o bezpečnosti České republiky.

- *Ekonomická bezpečnost*

Stav, ve kterém ekonomika objektu, jehož bezpečnost má být zajištěna (státu, seskupení států, mezinárodní organizace apod.), není ohrožena hrozbami, které výrazně snižují nebo by mohly snížit její výkonnost potřebnou k zajištění obranných i dalších bezpečnostních kapacit, sociálního smíru a konkurenceschopnosti objektu i jeho jednotlivých složek, tj. především jednotlivých podnikatelských subjektů na vnitřních i vnějších trzích.

- *Environmentální bezpečnost*

Stav, kdy lidská společnost a ekologický systém na sebe vzájemně působí trvale udržitelným způsobem, jednotlivci mají dostatečný přístup ke všem přírodním zdrojům a existují mechanismy na zvládání krizí a konfliktů přímo či nepřímo spojených s životním prostředím. V tomto stavu jsou minimalizovány hrozby spojené s životním prostředím a způsobené přírodními nebo společností vyvolanými procesy (popř. jejich kombinací) ať už záměrně, nezáměrně nebo následkem nehody. Tyto hrozby mohou zapříčinit nebo zhoršovat již existující sociální napětí nebo ozbrojený konflikt. Absolutní většina z nich navíc nerespektuje státní hranice a často může působit globálně.

- *Vnější bezpečnost státu*

Stav, kdy jsou na nejnižší možnou míru eliminovány hrozby ohrožující stát a jeho zájmy zvnějšku a kdy je tento stát k eliminaci existujících i potenciálních vnějších hrozeb efektivně vybaven a ochoten. Hrozby mohou být vojenské nebo

ekonomické povahy, mohou mít charakter migrační vlny apod. Je to také souhrn mezinárodněpolitických, ekonomických a vojenských vztahů státu s okolními státy a koalicemi, jejichž prostřednictvím prosazuje své státní zájmy.

- *Vnitřní bezpečnost státu*

Stav, kdy jsou na nejnižší možnou míru eliminovány hrozby ohrožující stát a jeho zájmy zevnitř a kdy je tento stát k eliminaci stávajících i potenciálních vnitřních hrozeb efektivně vybaven a k ní ochoten. Je to rovněž souhrn vnitřních bezpečnostních podmínek a legislativních norem a opatření, kterými stát zajišťuje demokracii, ekonomickou prosperitu a bezpečnost občanů, a jimiž stanoví a prosazuje normy morálky a společenského vědomí.[57]

Jak je vidět z tohoto výčtu, bezpečnost tedy označuje stav bez ohrožení, v případě kyberbezpečnosti je ovšem situace složitější, má totiž pouze vnitřní členění, její definice se tedy dá pojmout jako kompilát těchto několika uvedených definic. Je to tedy stav, kdy systém není ohrožen hrozbami výrazně snižujícími jeho výkonnost či je schopen efektivně těmto hrozbám odolávat, hrozby jsou tedy sníženy na minimální možnou míru přípustnou pro to, aby systém mohl ještě stále plnit svou funkci prostoru pro vytváření, sdílení a tok informací. Nejbližší z těchto definic při porovnání je pak definice environmentální bezpečnosti, argumentující systémovou rovnováhou a současnou interakcí lidské společnosti se systémem. Kyberbezpečnost je tedy stav, kdy lidská společnost a informační systém na sebe působí trvale udržitelným způsobem, jednotlivec má rovný a dostatečný přístup k informacím a existují zde mechanismy ochrany před hrozbami. Dokonce i závěrečné souvětí, mluvící o přeshraničním a globálním působení hrozeb, lze uplatnit v mezích kyberprostoru.

Standardy kyberbezpečnosti jsou teprve ve fázi utváření, efektivní systém ochrany představuje enormní výzvu, při které budou muset spolupracovat jak veřejné tak soukromé segmenty, nutná je celková osvěta, mezinárodní sbližování úprav a vzájemná výměna informací a zkušeností. Jedním z nejpoužívanějších standardů je ISO / IEC 27002[58], tvořený dvěma částmi, BS 7799 část 1 a 2, který v roce 1995 vytvořil BSI. Také NIST[59] připravil publikace řešící kyberbezpečnost

[57]Ministerstvo vnitra ČR. *Pojmy- Bezpečnost* © 2015 Ministerstvo vnitra České republiky, dostupné z: http://www.mvcr.cz/clanek/pojmy-bezpecnost.aspx

[58]ISO/IEC 27002:2013(online), © 2013 ISO/IEC dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

[59] Viz. NIST. © National Institute of Standards and Technology (NIST), dostupné z: http://www.nist.gov/

800-12 *"Příručka Informační bezpečnosti"*[60] a 800-14 *"Obecně uznávané zásady a postupy pro zabezpečení informačních technologií"*.[6162] Plynule tedy nyní můžeme přejít k současnému stavu právní úpravy kyberprostoru, nejprve v mezinárodním právu.

[60]NIST SP 800-12 *An Introduction to Computer Security* (online). 1995, National Institute of Standards and Technology, dostupné z: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

[61]NIST SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems*(online) 1996, National Institute of Standards and Technology, Gaithersburg, MD 20899-0001, dostupné z: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

[62] CyberSecurity.cz. *Cyber Security (Kybernetická bezpečnost),* © 2010 - 2015, CyberSecurity.cz, dostupné z: http://www.cybersecurity.cz/basic.html

2. Právní úprava v mezinárodním právu

Kybernetická bezpečnost dnes úzce souvisí s mezinárodními vztahy. Jde o novou oblast lidské činnosti, není tedy dostatečně upravena mezinárodním právem. Pokusů o komplexní mezinárodní úpravu kyberprostoru je ale stále poskrovnu. Tento nedostatek pramení ze samotné povahy kyberprostoru coby svobodného prostoru sdílení informací. Dosavadní hlavní aktéři mezinárodních vztahů – státy a mezinárodní organizace – zastávají stále pouze okrajovou roli, nesmíme zapomínat na nadnárodní společnosti a nevládní organizace. V současnosti vzniká mnoho iniciativ s cílem upravit pouze určité segmenty kyberprostoru. Stále však platí závěr, že mezinárodní úpravy, týkající se kyberprostoru, se nacházejí ve své první fázi.[63]

Přístup k právní úpravě je v zásadě dvojí. Jak už jsme zmínili v předchozích kapitolách, jednoznačná definice kyberkrimiality a kyberbezpečnosti téměř zcela chybí, stejně tak chybí i jednotná úprava. Zastavme se hned na počátku a podívejme se na mezinárodní úpravu kybernetické války, její definici, problémy ohledně autoritativní úpravy a její odlišení od kyberterorismu. Tato vsuvka nám posléze poslouží coby příklad při srovnání s právní úpravou kyberkriminality. Úprava užití kyberútoku jako prostředku ozbrojeného konfliktu jistě patří zcela výlučně do oblasti mezinárodního práva, jeho vymezení nám posléze poskytne odpověď na to, co kyberkriminalitou je a co není.

2.1. Cyber Warfare

Kyberprostor coby novodobé bojiště už není rozhodně pouze science fiction představou, to čemu se říká *„kybernetická studená válka“* dle všeho probíhá již velice intenzivně. Především velké země si navzájem testují obranné mechanismy, špehují se, nicméně kybernetická válka je velice přitažlivá právě i pro malé země. Lze vysledovat posun v trendu zbrojení, kdy se velké finanční sumy začínají investovat do ICT, softwaru a hackerských skupin. Kyberútoky mohou nepřítele poškodit v několika málo minutách, více než konvenční zásahy a

[63] MAURER, T. *Cyber norm emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-security; Discussion Paper #2011-11.* (online) Cambridge © 2011 President and Fellows of Harvard College, dostupné z: http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf

téměř neletálně, tedy beze ztrát na životech. Neužívají se už jen útoky na finanční sektor, ale současné kyberútoky jsou schopny napadat páteřní systémy, rozvodné sítě, mobilní zařízení, cloudové služby či se mohou soustředit na zahlcování kyberprostoru a tím obecně zpomalovat datový tok. Mezinárodní právo tedy musí reflektovat tento nový trend a pružně reagovat na nové možnosti vedení mezinárodního válečného konfliktu. Velice dlouho byla právě tato napadení považována pouze za kyberteror, ovšem je otázkou, zda případy jako jsou Estonsko 2007, Gruzie 2008, Írán 2010, americký bankovní sektor v roce 2012, Jižní Korea 2009, 2011 a 2013, NITRO, či FLAME či současné vzájemné kyberútoky doprovázející válečné dění na Ukrajině nejsou již projevem vojenských operací. Jaká je tedy právní situace?

Odpověď na tuto otázku se snaží přinést Tallinnský manuál mezinárodního práva použitelného na kybernetickou válku, který vydalo v březnu 2013 CCD COE. Přes své úzké zaměření má tento manuál nedozírný dopad na veškeré mezinárodní právo zabývající se kyberprostorem. Předně musíme poznat instituce a prameny, které se danou tématikou zabývají; ozbrojené konflikty spadají do mezinárodního humanitárního práva, hledat budeme tedy v jeho agendě. To se sice zcela specializovaně nezabývá kyberútoky, i na ně však platí mezinárodní pravidla, využitím Martensovy klauzule pak právní experti dovodili platnost zásad humanity i v případech, kdy téměř či zcela chybí přímo aplikovatelné úmluvy. „*Z tohoto můžeme také dovodit, že kyberprostor může být regulován jako analogie fyzického území států a není tedy specifickou oblastí, pro kterou by se měl vytvořit zcela nový soubor norem*.“[64] Za základ je pak nutné vzít čtyři Ženevské úmluvy a jejich Dodatkové protokoly.[65] Mezinárodní humanitární právo však upravuje primárně způsoby ozbrojených konfliktů, které jsou ve své podstatě násilné, vyvstává tedy definiční problém, jak podřadit kyberútok pod ozbrojené útoky

[64]FLÍDR, T. *Mezinárodní právo kyberprostoru a Talinský manuál*. (online) 22. 11. 2013. Kyberbezpečnost © Menier s.r.o. dostupné z: http://www.kyberbezpecnost.cz/?p=198

[65] Ženevská úmluva o zlepšení osudu raněných a nemocných příslušníků ozbrojených sil v poli
Ženevská úmluva o zlepšení osudu raněných, nemocných a trosečníků ozbrojených sil na moři
Ženevská úmluva o zacházení s válečnými zajatci
Ženevská úmluva o ochraně civilních osob za války
Dodatkový protokol k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí mezinárodních ozbrojených konfliktů (Protokol I)
Dodatkový protokol k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí ozbrojených konfliktů nemajících mezinárodní charakter (Protokol II)
dostupné z: http://www.cervenykriz.eu/cz/mhp_knihovna/zenevske_umluvy.pdf

(užití síly) tak, aby se na něj vztahovala stejná pravidla. Kyberútok totiž sám o sobě nesplňuje základní charakteristiku z Dodatkového protokolu I[66], navíc tato definice platí v rámci již vyhlášeného ozbrojeného konfliktu. Aby byl kyberútok takto přijímán, nesmí jít o izolovaný jev a musí způsobit plánované a zamýšlené ztráty na životech či markantní poškození objektů a infrastruktury. Takovéto útoky se tedy budou poměřovat vzhledem k porušení MHP co do své intenzity, způsobu provedení, způsobené škody či utrpení; pak ale některé vcelku očividné kybernetické útoky jednoznačně přičitatelné určitému státu nenabudou povahy užití síly v rámci ozbrojeného konfliktu. Dalším problémem je právě otázka přičitatelnosti – současné metody přičitatelnosti nejsou použitelné v kyberprostoru. *„Kybernetická válka je ovlivňována mnoha způsoby i aktéry natolik, že jejich řešení a určení viníků bývá velice složitou a někdy i neřešitelnou otázkou. Agrese ve formě kybernetického útoku se stále ještě nepovažují za napadení v pravém slova smyslu. Klasický vojenský útok by vyvolal mezinárodní skandál a byl by pravděpodobně příčinou odvety, elektronický útok by mohl zapadnout do ztracena, už proto, že státní účast na něm lze snadno popřít a prokázat ji je obtížné. A na vyšetření podobné události nemusí mít dotyčný stát dostupné prostředky."*[67] Prostředky jako botnety či cloudové služby, rozšířené po celém světě, téměř znemožňují napadenému subjektu shromáždit dostatečné důkazy k přičtení útoku určitému státu. Důležitým aspektem rozlišení od kyberterorismu je také povaha cíle, na který se kyberútok zaměřuje. Rozlišovat je vždy třeba mezi civilními a vojenskými cíli.[68] *„To vše se ovšem týká civilistů, kteří se nepřidali k armádě, ozbrojenému odporu nebo útočící skupině. Hacker, ač civilista, se vzdává práva na ochranu před vojenským útokem nepřátelské strany, pokud se do bojů aktivně zapojí.“*[69]

---

[66] Dodatkový protokol k Ženevským úmluvám z 12. srpna 1949; čl. 49: *"Útoky" jsou násilné činy proti protivníkovi, a to jak útočné, tak i obranné povahy.*

[67] KUŽEL, S. *Kybernetická kriminalita V: Cyberwar už není Sci-Fi.* (online) ©2011-2015 BusinessIT.cz, ISSN 1805-0522, dostupné z: http://www.businessit.cz/cz/kyberneticka-kriminalita-v-cyberwar-uz-neni-sci-fi.php

[68] Dodatkový protokol k Ženevským úmluvám z 12. srpna 1949; čl. 48: *K zajištění respektování a ochrany civilního obyvatelstva a objektů civilního rázu budou strany v konfliktu vždy činit rozdíl mezi civilním obyvatelstvem a kombatanty a mezi objekty civilního rázu a vojenskými objekty a v souladu s tím povedou své operace pouze proti vojenským objektům.*

[69] FLÍDR, T. *Mezinárodní právo kyberprostoru a Talinský manuál*. (online) 22. 11. 2013. Kyberbezpečnost © Menier s.r.o. dostupné z: http://www.kyberbezpecnost.cz/?p=198

Je tedy kyberútok nerozlišující zbraní, která je zakázána? Je třeba připomenout, že obecně užití síly jako prostředku řešení sporů mezi státy je kogentně zakázáno, tento zákaz je explicitně obsažen v článku 2 Charty OSN[70]. Pokud by tedy kyberútok uznaný za užití síly, byl klasifikován jako nerozlišující, byl by zakázán opětovně výslovně i v případě oprávněného ozbrojeného konfliktu. Opět zde záleží na druhu útoku, pokud se bavíme o chirurgicky přesné operaci, jejíž následky se dají lokalizovat a kontrolovat, je jejich užití možné ospravedlnit a za určitých podmínek lze takovéto řešení i upřednostnit, neboť se jedná o nesmrtící zbraň určenou pouze k dočasnému vyřazení personálu či infrastruktury. Ovšem na druhou stranu užití takových prostředků jako jsou viry či botnety, ilustrované případy jako StuxNet či DuQu, jasně ukazuje, že v takovém případě se provedená informační operace může vymknout původci z rukou a napáchat nezamýšlené škody i mimo legitimní, tedy vojenský sektor. Jejich užití je tedy zakázáno coby užití nerozlišující zbraně a to i v případě, kdy je užití síly, v tomto případě prostředků informačních operací a informační války a kyberšpionáže, dovoleno prolomením kogentního zákazu, například při opatření OSN s použitím ozbrojené síly nebo při individuální či kolektivní sebeobraně proti napadení při splnění daných podmínek.[71] Článek 58 Charty OSN je pak aplikován vždy bez výjimky, nehledě na povahu útočníka. Tento aspekt nás přivádí právě k přesahu Tallinnského manuálu mimo vymezení kybernetické války. Všichni aktéři si přirozeně uvědomují, že nebezpečí neskrývá pouze kybernetická válka, navíc při velmi vrtkavé možnosti podřadit určité útoky pod užití síly by pak mezinárodnímu právu a postihu mohla unikat veliká množství škodlivého chování, které poškozuje kyberprostor. Pohled na tuto problematiku se velice rozchází v jednotlivých zemích, tedy ani na půdě mezinárodních organizací nepanuje jednotná shoda.

Autoři Tallinnského manuálu se shodují, že stát se smí kyberútokům bránit ve chvíli, kdy je jisté ohrožení ze strany jiného státu či v případě napadení

[70] Charta Organizace spojených národů a Statut mezinárodního soudního dvora, 24.10. 1945:
3. Všichni členové řeší své mezinárodní spory pokojnými prostředky tak, aby ani mezinárodní mír a bezpečnost, ani spravedlnost nebyly ohrožovány.
4. Všichni členové se vystříhají ve svých mezinárodních stycích hrozby silou nebo použití síly jak proti územní celistvosti nebo politické nezávislosti kteréhokoli státu, tak jakýmkoli jiným způsobem neslučitelným s cíli Organizace spojených národů, dostupné z: http://www.osn.cz/dokumenty-osn/soubory/charta-organizace-spojenych-narodu-a-statut-mezinarodniho-soudniho-dvora.pdf

[71] Charta Organizace spojených národů a Statut mezinárodního soudního dvora, 24. 10. 1945: KAPITOLA VII AKCE PŘI OHROŽENÍ MÍRU, PORUŠENÍ MÍRU A ČINECH ÚTOČNÝCH

skupinou, která je podporována jistým státem. USA se rozchází s autory Tallinnského manuálu v tom, zda je možno provést zásah proti cílům, které jsou sice civilního charakteru, ale slouží válečné mašinérii, tedy proti kritické infrastruktuře, například ropným rafinériím či elektrárnám.

Další názor přináší Ruská federace. Už v září 2011 navrhla společně s Čínou, Tádžikistánem a Uzbekistánem „Mezinárodní pravidla chování v kyberprostoru" a to dopisem Generálnímu tajemníkovi OSN, který ovšem zůstal pouze ve stádiu návrhu. Přesto na Světové konferenci o mezinárodních telekomunikacích[72] byla přes odpor většiny západních států schválena novelizace Mezinárodního telekomunikačního řádu.[73] Principy prosazované Ruskem tak přeci jen doznaly určitého zakotvení; jde například o zvýšenou možnost kontroly států nad internetem oproti současnému decentralizovanému přístupu; zákaz používání kybernetických zbraní a kyberšpionáže; povinnost států stíhat škodlivé aktivity v kyberprostoru. I Tallinnský manuál v pravidle 6 mluví o odpovědnosti za kybernetické operace, které jsou státu přičitatelné a porušují závazek mezinárodního práva. Pokud má ovšem stát nést takovouto odpovědnost ve svém kyberprostoru, musí nad ním mít kontrolu. Takovýto závěr nahrává argumentaci pro větší kontrolu kyberprostoru včetně jeho obsahu. Právě Světová konference o mezinárodních telekomunikacích je takovým pokusem o podrobení internetu kontrole pod správou OSN. To by především znamenalo, že: „*Kyberbezpečnost a soukromí dat by byly podrobeno mezinárodní kontrole; bylo by umožněno, aby cizí telefonní společnosti účtovaly poplatky za „mezinárodní" internetový provoz, možná i „za kliknutí" pro určité webové destinace s cílem nahrabat výnosy státním telefonním společnostem a do vládních pokladen; bylo by možné uvalit bezprecedentní ekonomické regulace jako sazby, termíny a podmínky pro v současnosti neregulované dohody o přenosech provozu známých jako „peering; dále ustanovit panství ITU nad důležitými funkcemi správy internetu s množstvím stakeholderů se subjekty jako je internetová korporace pro udělování jmen a čísel, neziskovka, která koordinuje .com a .org webové adresy po celém světě; zavléct pod mezivládní kontrolu mnoho z funkcí Internet Engineering Task Force, Internet Society a dalších skupin s mnoha stakeholdery, které zajišťovaly*

[72] Konána v Dubaji v prosinci 2012

[73] INTERNATIONAL TELECOMMUNICATION REGULATIONS, Dubai, 2012. Dostupné z: http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf

inženýrské a technické standardy, které internetu umožňují fungovat.“[74] Neblahý dopad na kyberprostor coby svobodnou sféru je tedy patrný, většina západních zemí argumentovala již několikaletou zaběhlou praxí na základě Budapešťské úmluvy[75], která je základním dokumentem pro boj s kyberkriminalitou dnes a tím, že není třeba parcelovat Internet dle státních hranic a podrobit ho tak intenzivní kontrole ze strany státu či nadstátních organizací. Zde je tedy vidět přesah od problémů s kybernetickou válkou, její definicí či právním řešením, do celkového chápání kyberkriminality a snahy o ovládnutí kyberprostoru. Stále více jsou slyšet hlasy, které varují před současným trendem svazování kyberprostoru a kriminalizací jednání jen pro potřeby několika málo interesovaných skupin. Opusťme zde však toto téma, které je předmětem mnohých diskuzí a podívejme se na současnou úpravu kyberkriminality, tedy zaměřme se na současný stav a vývoj mezinárodní spolupráce v této věci. Prostor pro argumentaci ohledně možné budoucnosti a názorů na ideální směřování bude závěrem práce.

2.2. Cybercrime

Vzhledem k nadnárodnímu charakteru kyberkriminalita závisí na mezinárodní spolupráci. Stále budou existovat určité rozdíly v postihu určitého chování. Určitého úspěchu je tedy možné dosáhnout jen přijetím mezinárodních standardizačních úmluv, na které by navazovaly vnitrostátní právní úpravy. Situace je o to složitější v tom aspektu, že kyberprostor přesahuje jakékoliv hranice jurisdikce; mezinárodní spolupráce by tedy nemusela přinášet vysloveně kogentní ustanovení nutně závazná pro přistoupivší kooperující státy, nýbrž jakýsi návod, standardizační balíček, konsensuálně vytvořené normatické minimum, jehož dodržování by vedlo k postupnému snižování informační entropie a hrozby útoků na snesitelné minimum. V dnešním propojeném světě by takové minimum mohlo být měřítkem, jeho nedodržování či porušování by uvrhovalo nespolupracující země do faktického informačního embarga, což by pro vývoj jejich informační společnosti mělo neblahé následky. Vytvoření takového standardu by pak mělo částečně i seberegulační charakter. Jako příměr lze použít námořní dopravu, dopravce si také rozmyslí využití námořních cest či přístavů, ve

[74] AC24.cz. *OSN chce úplnou kontrolu nad Internetem.* (online) © 2011 - 2013 AC24.cz, překlad Miroslav Pavlíček, dostupné z: http://www.ac24.cz/zpravy-ze-sveta/642-osn-chce-uplnou-kontrolu-nad-internetem

[75] CETS No.: 185 Convention on Cybercrime. Budapest, 23. 11. 2001, dostupné na: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

kterých není zaručena alespoň elementární bezpečnost a spolupráce a kde může svůj náklad vcelku snadno bez určitých záruk ztratit.

Mezinárodní spolupráce při stíhání pachatelů kyberkriminality se nyní řídí mezinárodními úmluvami. Problémy jsou dnes způsobeny teritoriálním principem v kontrapozici ke globálnímu charakteru kyberprostoru, stejně jako problémy s vyšetřováním a dokazováním v této oblasti. Nejožehavějšími tématy jsou pak v současnosti oblasti potírání nelegálního a nechtěného obsahu na Internetu; technologická spolupráce pro zkvalitnění kybernetické bezpečnosti; snižování hospodářských škod kyberkriminality a ochrana vitálních systémů před kybernetickými hrozbami.

2.2.1. Mezinárodní právní rámec

Počátky mezinárodních pokusů o normativní řešení v rámci kyberprostoru musíme sledovat u OECD, která jako vůbec první vydala jakýsi návod ohledně možné harmonizace trestních předpisů pro mezinárodní boj s počítačovou kriminalitou, následovalo několik workshopů ve spolupráci APEC-OECD, v roce 2004 byl ustanoven Reakční tým pro SPAM, který přinesl první zprávu v roce 2006. Dnes je v rámci OECD ustanoven WPISP[76], který vytváří mezinárodní návody týkající se kyberbezpečnosti a budování důvěry a spolehlivosti v této oblasti. V roce 2009 pak OECD vydalo knihu s názvem *„Počítačové viry a jiné škodlivé programy: Hrozba pro Internetovou ekonomiku“*[77]

Jako formální základ pro vzájemné mezinárodní uznávání hodnocení uzavřely Kanada, Francie, Německo, Velká Británie a Spojené státy americké v roce 1998 dohodu CCRA (Common Criteria Recognition Arrangement). Česká republika se připojila k této dohodě v září roku 2004. CC jsou také mezinárodní normou ISO/IEC 15408 a pod názvem *"Společná kritéria pro hodnocení bezpečnosti informačních technologií"* byla přijata jako česká národní norma ČSN ISO/IEC 15408.

Vzrůstající důležitosti kyberbezpečnosti si všimla i G8, která v roce 1997 ustanovila Subskupinu pro High-tech kriminalitu, ve stejném roce přijaly její státy Deset principů pro boj s počítačovou kriminalitou, v roce 2000 pak G8 uspořádala

[76] http://www.oecd.org/sti/whatistheoecdworkingpartyoninformationsecurityandprivacywpisp.htm

[77] OECD. *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy*. 2009, 244s. ISBN: 978-92-64-05650-3, dostupné z: http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/computer-viruses-and-other-malicious-software_9789264056510-en#page1

Konferenci o počítačové trestné činnosti. V roce 2011 se uskutečnila schůzka ve Francii, kde byla přijata *Deauvillská Deklarace*[78], obsahující rovněž sekci týkající se Internetu.

Dnes je na mezinárodní úrovni v tomto směru nejaktivnější OSN, jež v roce 1990 přijala v Havaně *„Manuál o prevenci a kontrole trestných činů spojených s počítači"*.[79] Snahy OSN směřují dnes dvojím směrem. První směr je řekněme politicko-vojenský, tedy se dotýká kybernetické války; zde jsou hlavními platformami první výbor Valného shromáždění - politický a bezpečnostní, dále UNIDIR[80], CTITF[81] a především ITU[82], která je právě vedoucí entitou ohledně kyberbezpečnosti v rámci OSN. Pod ni spadá roku 2007 vytvořená GCA jako rámec pro mezinárodní spolupráci. V září roku 2008 organizace ITU a IMPACT[83] uzavřely dohodu o vybudování pobočky GCA v ústředí IMPACT v Malajsii. Důležitost IMPACT spočívá v politické neutralitě, spojení s ITU bylo první komplexní veřejno-soukromou spoluprací svého druhu na světě. Od té doby se IMPACT snaží propojit vlády, průmysl, akademickou půdu a mezinárodní organizace pro společný postup vůči globálním kyberhrozbám. V současnosti se také jedná o nejrozsáhlejší platformu pro zajištění kyberbezpečnosti, které se účastní 152 zemí světa. ITU v říjnu roku 2007 ustavila HLEG, skupinu o téměř sto členech, která do listopadu 2008 vypracovala zprávu obsahující doporučení týkající se právních, technických a procedurálních opatření, organizační struktury, budování kapacity a mezinárodní spolupráce. V roce 2011 ITU vydala knihu Marco Gerckea s názvem *„Understanding cybercrime: A Guide for Developing Countries"*[84], která je dnes považována za jednu z nejlepších publikací ohledně kyberkriminality vůbec. Druhý směr se pak zabývá především ekonomickými dopady kyberkriminality, na řešení této agendy se podílejí především třetí výbor

[78] DEAUVILLE G8 DECLARATION; RENEWED COMMITMENT FOR FREEDOM AND DEMOCRACY, dostupné z: http://ec.europa.eu/archives/commission_2010-2014/president/news/speeches-statements/pdf/deauville-g8-declaration_en.pdf

[79] International review of criminal policy - *United Nations Manual on the prevention and control of computer-related crime,* dostupné z: http://www.uncjin.org/Documents/EighthCongress.html

[80] Viz. http://www.unidir.org/ © UNIDIR 2015

[81] Viz. http://www.un.org/en/terrorism/ctitf/ © United Nations 2015

[82] Viz. http://www.itu.int/en/Pages/default.aspx © ITU 2015

[83] Viz. http://www.impact-alliance.org/home/index.html © 2015 IMPACT

[84] GERCKE, M. *„Understanding cybercrime: A Guide for Developing Countries",* (online) 2. vydání © ITU 2011 493s., dostupné z: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf

Valného shromáždění – sociální, humanitní a kulturní, dále ECOSOC[85], UNODC[86], a UNICRI[87].[88]

Nejdůležitějším nástrojem, kterým OSN disponují, jsou rezoluce; přestože nejsou právně závazné ani vymahatelné u Mezinárodního soudního dvora, představují významný pramen mezinárodního práva. Významné pro mezinárodní kyberbezpečnost jsou pak: Rezoluce Rady bezpečnosti OSN č. 1624 ze dne 14. září 2005, která zavazuje členy k zákazu podněcování páchání aktů terorismu; Rezoluce Rady bezpečnosti OSN č. 68/167 ze dne 18. prosince 2013 o právu na soukromí v digitální době ; Rezoluce Valného shromáždění č. 55/63 ze dne 22. ledna 2001 ; či Rezoluce Valného shromáždění č.65/230 , navazující na závěrečnou Deklaraci přijatou v brazilském Salvadoru na 12. Kongresu o prevenci kriminality a trestním soudnictví. „S odkazem na jedno z hlavních témat kongresu – přizpůsobení systémů trestní justice měnícím se podmínkám světa – vyzvaly členské státy k revizi standardů a norem OSN v oblasti prevence kriminality a trestního soudnictví. Diskuse se na kongresu točily kolem témat využívání nových technologií v boji proti zločinu, včetně kyberzločinu…“ Hlavním motivem pak mělo být vytvoření mezivládní expertní skupiny, která by měla za úkol zpracovat komplexní studii problémů souvisejících s kyberkriminalitou a rozšířit ji mezi členské státy, mezinárodní komunitu a spolupracující subjekty soukromého sektoru, navíc by měla zprostředkovávat výměnu zkušeností, informací o národních legislativách, mezinárodní spolupráci a technickou pomoc. „Debaty se vedly také o způsobech potírání nových forem zločinnosti, například trestných činů ohrožujících životní prostředí, pirátství v oblasti digitálních médií, zcizování identity či kyberzločinů. „Takové zločiny a jejich pachatele je těžké polapit. Pohybují se ve formě digitálních nul a jedniček, finančních transakcí apod. Jsou velmi komplexní, to nás ale nesmí odradit,“ říká Antonio Maria Costa. Jedním z průlomů na kongresu byla shoda mezi státy o potřebě mezinárodního regulačního mechanismu namířeného na boj s kyberzločinem. „Tato shoda může otevřít cestu k úmluvě o kyberzločinu,“ poznamenal Costa.“ Jak je z předchozích řádků vidět, snaha o prevenci a řešení dopadů kyberkriminality není ničím novým, stále je však jaksi decentralizovaná a

[85] Viz. http://www.un.org/en/ecosoc/ © United Nations 2015

[86] Viz. http://www.unodc.org/ ©2015 UNODC

[87] Viz. http://www.unicri.it/ ©2015 UNICRI

[88]CYBERCRIME LAW. *International and regional organizations.(online)* © Cybercrimedata AS, dostupné z: http://www.cybercrimelaw.net/International_organizations.html

málo koordinovaná. Zajímavá organizace je také AFCEA Jedná se o asociaci sdružující více než třicet pět sedm fyzických i právnických osob ve více než sto třiceti zemích. Sídlo asociace je ve Fairfaxu ve státě Virginia, evropská centrála sídlí v Bruselu. Zabývá se otázkami komunikačních, elektronických a informačních systémů, dnes již nejen ozbrojených a bezpečnostních sil, je neziskovou organizací, vytvářející fórum pro vedení dialogu mezi odborníky z řad členů, zástupci vojenských resortů, státní správy a akademické obce. Pořádá také každoroční mezinárodní konferenci ITTE, první již roku 1998. Od roku 2004 organizujeme odborné akce v rámci pracovní skupiny Digitalizace zájmového prostoru a od roku 2010 semináře a odborné akce v rámci pracovní skupiny Kybernetická bezpečnost. Česká pobočka má uzavřenou dohodu o spolupráci s Generálním štábem armády České republiky, s Policejní akademií České republiky v Praze a Univerzitou obrany v Brně.[89]

Než přistoupíme k rozboru v současnosti nejdůležitějšího dokumentu, měli bychom zmínit také soukromé iniciativy. Jedná se například o ICSPA, sdružení národních a nadnárodních společností ve snaze posílit kyberbezpečnost a ochranu obchodních komunit i občanů; snaží se směřovat zdroje a odborné znalosti ze soukromého sektoru na podporu domácích i mezinárodních orgánů. To zahrnuje podporu a poskytování pomoci těm zemím, které se snaží o zvýšení své kapacity a operability vůči kybernetickým hrozbám namířeným proti kritickým infrastrukturám nejexponovanějších zemí. Organizace vznikla v červnu roku 2011 v Londýně, pod záštitou britského ministerského předsedy Davida Camerona, od té doby rozšířila svou základnu do 42 zemí, kde spolupracuje s tisíci subjekty vládního, průmyslového či obchodního zařazení.[90] Dále stojí za zmínku též Global Cyber Security Capacity Centre se sídlem na oxfordské univerzitě. Britská vláda plánuje do tohoto centra investovat jeden milión liber v následujících dvou letech.[91] Úkolem centra bude výzkum efektivního kybernetického zabezpečení a jeho rozšíření jak ve Spojeném království, tak celosvětově, za účelem navýšit jak státní, tak soukromé kapacity k účinné ochraně kyberprostoru, aby nadále mohl udržovat svůj rozvoj a přispívat tak ke zvyšování životní úrovně, dodržování základních lidských práv a celkovému pokroku a prosperitě civilizace. Cílem

[89] AFCEA © AFCEA, dostupné z: http://afcea.cz/ceska-pobocka-afcea/

[90] ICSPA. *About Us* (online) ©2014 International Cyber Security Protection Alliance – ICSPA, dostupné z: https://www.icspa.org/about-us/

[91]HELP NET SECURITY. *UK to host global cybersecurity centre* (online) 9. 4. 2013 © 1998-2015 HELP NET SECURITY, dostupné z: http://www.net-security.org/secworld.php?id=14724

tohoto výzkumu je pak nalezení konsenzuálního kompromisního řešení kyberbezpečnosti ve snaze současně zachovat co nejširší kontrapoziční práva, jako je svoboda projevu a právo na soukromí.[92] Pro obsah budoucích kapitol je zde také záhodno připomenout vznik CERT-CC. V roce 1988 to byla malá, neinstitucializovaná skupinka ICT specialistů, která vznikla jako reakce na rozšíření tzv. „*Morrisova červa*“.[93] Dnes má tato skupina kolem 150 zaměstnanců a je součástí SEI na Univerzitě Carnegie Mellon.[94] [95]O úkolech CERT a CSIRT týmů však až dále v této práci. Zajímavým nástrojem je také veřejná iniciativa GCLD, která zpřístupňuje a porovnává právní úpravu kyberprostoru tak, jak je aktuálně řešena ve více než čtyřech desítkách zemí. Velice přehledně jsou zde ke každé zemi vypsány příslušné vnitrostátní předpisy i závazné mezinárodněprávní dokumenty s uvedeným odkazem na originální text. Tato iniciativa si klade za cíl nejen usnadnění právní komparatistiky, ale i snazší dostupnost informací v tomto odvětví.[96]

2.2.2. Budapešťská úmluva o kyberkriminalitě

Dalším mezinárodním subjektem, pohybujícím se v oblasti zajištění kyberbezpečnosti a potlačování kyberkriminality, je Rada Evropy[97]. Ta v prvé řadě vede na svých webových stránkách přehledný seznam téměř všech mezinárodních organizací a iniciativ, které se zabývají ochranou lidských práv

[92] Global Cyber Security Capacity Centre. *Our aim is to understand how to deliver effective cyber security both within the UK and internationally* (online) © University of Oxford, 2015, dostupné z: http://www.oxfordmartin.ox.ac.uk/cybersecurity/

[93] Morrisův červ (Morris worm) byl jeden z prvních počítačových červů. Jeho tvůrcem byl Robert Tappan Morris, student Cornellovy univerzity. K rozšíření došlo 2. 11. 1988 z institutu MIT. R. T. Morris byl poté prvním obviněným z porušení zákona Computer Fraud and Abuse Act z roku 1986. Federální úřady odhadovaly škody od 100 tisíc do 10 milionů USD, R. T. Morris byl poté odsouzen k tříletému podmíněnému trestu, 400 hodinám veřejných prací a pokutě 10 tisíc USD.

[94] *Hrozba právním postihem ze strany CMU při užití názvu CERT poté vedla k tomu, že po světě vznikaly právě CSIRT, přestože se dnes jedná o skupiny s totožnou agendou.*

[95] CERT, SEI. About Us (online) ©2015 Carnegie Mellon University, dostupné z: https://www.cert.org/about/

[96] Více viz GLOBAL CYBER LAW DATABASE (online) © 2010 - 2015 ASIAN SCHOOL OF CYBER LAWS, dostupné z: http://www.cyberlawdb.com/gcld/

[97] Viz. http://www.coe.int/en/web/portal/home © Council of Europe 2014

před poškozením způsobeným kyberkriminalitou.[98] Největším současným přínosem je ovšem Úmluva o kyberkriminalitě[99] z roku 2001, která sleduje harmonizaci národních právních systémů v oblasti kyberkriminality. Byla přijata spolu se svou důvodovou zprávou Výborem Ministrů Rady Evropy na jeho sto deváté schůzi 8. listopadu 2001 v Budapešti. K podpisu byla předložena 23. listopadu 2001 a v platnost vstoupila 1. června 2004. K současnému dni tuto Úmluvu podepsalo padesát tři členských či nečlenských zemí Rady Evropy, přičemž osm států ji zatím ještě neratifikovalo.[100] Dne 1. března 2006 poté přibyl k Úmluvě ještě Dodatkový protokol, zabývající se kriminalizací projevů rasismu a xenofobie spáchaných pomocí počítačových systémů.[101] Tyto dva dokumenty znamenaly zlom v boji proti kyberzločinu, nicméně je dobré si uvědomit, že se rozhodně nejedná o veškeré kodifikované právo související s kyberkriminalitou. Navzdory tomu společně se všemi doporučeními organizací jako je G8, OECD, OAS, OSN a APEC může pomoci dosáhnout uceleného rámce mezinárodního práva pro kyberkriminalitu. Výše už jsme uváděli na příkladu Salvadorské deklarace, že takové snahy o fúzi rozdrobených norem a doporučení do uceleného komplexního systému už jsou v plném proudu, nicméně i tyto snahy jsou stále jen hudbou (doufejme blízké) budoucnosti, tedy stále je Budapešťská úmluva nejvyšším dosaženým úspěchem mezinárodní spolupráce na poli boje proti kyberkriminalitě.

2.2.2.1. Systematika a obsah Úmluvy

Budapešťská úmluva se dělí na Preambuli a čtyři kapitoly, obsahující celkem čtyřicet osm článků. Po úvodních definicích následuje katalog kriminalizovaných činů, které Úmluva dělí do čtyř skupin, na zločiny proti důvěrnosti, integritě a dosažitelnosti dat a systémů, přičemž sem řadí nezákonný přístup, nezákonné odposlouchávání, narušování dat, narušování systémů

[98] Více viz Council of Europe. *Resources: Anti-cybercrime networks, organisations and initiatives* (online)© Council of Europe 2014, dostupné z: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/networks/Networks_en.asp

[99]CETS No.: 185 Convention on Cybercrime. Budapest, 23. 11. 2001, dostupné z: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[100] Viz. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG © Council of Europe 2014

[101] CETS No.: 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Štrasburk 28. 1. 2003, dostupné z: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

a zneužití prostředků; dále na zločiny se vztahem k počítači, kam patří počítačové padělání a počítačový podvod; za třetí na zločiny se vztahem k obsahu počítače, tedy výroba, distribuce, získávání a držení dětské pornografie na datových nosičích; a nakonec na zločiny se vztahem k autorským nebo obdobným právům. Tyto vymezené skutky musí jednotliví signatáři stíhat. Ale například v České republice[102] lze takovéto skutky stíhat již dle současného práva. Cílem Úmluvy je veškeré skutky sjednotit, aby bylo možné je jednotně, bez výjimek stíhat. Nelze ale opomíjet skutečnost, že Úmluva jakožto mezinárodní úmluva má přednost před zákony, a proto, dojde-li k rozporu vnitrostátní normy s Úmluvou, dojde v takovém případě k aplikační přednosti. Kromě povinnosti stíhat vymezené zločiny Úmluva zasahuje i do dalších oblastí trestního práva. Po signatářích vyžaduje postih rovněž úmyslných forem účastenství (organizace, návod a pomoc) či trestnost pokusu. Zpoždění ratifikace v České republice bylo způsobeno dalším požadavkem, a to na postih též právnických osob, což bylo v ČR zavedeno až rokem 2012.

Následující kapitola se věnuje trestnímu právu procesnímu. Signatářům stanoví povinnosti v oblasti vyšetřovacích postupů a pravomocí a to zejména s ohledem na zajištění urychleného uchování a zpřístupnění uložených počítačových dat, shromažďování dat v reálném čase či odposlouchávání dat, prohlídky a zajištění uložených počítačových dat či vydání příkazu k předložení. Český právní řád neobsahuje takto specifické instituty, jen obecné vymezení, které je ovšem vcelku dostačující. K dosažení účelu Úmluvy je nutné nastavit i základní pravidla mezinárodní spolupráce signatářů, kdy bude ovšem Úmluva působit pouze subsidiárně v případě existence jiné bilaterální mezinárodní smlouvy o právní pomoci či vydávání. Signatáři mají rovněž povinnost určit a provozovat kontaktní místo, na které se mohou ostatní státy obrátit.[103] Jak už jsme však předznamenali, ani Budapešťská úmluva nereflektuje veškeré aspekty kyberkriminality, navíc i přes snahu T-CY či Rady Evropy samotné, například vydáním navazující Rezoluce Rady Evropy č. 1565 (2007)[104], která se snaží reagovat a vystihnou nejpalčivější problémy současného boje s kyberkriminalitou

102 ČR Budapešťskou úmluvu podepsala 9. 2. 2005, ratifikační proces byl ukončen dne 22. 8. 2013 a Úmluva vstoupila v platnost dne 1. 12. 2013.

103 V České republice je takovýmto kontaktním místem Nejvyšší státní zastupitelství, respektive Policejní prezidium.

104 Resolution 1565 (2007) *How to prevent cybercrime against state institutions in member and observer states?*, dostupné na: http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta07/ERES1565.htm

a vyzývá státy nejen k právnímu ošetření, ale i k vývoji účinných systémů zabezpečení kritické infrastruktury a odvolává se také na Úmluvu Rady Evropy pro potlačování terorismu CETS No. 196[105] pro potřeby rozlišení a boje s kyberterorismem, připomíná, že kyberbezpečnostní právo musí stále respektovat základní lidská práva a nabádá k mezinárodní kooperaci, přičemž láká ostatní státy k participaci na Úmluvě; přes to vše Úmluva bezmocně zastarává a nestíhá reagovat na poslední vývoj a trendy ve své oblasti.

Jak z doporučení mezinárodních organizací, tak právě z Úmluvy čerpá pro svou legislativu další velký nadnárodní subjekt, se kterým nadále setrváme v evropském prostoru, je jím přirozeně Evropská unie. Tomuto právnímu prostředí, které se nás přímo dotýká více než jakékoliv jiné, věnujeme následující kapitolu.

[105] Council of Europe Convention on the Prevention of Terrorism, Varšava, 16. 5. 2005, dostupné na: http://conventions.coe.int/Treaty/EN/Treaties/Html/196.htm

3. Právní úprava v právu EU

3.1. Obecně k fungování EU

Na úvod bude nutné přeci jen popsat základní strukturu, principy, historii a fungování EU pro pochopení vztahů, ve kterých tato supranacionální entita ovlivňuje své členské státy a jejich právní řády.

Evropská unie je hospodářské a politické společenství 28 evropských zemí, s 507,7 miliony obyvatel (přibližně 7,3 % světové populace). Základy evropské integrace byly položeny již několik let po konci druhé světové války. V roce 1958 bylo založeno Evropské hospodářské společenství (EHS), od té doby došlo k vytvoření jednotného trhu, postupně došlo ke spolupráci i v řadě jiných, již politických, oblastí.

Samotná EU pak vzniká roku 1993 na základě Smlouvy o Evropské unii, známé jako Maastrichtská smlouva.[106] Veškerá její činnost se odvíjí od smluv a přístupových protokolů, které tvoří primární právo EU[107], běžný legislativní proces (dříve spolurozhodování) mají na starosti tři hlavní orgány: Evropský parlament, přímo volený občany EU, které zastupuje; Rada Evropské unie, složená ze zástupců jednotlivých členských států, předsednictví je dle určitých pravidel putovní, členské státy si ho předávají; a Evropská komise, která má na starosti zájmy EU jako celku, dohlíží na plnění závazků vyplývajících z primárního práva.

V zásadě je to Evropská komise, kdo navrhuje nové předpisy, přičemž Evropský parlament a Rada EU je schvalují. Výsledkem těchto procesů je sekundární právo EU, složené z nařízení, která jsou přímo použitelná, nevyžadují žádnou formu „včlenění“ do vnitrostátních právních systémů; směrnic, které stanovují legislativní cíle a ponechávají státům volný způsob, jak jich dosáhnout, při porušení této povinnosti jim hrozí žaloba za nedodržení smluv i sankční povinnost náhrady škody, která by nevznikla, kdyby stát danou směrnici řádně

[106] SMLOUVA O EVROPSKÉ UNII (92/C 191/01), dostupné na: http://www.euroskop.cz/gallery/2/758-smlouva_o_eu_puvodni_verze.pdf © 2005-15 Vláda České republiky

[107] Primární právo tedy tvoří zakládací smlouvy (Smlouva o Evropské unii, Smlouva o fungování Evropské unie); jejich dodatky a protokoly; jejich novely (především Jednotný evropský akt, Amsterdamská smlouva, Smlouva z Nice, Lisabonská smlouva); Listina základních práv Evropské unie (měla být součástí Smlouvy o ústavě pro Evropu, státy se k jejímu dodržování zavázaly v rámci Lisabonské smlouvy)

implementoval; doporučení a stanovisek, což jsou nezávazné právní akty, vyjádření orgánů EU k určitému problému.[108]

Někdy se též rozlišuje právo terciární, tedy dohody mezi členskými státy, které usnadňují fungování EU, s postupujícím prohloubením evropské integrace však postupně ztrácí na významu. [109]

Dříve, od Maastrichtské smlouvy, se politika EU dělila do tří pilířů: Evropské společenství; společná zahraniční a bezpečnostní politika; spolupráce v oblasti vnitřní bezpečnosti a justice. V takto složité struktuře docházelo k překryvu několika typů pravomocí. Tento systém zrušila Lisabonská smlouva.[110] Evropské společenství je nahrazeno EU, která může plně využívat přidělených pravomocí.[111] Připomeňme, že otázka kyberkriminality a kyberbezpečnosti obecně spadala na pomezí druhého a třetího pilíře, nyní tedy tyto otázky EU formuje jako společnou politiku; zvláštní pravomoci však zůstávají v oblasti společné zahraniční a bezpečnostní politiky, kterou definuje především prostřednictvím předsedy Evropské rady a vysokého představitele Unie pro zahraniční věci a bezpečnostní politiku.[112]

3.2.Legislativa

Nyní je třeba se zaměřit na akty, které oblast kyberbezpečnosti uvnitř EU upravují. Jedná se především o:

- Nařízení Evropského parlamentu a Rady (EU) č. 526/2013 o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA) a o zrušení nařízení (ES) č. 460/2004;

[108] Dále se sem mohou ještě řadit rozhodnutí – což je obdoba vnitrostátních správních aktů, platí pro určitou konkrétní situaci, patří sem i rozsudky Evropského soudního dvora; a historické typy právních aktů, které nepozbyly svojí platnost, například rámcová rozhodnutí, rámcové postoje atp.

[109] Více viz europa.eu. *Jak funguje Evropská unie* (online) © Evropská unie, 1995-2015, dostupné z: http://europa.eu/about-eu/index_cs.htm

[110] Lisabonská smlouva pozměňující smlouvu o Evropské unii a smlouvu o založení Evropské unie CIG 14/07, dostupné z: http://www.euroskop.cz/gallery/2/738-lisabonska_smlouva.pdf © 2005-15 Vláda České republiky

[111] výlučné pravomoci (článek 3 SFEU)

sdílené pravomoci (článek 4 SFEU)

podpůrné pravomoci (článek 6 SFEU)

[112] Pravomoci vysokého představitele byly dříve vykonávány vysokým zmocněncem pro společnou zahraniční a bezpečnostní politiku (SZBP) a komisařem pro vnější vztahy.

- Nařízení Evropského parlamentu a Rady ze dne 21. února 2006, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s ustavením veřejně přístupných elektronických komunikačních služeb;
- Nařízení Evropského parlamentu a Rady (ES) č. 1211/2009 ze dne 25. listopadu 2009 o zřízení Sdružení evropských regulačních orgánů v oblasti elektronických komunikací (BEREC) a Úřadu (Text s významem pro EHP);
- Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů;
- Návrh Nařízení Evropského parlamentu o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů);
- Směrnice Evropského parlamentu a Rady č. 2002/20/EC o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice);
- Směrnice Evropského parlamentu a Rady č. 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů ve znění směrnice č. 98/48/ES;
- Směrnice 2013/40 ze dne 12. srpna 2013 o útocích na informační systémy;
- Směrnice Evropského parlamentu a Rady 2002/20/ES ze dne 7. března 2002 o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice);
- Směrnice Evropského parlamentu a Rady 2002/19/ES ze dne 7. března 2002 o přístupu k sítím elektronických komunikací a přiřazeným zařízením a o jejich vzájemném propojení (přístupová směrnice);
- Směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice);
- Směrnice Komise č. 2002/77/ES o hospodářské soutěži na trzích s elektronickými komunikačními sítěmi a službami (soutěžní směrnice);
- Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o určitých aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu;
- Směrnice 91/250/EC, k právní ochraně počítačových programů, zejména pak stanovisko expertů k tomuto Nařízení *"Právní ochrana počítačových programů v Evropě: Průvodce Nařízením Evropského společenství";*
- Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích);

- Směrnice Evropského parlamentu a Rady 2002/22/ES ze dne 7. března 2002 o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací (směrnice o univerzální službě);
- Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců se zřetelem na zpracování osobních dat a o volném pohybu takových dat;
- Návrh Směrnice Evropského parlamentu a Rady Unii č. 2013/2007 (COD) ze dne 7. 2. 2013 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací COM/2013/048;
- Sdělení Komise Evropskému parlamentu a Radě KOM (2007) 228 v konečném znění ze dne 2. 5. 2007 o podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PETs)
- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Politika v oblasti internetu a jeho správa - Úloha Evropy při formování budoucnosti internetové správy (COM (2014) 72 v konečném znění ze dne 12. 2. 2014 - nebylo zveřejněno v Úředním věstníku);
- Sdělení komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů - Sdělení týkající se budoucích sítí a internetu {SEC (2008) 2507} {SEC (2008) 2516} KOM/2008/0594 v konečném znění ze dne 29. 9. 2008;
- Sdělení Komise Evropskému Parlamentu, Radě, Evropskému Hospodářskému a Sociálnímu Výboru a Výboru Regionů boj proti spamu a špionážnímu („spyware“) a škodlivému softwaru („malicious software“) KOM/2006/0688 v konečném znění ze dne 15. 11. 2006;
- Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor (JOIN(2013)01 v konečném znění ze dne 7. 2. 2013);
- Rozhodnutí Rady ze dne 31. března 1992 o bezpečnosti informačních systémů (92/242/EHS);
- Rozhodnutí Rady ze dne 29. května 2000, o boji s dětskou pornografií na Internetu;
- Rozhodnutí Rady ze dne 28. ledna 2002, ke společnému přístupu v oblasti síťové a informační bezpečnosti.
- Rozhodnutí Evropského parlamentu a Rady č. 1351/2008/ES ze dne 16. prosince 2008 o zavedení víceletého programu Společenství pro ochranu dětí využívajících internet a jiné komunikační technologie;

- Rámcové rozhodnutí Rady 2002/465/JHA ze dne 13 července 2002, o Společných vyšetřovacích týmech;
- Rámcové rozhodnutí Rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy;
- Rámcové rozhodnutí Rady 2001/413/SVV o potírání podvodů a padělání bezhotovostních platebních prostředků;
- Rámcové rozhodnutí Rady 2004/68/SVV o boji proti pohlavnímu vykořisťování dětí a dětské pornografii;
- Rámcové rozhodnutí Rady 2005/222/SVV o útocích proti informačním systémům;
- Rámcové rozhodnutí Rady 2005/222/JHA ze dne 24. února 2005, o útocích proti informačním systémům;
- Sdělení Komise Evropskému parlamentu, Radě a Evropskému výboru regionů k obecné politice v boji proti počítačové kriminalitě ze dne 22. 5. 2007;
- Sdělení Komise Radě, Evropskému parlamentu, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů - Strategie pro bezpečnou informační společnost – „Dialog, partnerství a posílení účasti“ {SEK (2006) 656} KOM (2006) 251 v konečném znění ze dne 31. 5. 2006;
- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o ochraně kritické informační infrastruktury *„Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost“* ze dne 30. 3. 2009;
- Stanovisko Evropského hospodářského a sociálního výboru k návrhu rozhodnutí Evropského parlamentu a Rady o založení víceletého programu Společenství pro podporu bezpečnějšího používání Internetu a nových on-line technologií COM (2004) 91 v konečném znění – 2004/0023 (COD);
- Doporučení Rady ze dne 25. června 2001, o kontaktních bodech 24 - hodinové služby pro boj s kriminalitou za použití vyspělých technologií;
- Závěry Rady o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti ze dne 27. 11. 2008.[113]

Výčet těchto pro kyberbezpečnost nejdůležitějších aktů práva EU zaplnil bezmála tři strany, je nutné si však povšimnout, že závazných předpisů je z tohoto výčtu poskrovnu, přičemž páteř tvoří směrnice, které mají čistě harmonizační úlohu a ponechávají členským státům určitou volnost, což není pro regulaci kyberkriminality a jednotnou úroveň právě nejvhodnější; nařízení by naopak byla

[113] Veškeré vyhledávání předpisů práva EU na portále EUR-Lex (online) © Evropská unie, 1998-2015, dostupné z: http://eur-lex.europa.eu/homepage.html

přespříliš rigidní, nereflektovala by překotný vývoj ani regionální potřeby takovéto úpravy. Z tohoto důvodu se v rámci EU vytváří, a to často i ve spolupráci se soukromou sférou, různé agendy, akční plány, programy, iniciativy, zastřešující centra pro interoperabilitu atp. Pojďme se nyní podívat, co vlastně všechny tyto výše uvedené předpisy upravují a jak se orgány EU snaží o naplnění cílů a smyslu těchto ustanovení.

3.3.Strategie EU pro kyberbezpečnost

Jak už bylo řečeno, kyberkriminalita a otázky bezpečnosti kyberprostoru přesahují geografické hranice, tedy jejich zodpovězení vyžaduje naprosto unikátní a svého druhu nový přístup k věci. Již v roce 1999 na zasedání v Helsinkách vyhlásila Evropská komise celoevropskou strategickou iniciativu eEurope - Informační společnost pro všechny. Jejím hlavním cílem bylo poskytnutí výhod informační společnosti všem obyvatelům. Tato iniciativa se postupem času v určitých časových úsecích aktualizovala dle pokroku v dosahování vytyčených cílů. Nejširší rámec, kterým se od roku 2010 EU řídí, se pak nazývá Evropa 2020; jedná se o desetiletou strategii, jejímž cílem je dosáhnout hospodářského růstu. Klade si za cíl pět bodů, kterých chce dosáhnout prostřednictvím sedmi iniciativ; jednou z nich je tzv. Digitální agenda pro Evropu, která sama navrhuje sedm klíčových oblastí, ve kterých je třeba vhodnými nástroji dosáhnout požadovaných cílů; jsou jimi tyto oblasti: [114]

- vytvoření jednotného digitálního trhu
- zlepšení rámcových podmínek pro interoperabilitu mezi výrobky a službami v oblasti ICT
- posílení důvěry v Internet a jeho bezpečnost
- záruka poskytování výrazně rychlejšího internetového připojení
- podpora investic do výzkumu a vývoje
- zvýšení digitální gramotnosti, dovedností a začlenění
- zavádění IKT k řešení společenských úkolů, jako jsou změna klimatu, zvyšující se náklady na zdravotní péči a stárnoucí populace.

K tomu jí mají pomoci vytvořené akční plány a programy, jako je například Akční plán pro eGovernment, zaměřený na zvýšení podílu občanů

[114] European Commission. *Digitální agenda pro Evropu: klíčové iniciativy* (online) © European Union, 1995-2015, dostupné z: http://europa.eu/rapid/press-release_MEMO-10-200_cs.htm?locale=EN

a společností využívajících elektronickou veřejnou správu; program Safer Internet (Bezpečnější internet) cílí na zvyšování bezpečnosti internetu zejména pro děti. Orientuje se i na jevy, jakými jsou tzv. grooming[115]či on-line šikana. Program ISA[116] - Řešení interoperability pro evropské orgány veřejné správy má pak orgánům veřejné správy členských států EU pomoci usnadnit spolupráci a komunikaci elektronickými cestami. Iniciativa i2010 - Evropská strategie pro růst a zaměstnanost, na níž navazuje program CIP ICT-PSP má za cíl sjednocení Evropského informačního prostoru, především pro posílení konkurenceschopnosti a inovací především efektivním využíváním IT státní správou, společnostmi a občany. Nebo například program NGA[117], jehož cílem má být budování informační infrastruktury. V roce 2020 by dle plánu tohoto programu měly mít všechny evropské domácnosti možnost připojit se k internetu rychlostí alespoň 30 Mb/s, polovina z nich pak rychlostí přes 100 Mb/s. Dále je třeba zmínit přípravný program PASR, řízený poradním výborem ESRAB, zabývající se problematikou bezpečnosti infrastruktury; na něj pak navazující VII. rámcový program výzkumu, v jehož prostoru vznikla zvláštní sekce „Bezpečnost a prostor“, kladoucí si za cíl zajištění vývoje technologií a získání znalostí nutných pro bezpečnost občanů před hrozbami zahrnujícími terorismus, organizovaný zločin.

Za zmínku stojí také projekt lokálnějšího rázu CSV4[118],na kterém spolupracují státy Visegrádské skupiny.[119] Má tři oblasti, které se snaží rozvíjet, jsou jimi aktuální a účelná terminologie, náčrt možných scénářů pro nové krizové situace, které by mohly státní orgány lépe připravit na současné kybernetické

[115] situace, kdy se dospělý spřátelí s dítětem s úmyslem jej pohlavně zneužít.

[116] Viz. Ministerstvo vnitra České republiky. *Interoperability Solutions for European Public Administrations - ISA* (online) © 2015 Ministerstvo vnitra České republiky, dostupné z: http://www.mvcr.cz/clanek/interoperability-solutions-for-european-public-administrations-isa.aspx

[117] Více viz Internet pro všechny. *Za 14 evropských miliard do NGA máme mít všichni internet alespoň 30 Mb/s* (online). © 2002 – 2015 Internet pro všechny, o. s ISSN 1801-1160, dostupné z: http://www.internetprovsechny.cz/za-14-evropskych-miliard-do-nga-mame-mit-vsichni-internet-alespon-30-mbs/

[118] Central European Policy Institute. *Cyber Security in the Visegrad Region (CSV4).* (online) © Central European Policy Institute, dostupné z: http://www.cepolicy.org/projects/cyber-security-visegrad-region-csv4

[119] Visegrádská skupina vznikla z úsilí zemí střední Evropy o spolupráci v řadě oblastí společného zájmu v rámci celoevropské integrace.Složena je z České republiky, Maďarska, Polska a Slovenska, více viz. Visegradgroup (online) © 2000–2015, International Visegrad Fund, dostupné z: http://www.visegradgroup.eu/v4-110412

hrozby a konečně rozbor právní úpravy kybernetické strategie EU a snaha o vypracování co nejlepšího návodu na její implementaci[120]

Není samozřejmě možné v této práci postihnout všechny iniciativy, které v rámci EU vznikají, shrňme tedy obecně cíle celé kybernetické strategie EU[121]: sjednocení dnes velmi rozličné úrovně opatření k zajištění kybernetické bezpečnosti napříč členskými státy; související zvýšení konkurence mezi dotčenými kategoriemi subjektů v rámci jednotného trhu EU; nastavení efektivní spolupráce mezi členskými státy a EU; zavedení důvěry a spolupráce mezi soukromým a veřejným sektorem a civilní a vojenskou sférou jednotlivých členských států v oblasti kybernetické bezpečnosti a ochrana základních práv a zásad právního státu v kyberprostoru.[122]

Prozkoumejme nyní orgány, které se snaží tyto cíle naplňovat. První je ENISA. Byla zřízena nařízením č. 460/2004 za účelem zvýšení možností EU, členských států a obchodní komunity při prevenci, odhalování a odpovědí na bezpečnostní hrozby, jimž je informační společnost vystavena; funguje pak od 1. září 2005 a sídlí v Řecku ve městě Hérakleion na Krétě.[123]V rámci své činnosti shromažďuje informace pro analýzu bezpečnostních hrozeb v Evropě a vzrůstajících rizik; poskytuje pomoc a poradenství Komisi a členským zemím ohledně kybernetické bezpečnosti v jejich dialogu s průmyslem v otázkách bezpečnostních problémů hardwarových a softwarových produktů; usnadňuje spolupráci mezi Komisí a zeměmi EU při rozvoji společných metod předcházení obtížím v oblasti bezpečnosti; přispívá k růstu uvědomění a dostupnosti včasných, objektivních a úplných informací o otázkách bezpečnosti sítí a informací pro všechny uživatele; přispívá k úsilí EU spolupracovat se zeměmi mimo EU a s mezinárodními organizacemi, snaží se, aby byl prosazován globální přístup k otázkám bezpečnosti.

---

[120] Ministerstvo vnitra České republiky. *Obecně k agendám EU* (online) © 2015 Ministerstvo vnitra České republiky, dostupné z: http://www.mvcr.cz/clanek/obecne-k-agendam-eu-461106.aspx?q=Y2hudW09Mw%3D%3D

[121] European Commission, *EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive* (online) European Union, 1995-2015, dostupné z: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[122] CAFOURKOVÁ, T. *Cena za kybernetickou bezpečnost* (online) © epravo.cz, a.s. 1999-2015, ISSN 1213-189X , dostupné z: http://www.epravo.cz/top/clanky/cena-za-kybernetickou-bezpecnost-92586.html

[123] Viz. ENISA. ©2013 European Union Agency for Network and Information Security, dostupné z: https://www.enisa.europa.eu/about-enisa

Další organizací fungující v rámci EU a sledující kyberkriminalitu z trestněprávního a kriminalistického hlediska je EUROPOL, jeho nejnovějším počinem ohledně tohoto tématu je publikace iOCTA (The Internet Organised Crime Threat Assessment)[124], kterou má na svědomí EC3[125], centrum fungující v rámci EUROPOLU coby středisko pro boj s kyberkriminalitou v Evropě. Zaměřuje se na nezákonnou činnost organizovaného zločinu. Úkolem centra je varovat členské státy před kybernetickými hrozbami a upozorňovat na nedostatky jejich bezpečnostních systémů. Identifikuje organizované sítě a nebezpečné pachatele trestných činů a zároveň poskytuje podporu při vyšetřování, od forenzní pomoci až po pomoc při vytváření společných vyšetřovacích týmů, soustřeďuje jak informace z veřejných i soukromých zdrojů, od policejních orgánů a akademické obce, reaguje na dotazy o specifických technických a kriminalistických otázkách. Má se také stát platformou pro diskusi s partnery na mezinárodní úrovni při spolupráci na iniciativách v oblasti kyberkriminality.[126]

Čas musíme věnovat i evropské platformě NIS, složené ze zástupců soukromého i veřejného sektoru, soukromých subjektů operujících v nejvíce dotčených sektorech, ale i organizací sdružujících např. spotřebitele. Jejím úkolem je širokospektrá diskuze ohledně kroků, které by měly být učiněny v rámci zlepšování možností účinných kyberbezpečnostních opatření. V současnosti sdružuje něco přes sto dvacet rozličných organizací. Činnost platformy slouží k dalšímu směřování strategie kybernetické bezpečnosti. Jejím hlavním výstupem má být Strategická výzkumná agenda pro zabezpečení ICT, která bude klíčovým zdrojem pro Evropskou agendu výzkumu a inovací.[127]

Velice účinný a efektivní nástroj rychlé odpovědi na právě probíhající hrozby a za účelem jejich zamezení představují CERT/CSIRT. V evropském prostředí sjednocení představuje EGC[128], tedy sdružení národních CERT týmů.

---

[124] The Internet Organised Crime Threat Assessment 29. 9. 2014, dostupné z: https://www.europol.europa.eu/iocta/2014/toc.html

[125] Více viz EUROPOL. European Cybercrime Centre (EC3) © 2015 Europol, dostupné z: https://www.europol.europa.eu/content/megamenu/european-cybercrime-centre-ec3-1837

[126] Evropská komise, zastoupení v České republice. *Nové Evropské centrum pro boj proti kyberkriminalitě bude potírat internetový zločin a chránit spotřebitele* (online) 28. 3. 2012. © Evropská unie, 1995–2015, dostupné z: http://ec.europa.eu/ceskarepublika/press/press_releases/12_317_cs.htm

[127] European Commission. *NIS Platform - Kick-off meeting of the the Working Groups* (online) 27. 9. 2013 © European Union, 1995-2015, dostupné z: http://ec.europa.eu/digital-agenda/en/news/nis-platform-kick-meeting-working-groups

[128] Více viz EGC Group © 2006-2014 EGC, dostupné z: http://www.egc-group.org/

Členů EGC je v současnosti čtrnáct a náplň jejich činnosti spočívá ve společném vytváření opatření, vhodných k vypořádání se s rozsáhlými i regionálními síťovými bezpečnostními hrozbami; v zajištění sdílení informací a výměny zkušeností o bezpečnostních hrozbách, o výskytu a vývoji škodlivých kódů, též o zranitelnostech systémů; ve sdílení specializovaných vědomostí a expertíz uvnitř skupiny; v určení oblastí společného výzkumu a vývoje; v komunikaci výsledků s ostatními iniciativami a organizacemi. Uvědomujíc si nadnárodní rozměr kybernetických hrozeb, spolupracuje ECG s dalšími CERT iniciativami, většina členů je zároveň členy FIRST a TFCSIRT, což jsou nadnárodní platformy pro komunikaci a přenos hlášení o rizikách a zkušenostech s nápravou bezpečnostních trhlin, sdružují CERT a CSIRT týmy z celého světa.[129]

V neposlední řadě je nutno uvést také váhu soudních rozhodnutí. Vzpomeňme dvě nejvýznamnější, a to Rozsudek Soudního dvora (velkého senátu) ze dne 13. května 2014, ve věci C 131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González, který fakticky zavedl právo „být zapomenut“[130], rozhodnutí SDEU ze dne 8. dubna (ve spojených věcech C-293/12 a C-594/12) posuzoval soulad tzv. data retention směrnice (2006/24/EC) s Chartou základních práv EU. Směrnice byla dle SDEU přílišným zásahem do soukromé sféry občanů a byla rozhodnutím zrušena. [131]

Problém právní úpravy kyberkriminality a otázky politiky kyberbezpečnosti v EU jsou příliš objemné vzhledem k rozsahu této práce. Dopad právních úprav a míru ovlivnění lze nejlépe ilustrovat na projevu, podobě, jakou nabývá reflexe takovéto regulace a harmonizace v jednotlivých právních řádech členských států. V tuto chvíli se tedy přesuňme k právní situaci ohledně kyberkriminality a kyberbezpečnosti obecně v právním prostředí České republiky.

---

[129] Více viz terena © GÉANT Association, dostupné z: https://www.terena.org/activities/tf-csirt/
FIRST, Improving security together © 1995 - 2015 by FIRST.org, Inc., dostupné z: http://www.first.org/

[130] Viz. SLANINA, J. *PRÁVO BÝT ZAPOMENUT A DALŠÍ DOPADY ROZSUDKU SDEU C-131/12 GOOGLE SPAIN* (online) © © epravo.cz, a.s. 1999-2015, ISSN 1213-189X, dostupné z: http://www.epravo.cz/top/clanky/pravo-byt-zapomenut-a-dalsi-dopady-rozsudku-sdeu-c-13112-google-spain-94498.html

[131]VOBOŘIL, J. *JAKÉ BUDOU DOPADY ZRUŠENÍ SMĚRNICE O DATA RETENTION?* (online) © epravo.cz, a.s. 1999-2015, ISSN 1213-189X ,dostupné z: http://www.epravo.cz/top/clanky/jake-budou-dopady-zruseni-smernice-o-data-retention-94415.html

4. Právní úprava v českém právním řádu

4.1. Legislativní vývoj

Žádost o vstup do Evropské unie podala vláda České republiky 17. ledna 1996, žádosti bylo vyhověno k 1. květnu 2004. Už při přístupových jednáních bylo podmínkou určité sbližování právních řádů, cílem bylo dosáhnout určité standardizace u nově přijímaných členů. Právo EU tedy náš vnitrostátní právní řád nepřímo ovlivňovalo již před rokem 2004. Pojďme popsat tento historický vývoj právních předpisů a vládních akcí ovlivňujících kyberprostor. Zpočátku se otázce kyberkriminality a informační společnosti vůbec věnovalo velice málo prostoru, nicméně fakticita, reálné vytváření informační společnosti, nakonec počalo vyvíjet tlak i na formálně-právní struktury. Kyberprostor se stal realitou, se kterou se muselo právo vypořádat, pochopit ji, zpracovat, navrhnout optimální řešení a přijmout ho do svých struktur. V roce 1993 byla vydána Ministerstvem hospodářství první verze přeložených harmonizovaných evropských kriterií pro hodnocení bezpečnosti informačních technologií ITSEC (Information Technology Security Evaluation Criteria). Byly tím vytvořeny předpoklady pro to, aby jak ze strany výrobců produktů a systémů IT, tak ze strany jejich uživatelů bylo pohlíženo na hodnocení bezpečnosti IT jednotně. V roce 2000 vznikají dva zákony, 240/2000 Sb. o krizovém řízení a změně některých zákonů a 365/2000 Sb. o informačních systémech veřejné správy, které nesou určité spojení s danou problematikou. Dalšími předpisy, přijatými před rokem 2004 a dotýkajícími se v nějakém směru významněji informační společnosti a kyberkriminality, jsou:

Zákon č. 2/1993 Sb., Listina základních práv a svobod

Zákon č. 110/1998 Sb., o bezpečnosti České republiky

Zákon č. 141/1961 Sb., o trestním řízení soudním

Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže

Zákon č. 121/2000 Sb., autorský zákon

Zákon č. 101/2000 Sb., o ochraně osobních údajů

Zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví

Zákon č. 441/2003 Sb., o ochranných známkách

Zákon č. 527/1990 Sb., o vynálezech a zlepšovacích návrzích

Zákon č. 227/2000 Sb., o elektronickém podpisu

Zákon č. 160/1999 Sb., o svobodném přístupu k informacím

Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon).

Všechny tyto předpisy pouze roztříštěně dávají určitý základ ochraně jednotlivých práv občanů v kyberprostoru; rozmach kyberkriminality ovšem ukázal, že je třeba mnohem většího úsilí a koncepčnějšího přístupu, který se dynamicky vyvíjí zároveň s pokrokem kriminálních činností v kyberprostoru. Začaly se utvářet koncepce, akční plány a strategie na budování legislativního rámce, který by reflektoval aktuální vývoj a doporučení v mezinárodním právu a vhodně a účelně implementoval právní předpisy EU. Postupně tak vznikaly další předpisy, např.:

Zákon č. 40/2009 Sb., trestní zákoník

Zákon č. 127/2005 Sb., o elektronických komunikacích[132]

Zákon č. 480/2004 Sb., o některých službách informační společnosti

Zákon č. 273/2008 Sb., o Policii České republiky

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Zákon č. 89/2012 Sb. občanský zákoník

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a změně některých zákonů (Zákon o kybernetické bezpečnosti)

Usnesení vlády 677/2007, Akční plán plnění opatření Národní strategie bezpečnosti České republiky

Usnesení vlády 564/2011, o Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015

Usnesení vlády 781/2011, o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast

Vyhláška č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení

[132] Ustanovení o takzvaném data retention přitom Ústavní soud pro překročení ústavněprávních limitů zrušil. NÁLEZ Ústavního soudu Pl.ÚS 24/10 ze dne 22. 3. 2011, 94/2011 Sb., N 52/60 SbNU 625 Shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu, dostupné z: http://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-24-10_1 © 2006 AutoCont CZ, a.s.

náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

Vyhláška č. 317/2014 Sb. o stanovení významných informačních systémů a jejich určujících kritériích

Vyhláška 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor

Vyhláška 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací

Vyhláška 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací

Vyhláška 526/2005 Sb., o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti), ve znění vyhlášky č. 11/2008 Sb.

Vyhláška 527/2005 Sb., o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti)

Vyhláška 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.

Vyhláška 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb.

Toto jsou tedy hlavní předpisy postihující oblast kyberprostoru, takto vyjmenované nám samozřejmě nic neřeknou, pojďme se tedy podívat blíže na nejdůležitější z nich.

Vcelku podařená je novelizace trestního zákoníku z roku 2009[133], která reflektovala počítačovou kriminalitu na základě souhrnu z Budapešťské úmluvy, o které byla řeč výše. V tomto směru je určující § 230 Neoprávněný přístup k počítačovému systému a nosiči informací:

[133] ÚSTAVNÍ ZÁKON ze dne 22. dubna 1998 č. 110/1998 Sb., o bezpečnosti České republiky, dostupné z: http://www.zakonyprolidi.cz/cs/1998-110 © AION CS 2010-2015

„(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“

Dále pak obsahově zcela nový § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat:

„(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 180 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný

a) prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup do počítačového systému nebo jeho části, bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti.“

A konečně § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

„(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté

a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo

b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat,

a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“

Nová úprava není něčím zcela novým a nevídaným, je pouze rozsáhlejší, z původního § 257a trestního zákona se vyčlenila dvě ustanovení: § 230 a § 231. Nově je však i nad rámec Úmluvy možnost postihu i hrubé nedbalosti, který bylo nutno doposud řešit soukromoprávními prostředky.[134]Hlavní skupiny TČ postihované trestním zákoníkem se tedy mohou dělit na skupinu TČ spáchaných tzv. „veřejně“, tedy se jedná o podněcování; schvalování trestného činu; výtržnictví; šíření poplašné zprávy; podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod; hanobení národa, etnické skupiny, rasy a přesvědčení; ohrožování mravnosti; šíření toxikomanie; porušování listovního tajemství. Dále jde o skupinu TČ páchaných v prostředí Internetu, tedy o zásahy do cizích programů a databází; kopírování cizích autorských děl; kopírování www stránek; umísťování cizích autorských děl na vlastní stránky, neoprávněné užívání a distribuce počítačových programů; počítačová špionáž; internetová letadla nebo pyramidy; bankovní podvody; zadávání nepravdivých čísel nebo čísel cizích platebních karet. A za třetí jde o skupinu, která by se dala nazvat obecně podvody, Phishing; Pharming; Spear Phishing; Sniffing, sociální inženýrství, převážně §§ 120, 182, 183, 209, 231, 234 TZ.

Opusťme nyní trestněprávní rovinu a podívejme se na možnosti a řešení, které přináší

---

[134] Dříve např. § 415 zák. 40/1964 Sb., *„Každý je povinen počínat si tak, aby nedocházelo ke škodám na zdraví, na majetku, na přírodě a životním prostředí“*

§ 420 „(1) *Každý odpovídá za škodu, kterou způsobil porušením právní povinnosti.“*

Dnes upraveno §2900 zák. 89/2012 Sb., *„Vyžadují-li to okolnosti případu nebo zvyklosti soukromého života, je každý povinen počínat si při svém konání tak, aby nedošlo k nedůvodné újmě na svobodě, životě, zdraví nebo na vlastnictví jiného.“*

§ 2894 a násl. Odpovědnost za škodu a povinnost náhrady škody

Zákon č. 110/1998 Sb., o bezpečnosti České republiky[135] ve svém čl. 1 stanoví, že *„zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot je základní povinností státu“*, a ve svém čl. 5(1) *„Vláda může vyhlásit nouzový stav v případě živelních pohrom, ekologických nebo průmyslových havárií, nehod nebo jiného nebezpečí, které ve značném rozsahu ohrožují životy, zdraví nebo majetkové hodnoty anebo vnitřní pořádek a bezpečnost*“. V návaznosti na něj zákon č. 240/2000 Sb., krizový zákon, který § 1 (1) *„stanoví působnost a pravomoc státních orgánů a orgánů územních samosprávných celků a práva a povinnosti právnických a fyzických osob při přípravě na krizové situace, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením, a při jejich řešení a při ochraně kritické infrastruktury a odpovědnost za porušení těchto povinností.“* Tento zákon má tedy taktéž význam pro trestněprávní regulaci.

Opusťme nyní ovšem trestněprávní rovinu a podívejme se na možnosti a řešení, které přináší legislativa ohledně kyberbezpečnosti, tedy pro prevenci, předcházení a zamezování bezpečnostních hrozeb či odstraňování jejich nepříznivých následků. Zákon č. 110/1998 Sb., o bezpečnosti české republiky[136] ve svém čl. 1 stanoví, že *„zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot je základní povinností státu“, a ve svém čl. 5(1) „Vláda může vyhlásit nouzový stav v případě živelních pohrom, ekologických nebo průmyslových havárií, nehod nebo jiného nebezpečí, které ve značném rozsahu ohrožují životy, zdraví nebo majetkové hodnoty anebo vnitřní pořádek a bezpečnost“*. V návaznosti na něj zákon č. 240/2000 Sb., krizový zákon[137], který v § 1 (1) *„stanoví působnost a pravomoc státních orgánů a orgánů územních samosprávných celků a práva a povinnosti právnických a fyzických osob při přípravě na krizové situace, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením, a při jejich řešení a při ochraně kritické*

[135] ZÁKON ze dne 22. února 2005 č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), dostupné z: http://www.zakonyprolidi.cz/cs/2005-127#cast1 © AION CS 2010-2015

[136] ÚSTAVNÍ ZÁKON ze dne 22. dubna 1998 č. 110/1998 Sb., o bezpečnosti České republiky, dostupné z: http://www.zakonyprolidi.cz/cs/1998-110 © AION CS 2010-2015

[137] ZÁKON ze dne 28. června 2000 č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), dostupné z: http://www.zakonyprolidi.cz/cs/2000-240 © AION CS 2010-2015

infrastruktury a odpovědnost za porušení těchto povinností.“. Dne 15. března 2010 bylo schváleno usnesení č. 205 o řešení problematiky kybernetické bezpečnosti, kterým se Ministerstvo vnitra ČR stalo gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Dne 24. května 2010 bylo usnesením č. 380, zřízena Meziresortní koordinační rada pro oblast kybernetické bezpečnosti. Podpisem memoranda mezi MVČR sdružením CZ. NIC[138] dne 9. prosince 2010 vzniká Národní CSIRT. Vláda České republika přijala usnesení č. 564 ze dne 20. července 2011, kterým schválila Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011 - 2015. Naprosto zásadním počinem poté bylo Usnesení vlády 781/2011, o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Přílohou usnesení je Statut Rady pro kybernetickou bezpečnost.[139] Na základě tohoto usnesení pak v rámci Národního bezpečnostního úřadu vzniklo dne 13. května 2014 Národní centrum kybernetické bezpečnosti (NCKB), sídlící v Brně. Dne 1. dubna nahradilo memorandum uzavřenou mezi CZ. NIC a MVČR nové memorandum s Národním bezpečnostním úřadem. Úkolem NCKB je především provoz vládního CERT České republiky (GovCERT.CZ); spolupráce s ostatními národními i mezinárodními CERT a CSIRT; příprava bezpečnostních standardů; šíření osvěty, IT gramotnosti a podpora vzdělávání v oblasti kybernetické bezpečnosti; provádění výzkum a vývoj v oblasti kybernetické bezpečnosti.[140] NCKB poté v rámci Strategii pro oblast kybernetické bezpečnosti na období 2011 – 2015 plnilo určité úkoly, ČR se pravidelně účastní mnoha mezinárodních cvičení kybernetické bezpečnosti, započalo se s definováním a určováním KII a VIS, a zahájila efektivní spolupráci se subjekty jak na národní, tak na mezinárodní úrovni.

4.2. Milník kybernetické bezpečnosti

Vrcholem snah v rámci Strategii pro oblast kybernetické bezpečnosti 2011 – 2015 pak bylo vytvoření návrhu, na kterém pracovalo NCKB, a posléze přijetí

[138] CZ. NIC, Správce domény CZ © 2015 CZ. NIC, z. s. p. o., dostupné na: https://www.nic.cz/
Další memoranda podepsalo sdružení například s ČTÚ, Ministerstvem obrany, Ministerstvem průmyslu a obchodu a mnohými dalšími.

[139] Rada je poradním orgánem předsedy vlády pro oblast kybernetické bezpečnosti. Více na: http://www.govcert.cz/cs/rkb/rada-pro-kybernetickou-bezpecnost/

[140] NCKB © Národní bezpečnostní úřad, dostupné z: http://www.govcert.cz/cs/

zákona č. 181/2014 Sb., o kybernetické bezpečnosti a změně některých zákonů[141], který byl dne 13. srpna 2014 podepsán prezidentem České republiky, účinný je od 1. ledna 2015. Posléze byly vypracovány dva prováděcí předpisy - vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti[142] a vyhláška o stanovení významných informačních systémů a jejich určujících kritériích.[143] Tento zákon je prakticky obdobou krizového zákona pro řízení v případě bezpečnostních incidentů v kyberprostoru.

Měl by sjednotit pasivní kybernetickou ochrana státu a snadnější rozpoznání a boj s útoky na elektronické úrovni. Lepší ochrany se tak dostane i občanům ohledně jejich osobních dat. Může dojít i k zatraktivnění tuzemského prostředí pro zahraniční investory, což by mohlo pomoci ekonomice. Zákon stojí na dvou zásadách. První je minimalizace zásahu do práv soukromoprávních subjektů, druhou je pak individuální odpovědnost za bezpečnost vlastních informačních systémů. Zajištění kybernetické bezpečnosti státu má dosáhnout pomocí spolupráce mezi soukromými osobami a veřejnou správou k zajištění přehledu o rizicích a pružné reakce na škodlivé bezpečnostní incidenty pro udržení konzistentního informačního prostředí. Povinnými osobami v oblasti kybernetické bezpečnosti jsou dle § 3 :

„a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),

b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem komunikačního systému podle písmene d),

c) správce informačního systému kritické informační infrastruktury,

d) správce komunikačního systému kritické informační infrastruktury a

[141] ZÁKON č. 181/2014 Sb. ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), dostupné z: http://www.zakonyprolidi.cz/cs/2014-181 © AION CS 2010-2015

[142] VYHLÁŠKA č. 316/2014 Sb. ze dne 15. prosince 2014 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), dostupné z: http://www.epravo.cz/top/zakony/sbirka-zakonu/vyhlaska-ze-dne-15-prosince-2014-o-bezpecnostnich-opatrenich-kybernetickych-bezpecnostnich-incidentech-reaktivnich-opatrenich-a-o-stanoveni-nalezitosti-podani-v-oblasti-kyberneticke-bezpecnosti-vyhlaska-o-kyberneticke-bezpecnosti-20344.html © epravo.cz, a.s. 1999-2015, ISSN 1213-189X

[143] VYHLÁŠKA č. 317/2014 Sb. ze dne 15. prosince 2014 o významných informačních systémech a jejich určujících kritériích, dostupné na: http://www.epravo.cz/top/zakony/sbirka-zakonu/vyhlaska-ze-dne-15-prosince-2014-o-vyznamnych-informacnich-systemech-a-jejich-urcujicich-kriteriich-20345.html © epravo.cz, a.s. 1999-2015, ISSN 1213-189X

e) správce významného informačního systému.“

Kromě orgánů veřejné moci podzákonné předpisy související se zákonem definují též subjekty působící v oblasti kritické infrastruktury, jejichž provoz je nezbytný pro fungování infrastruktury, a tedy k zajištění základních potřeb společnosti. Prostředky k zajištění zákon rozlišuje tři, a to bezpečnostní opatření, dělící se na organizační - §5 (2)

„a) systém řízení bezpečnosti informací,

b) řízení rizik,

c) bezpečnostní politika,

d) organizační bezpečnost,

e) stanovení bezpečnostních požadavků pro dodavatele,

f) řízení aktiv,

g) bezpečnost lidských zdrojů,

h) řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému,

i) řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému,

j) akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů,

k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

l) řízení kontinuity činností a

m) kontrola a audit kritické informační infrastruktury a významných informačních systémů“

a technická opatření - §5 (3)

„a) fyzická bezpečnost,

b) nástroj pro ochranu integrity komunikačních sítí,

c) nástroj pro ověřování identity uživatelů,

d) nástroj pro řízení přístupových oprávnění,

e) nástroj pro ochranu před □škodlivým kódem,

f) nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů,

g) nástroj pro detekci kybernetických bezpečnostních událostí,

h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,

i) aplikační bezpečnost,

j) kryptografické prostředky,

k) nástroj pro zajišťování úrovně dostupnosti informací a

l) bezpečnost průmyslových a řídicích systémů,“

dále pak hlášení kybernetických bezpečnostních incidentů a jejich evidence - § 8 - 10; a nakonec protiopatření, tzn. reakce na incidenty. Rozumí se jimi úkony NBÚ, jichž je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací či k řešení probíhajícího kybernetického bezpečnostního incidentu. Jsou definovány tři druhy protiopatření - §11(2) varování, reaktivní protiopatření a ochranné protiopatření. Varování vydává NBÚ, pokud se dozví o hrozbě v oblasti kybernetické bezpečnosti. Reaktivní protiopatření nastupuje ve chvíli, kdy je potřeba aktivně zasáhnout. Vydává se opatřením obecné povahy. Ochranná protiopatření stanoví způsob zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací a lhůtu k jeho provedení. V případě masivního ohrožení je možné vyhlásit takzvaný stav kybernetického nebezpečí (HLAVA III § 21 a násl.) vyhlašovaný předsedou vlády na návrh ředitele NBÚ nejdéle na dobu sedmi dnů s možností prodloužení na maximálně třicet dnů, pokud se ani do té doby nepodaří kybernetické nebezpečí odvrátit, přejde se do tzv. nouzového stavu, který se řídí zákonem o bezpečnosti ČR.

Zákon také stanoví kontrolní prostředky. Kontrolu provádí NBÚ a Ministerstvo vnitra v oblasti kybernetické bezpečnosti. U zákonem povinovaných subjektů, probíhá kontrola plnění uložených povinností. Při poruše může kontrolní orgán uložit zjednání nápravy, případně přijmout opatření. V kritickém případě kompletního ohrožení systému incidentem může být tento systém odstaven z provozu do doby odstranění potíží. Konečně lze uložit pokutu, jako krajní opatření, která může být uložena až do výše 100 000 Kč. V případě neoznámení kontaktních údajů či jejich změny pouze do výše 10 000 Kč. Zákon se také v neposlední řadě snaží sjednotit a ustálit definice důležitých pojmů.[144]

Na dodržování legislativních ustanovení budou dohlížet organizace CSIRT a CERT. Ty hrají klíčovou roli při ochraně Kritické informační infrastruktury Národní CERT je pracoviště provozované zpravidla osobou soukromého práva, které zajišťuje sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti, a to zejména pro osoby soukromého práva. V

[144] Zákon o kybernetické bezpečnosti Vše podstatné k tomu, co přináší nový zákon platný od 1. 1. 2015 (online) © 2014 AutoCont CZ a.s., dostupné z: http://www.kybernetickyzakon.cz/

současnosti je provozován sdružením CZ. NIC na základě memoranda s NBÚ. Pro příště by však měl být provozovatel vybrán na základě výběrového řízení. Ve světě je v současnosti zformováno okolo 300 bezpečnostních týmů typu CERT/CSIRT, které jsou buď členy organizace FIRST, nebo evropské platformy TF-CSIRT či obou. V ČR je aktuálně oficiálně zřízeno a na světovou infrastrukturu napojeno pět bezpečnostních týmů typu CERT/CSIRT – dva působí v prostředí sítě národního výzkumu a vzdělávání CESNET2 (týmy CESNET-CERTS a CSIRT-MU), jeden provozuje sdružení CZ. NIC pro dohled nad sítí sdružení a DNS servery domény .cz (CZ.NIC-CSIRT) a zatím pouze jeden působí v komerčním prostředí – tým Active24-CSIRT provozovaný jedním z předních českých registrátorů společností Active24. Posledním týmem v tomto výčtu je CSIRT.CZ, který je Národním CSIRT týmem České republiky. Týmy typu CERT/CSIRT a jejich infrastruktura obecně nejsou samy o sobě všespasitelné. Jejich existence je však pro oblast budování bezpečnosti internetu, ve kterém hrají svou důležitou roli všichni – správci sítí, služeb, manažeři, kteří rozhodují o zázemí pro efektivní zabezpečení sítí a služeb, ISP, provozovatelé kritických služeb, bezpečnostní složky, stát, a v neposlední řadě také my uživatelé – velice významná.[145] Zákon o kybernetické bezpečnosti však vyvolává i obavy. Za prvé ponechal pouze velmi malý čas na implementaci změn, které přinesl. Odhadem dvacet procent soukromých společností a 80 procent institucí veřejné správy nestihlo splnit požadavky na informační bezpečnost. Dotčené subjekty mají pouze rok na to, aby uvedli svůj systém bezpečnosti informací v soulad se zákonem,[146] který se spíše podobá standardu řízení bezpečnosti informací ISO 27002 než legislativám počinu. Vlastně dosažení certifikace tohoto standardu téměř zaručuje subjektům shodu s dotčeným zákonem. Přesto je zákon o kybernetické bezpečnosti je krokem k bezpečnějšímu informačnímu prostředí. Klade však značné nároky, proto bude nutné hledat efektivní řešení pro podporu naplnění těchto požadavků. „*Je ale postaven na solidních základech a nabízí inspiraci i podnikům, které nejsou součástí povinných osob. Pomůže zvýšit povědomí o bezpečnosti a vhodných praktikách i o tom, že bezpečnost není pouhé jednorázové*

[145] KROPÁČKOVÁ, A. *CERT/CSIRT týmy a jejich role* (online) Root.cz 6. 5. 2013© 1998 – 2015 Internet Info, s.r.o., dostupné z: http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

[146] CIO. *Většina úřadů v ČR nevyhoví nárokům na kyberbezpečnost* (online) 8. 10. 2014, © IDG Czech Republic, a. s., dostupné z: http://businessworld.cz/bezpecnost/vetsina-uradu-v-cr-nevyhovi-narokum-na-kyberbezpecnost-11935

technické řešení problému, ale naopak organizační úsilí podpořené adekvátními technickými řešeními.“[147]

Česká policie v roce 2014 zaznamenala 4348 případů kyberkriminality[148].Vzhledem k tomuto enormnímu nárůstu (v tomto byl kritickým rok 2013), zřídila policie on-line formulář *„Hlášení kyberkriminality“*, umístěný přímo na hlavní stránce internetových stránek policie. Od 1. ledna 2016 by také měla začít fungovat speciální policejní jednotka pro boj proti kybernetické kriminalitě,[149] zvláštní útvar pro kybernetickou válku do budoucna plánuje zřídit i ministerstvo obrany. Posiluje se i mezinárodní spolupráce, například Ubifrance Praha, francouzská agentura pro mezinárodní rozvoj podniků, uspořádala společně s Bull/Atos a za spoluúčasti Komerční banky, první Francouzsko-české fórum kybernetické bezpečnosti.[150]Či intenzivní spolupráce s Izraelem ohledně kybernetické bezpečnosti, která vyústila v podpis několika memorand na společném mezivládním jednání. Společná deklarace v oblasti kybernetické bezpečnosti tedy zavazuje obě strany ke „*sdílení informací a zkušeností s cílem posílit ochranu proti možným kybernetickým hrozbám. Dále si budou vyměňovat informace o výzkumu a vývoji v oblasti kybernetické bezpečnosti.“*[151]

„Kybernetická bezpečnost bude i v roce 2014 jedním z nejdůležitějších témat v oblasti technologií a pravděpodobně i mimo ni. Nedostatek odborníků však může znamenat komplikaci v boji proti kybernetické kriminalitě. Zvláště v nyní, kdy jsou útoky stále sofistikovanější, je důležité zaměřit se na přípravu kvalitních odborníků a vývoj moderních technologií, které by dokázaly čelit takovým útokům v každé jejich fázi, před, během nich i po nich.“ Tato slova Ivo Němečka, technického ředitele společnosti Cisco, upozorňují však také na další aspekt. Studie společnosti Cisco odhaduje, že bude na celém světě chybět více než

---

[147] KRÁTKÝ, P. *Zákon o kybernetické bezpečnosti v praxi* (online) © 2001 - 2015 CCB spol. s r.o. ISSN 1802-615X, dostupné z: http://www.systemonline.cz/clanky/zakon-o-kyberneticke-bezpecnosti-v-praxi.htm

[148]Statistické přehledy kriminality za rok 2014 © 2015 Policie ČR, dostupné z: http://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2014.aspx

[149] České noviny.cz . *Útvar proti kyberkriminalitě by měl fungovat od příštího roku*. (online) 23. 1. 2015 © 2015 ČTK, ISSN: 1213-5003, dostupné z: http://www.ceskenoviny.cz/zpravy/utvar-proti-kyberkriminalite-by-mel-fungovat-od-pristiho-roku/1172499

[150] Francie v České republice. *Francouzsko-české fórum kybernetické bezpečnosti* (online) 19. 1. 2015, dostupné z: http://www.france.cz/Francouzsko-ceske-forum

[151] Vláda ČR. *Členové vlád České republiky a Státu Izrael společně jednali v Jeruzalémě* (online) 25. 11. 2014, © 2009-2014 Vláda ČR, dostupné z: http://www.vlada.cz/cz/media-centrum/aktualne/clenove-vlad-ceske-republiky-a-statu-izrael-spolecne-jednali-v-jeruzaleme-124757/

milion odborníků na IT bezpečnost. Je tedy nutné reformovat a podpořit vzdělání v oblasti IT bezpečnosti a rozšiřování obzorů mezi většinovou populací spějící ke zvýšení procenta IT gramotnosti,[152] což je i jedním z významných cílů schválené Strategie pro kyberbezpečnosti v letech 2015 – 2020, která toto chtěla prosadit také do vzdělávacích programů na základních a středních školách.[153]

„F. Podpora vzdělávání, osvěta a rozvoj informační společnosti
Navyšovat povědomí a gramotnost v otázkách kybernetické bezpečnosti jak u žáků a studentů základních a středních škol, tak i u široké veřejnosti, respektive koncových uživatelů, pomocí podpory iniciativ a osvětových kampaní, pořádáním konferencí pro veřejnost apod.
Modernizovat stávající vzdělávací programy na základní a středoškolské úrovni a podporovat na vysokoškolské úrovni nové studijní programy, které budou přímo vytvářet experty na kybernetickou bezpečnost.
Vzdělávat a školit zaměstnance veřejné správy působící nejen v oblasti kybernetické bezpečnosti a informační kriminality.“

Takovou roli plní například český institut manažerů informační bezpečnosti, profesní sdružení, sdružující přes sto odborníků z mnoha institucí státní správy, finanční a komerční sféry. Toto sdružení bylo založeno roku 2007. Sdružení bylo dokonce akreditováno Ministerstvem vnitra a Ministerstvem školství pro vzdělávání v oblasti informační bezpečnosti.[154] Tato snaha nachází také odraz např. v novém oboru Fakulty elektrotechniky a komunikačních technologií VUT v Brně nazvaný Informační bezpečnost, který je na české poměry jedinečný. *„Absolventi budou vědět, jak funguje etický hacking, jak přistupovat k ochraně dat a soukromí, jak pracovat s šifrováním, cloudy a podobně. Mezi jejich znalosti bude patřit kromě základů matematiky a informatiky také například kryptografie.“* [155]Ač se jedná zatím jen o bakalářský studijní obor, do budoucna se plánuje otevření magisterského přímo navazujícího programu.

---

[152] *Velké části koncových uživatelů nejen v rámci veřejné správy, ale i z řad veřejnosti chybí základní povědomí o běžných metodách počítačových útoků (zejména phishing, falešné e-shopy apod.), jejichž obětí se ročně stávají tisíce občanů České republiky.*

[153] Národní strategie kybernetické bezpečnosti české republiky na období let 2015 – 2020, dostupné z: https://www.kybez.cz/documents/10184/12170/N%C3%A1rodni+strategie/6b03b7f8-0609-4353-aeed-c9fd6bb0d1a1

[154] Více viz ČIMIB. © 2013 ČIMIB, dostupné z: http://www.cimib.cz/stranka/24-o-nas

[155]SPĚŠNÝ, J. *OBOR PROPOJÍ LEGISLATIVU A KYBERBEZPEČNOST* (online) NAVUT.CZ. 20. 3. 2015 2015, ©VUT v Brně, dostupné z: http://www.vutbr.cz/zivot-na-vut/fakta-o-vut/vut-v-mediich/vut-a-media-f19526/obor-propoji-legislativu-a-kyberbezpecnost-d100653

Také se uvažuje o zcela novém koncepčním řešení v zavedení předmětů souvisejících s IT bezpečností do školních osnov.[156] Dalším takovým příkladem může být školící centrum Conceptica[157], provozující Akademii kybernetické bezpečnosti, slibující účastníkům, kterým se může stát prakticky kdokoliv, dokonalou znalost zákona o kybernetické bezpečnosti s cílem jeho uplatnění v praxi, zvýšení kybernetické bezpečnosti informačních systémů organizací, zvýšení efektivity lidských zdrojů, zajištěním správného a bezpečného využití informačních technologií, zvýšení prestiže mezi partnery, know-how v oblasti bezpečnosti, které může být zapracováno do služeb organizace.

[156] *Český model vzdělávání a výchovy v oblasti kybernetické bezpečnosti neodpovídá v současné podobě aktuálním požadavkům a trendům. Z tohoto důvodu pak nedostatečně vzdělává a vychovává na základním a středním stupni žáky a také v nedostatečné míře nabízí vysokoškolské programy, které by vytvářely odborníky na kybernetickou bezpečnost. Poptávka po těchto odbornících je přitom vysoká.*

[157] Viz Conceptica. *AKADEMIE KYBERNETICKÉ BEZPEČNOSTI* (online) © CONCEPTICA S.R.O., dostupné z: http://www.conceptica.cz/akreditovane-kurzy/akademie-kyberneticke-bezpecnosti/

Závěr

Právní regulace kyberprostoru má v současnosti několik trhlin. Za prvé, realizace celosvětově bude nákladná a náročná, většina subjektů nesplňuje cíle standardizace ani z části, dalším nedostatkem je pak právě kritický nedostatek personálního substrátu. Problémem může být také neustálá proměnlivost tohoto úseku, nepříliš rozsáhlá zkušenost s právní regulací, i nedostatek vzorů a informací ohledně této problematiky, což pramení z roztříštěnosti, nejednotnosti v postoji a z definičních problémů v mezinárodním právu. Přes to vše je snaha pro zabezpečený virtuálního informačního prostoru ohromná. Některé skupiny však mají strach z přílišných pravomocí interesovaných orgánů, obávají se přebujelosti kontroly a zlovůle v rozhodování o tom, koho perzekuovat a *„odstřihnout“* od sítě.

Jak vyvážená by účelná a efektivní právní úprava měla být, ukáže až její delší působení v praxi a interakce s kybernetickými hrozbami a bezpečnostními incidenty v budoucnu. Nicméně je jasné, že je nutné nejen autoritativně upravovat pravidla platící pro kyberprostor, ale i zvyšovat povědomí o kybernetické hygieně i zcela běžných uživatelů, jichž se denně připojují online celé miliardy. Cílem této práce byla snaha o průřezový pohled do systematiky právní úpravy kyberprostoru a popis hlavních proudů i limitů současné úpravy. Jak z tohoto vyplynulo, právní ošetření této problematiky je stále o krok pozadu za pachateli kyberkriminality obecně, a tak se kyberkriminalita, zvláště motivována ekonomicky, politicky či mocensky, stává reálnou každodenní hrozbou, jejíž nebezpečnost stále narůstá s tím, jak se zvyšuje její objem a s tím, jak jsou ochranné prvky netečné a neschopné pružné a včasné reakce na napadení, která poškozují prostor, v němž se odehrává sociální interakce formující se informační společnosti, tedy v zásadě nás všech.

Seznam použitých zdrojů

Literatura

1. POLČÁK, R. GŘIVNA, T. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. 220 s. Auditorium. ISBN 978-80-903786-7-4.
2. KOLEKTIV AUTORŮ. *Sborník: Kybernetické útoky na Informační systémy. 2012*. ISBN 978-80-7251-371-0.
3. POLČÁK, R. *Právo a evropská informační společnost.* Brno: Masarykova Univerzita, 2009. 202 s. Acta Universitatis Brunensis Iuridica 344. ISBN 978-80-210-4885-0.
4. POLČÁK, R. *Autoritativní regulace kyberprostoru a legitimita trestního práva. In Kyberkriminalita a právo.* Praha: AUDITORIUM, 2008. s. 12-24, ISBN 978-80-903786-7-4.
5. KOLEKTIV AUTORŮ. *Sborník Kybernetická bezpečnost a obrana. 2011*.ISBN978-80-7251-363-5.
6. POLČÁK, R. ČERMÁK, J. LOEBL, Z. GŘIVNA,T. MATEJKA, J. PETR, M. *Cyber Law in the Czech Republic. Alpen aan den Rijn: Kluwer Law International,* 2012. 228 s. Encyclopaedia of Laws/Cyberlaw. ISBN 978-90-411-4010-4.
7. JIROVSKÝ, V. *Kybernetická kriminalita*, 2007. ISBN 978-80-247-1561-2.
8. POŽÁR, J. *Informační bezpečnost*. 2005, 311 stran. ISBN: 80-8689-838-5.
9. HARAŠTA, J. KENNETH, G. *Strategic Cyber Security. Revue pro právo a technologie*, Brno: Masarykova univerzita, 2014, roč. 2014, č. 9, s. 265-266. ISSN 1804-5383.
10. POLČÁK, R. *European Policies for the Information Society. In One or Many? The Law and the Structure of the European Union and the United states*. Rock Island: East Hall Press, 2011. s. 171-174, 4 s. Neuveden. ISBN 978-1-878326-20-1.
11. POLČÁK, R. *Působení práva EU ve sféře českého práva a informační společnosti. Časopis pro právní vědu a praxi.* Brno: Právnická fakulta Masarykovy univerzity, 2011, roč. 19, č. 4, s. 392-396. ISSN 1210-9126.
12. POLČÁK, R. *Vygum v kyberprostoru: Právní problémy české a evropské kybernetické bezpečnosti. In Haňka, R., Kaplan, Z., Matyáš, V. Mikulecký, J. Říha, Z. Information Security Summit 2011*. Praha: Data Security Management, 2011. s. 159-165, 7 s. ISBN 978-80-86813-22-6.
13. HARAŠTA, J. *Cyber Security in NATO & EU. In Eva Žatecká. COFOLA 2013: The Conference Proceedings. 2013*. Brno: Masarykova univerzita, 2013. s. 167-178, 12 s. ISBN 978-80-210-6625-0.
14. POLČÁK, R. *Czech Legal Reflection of the Concept of Information Society. In Czech Law in European Regulatory Context.* München: Medien und Recht, 2009. s. 143-161, 19 s. MUR. ISBN 978-3-939438-09-0.
15. POLČÁK, R. *Kyberprostor - nové výzvy právní teorii. Právny obzor,* Bratislava: Slovenská akadémia vied, 2004, Roč. 87, č. 3, s. 261-265. ISSN 0032-6984.
16. POLČÁK, R. *Law and Other Normative Systems in Cyberspace. In Cyberspace 2003: Normative Framework.* Brno: Masarykova univerzita v Brně, 2004. s. 13-18, 6 s. ISBN 80-210-3387-8.

17. POLČÁK, R. *Některé otázky práva v kyberprostoru. Časopis pro právní vědu a praxi,* Brno: Masarykova univerzita. Právnická fakulta, 2004, Roč. 12, č. 3, s. 227-231. ISSN 1210-9126.
18. WALL, D. S. *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge, 2007, Polity Press, 288s. ISBN 0-7456-2736-6.
19. JIRÁSEK, P. NOVÁK, L. POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Druhé aktualizované vydání. Policejní akademie ČR & Česká pobočka AFCEA, 2013. 200s. ISBN 978–80–7251–397–0.
20. SMEJKAL, V. a kol. *Právo informačních a telekomunikačních systémů.* Praha: C. H. Beck, 2001, 542 s. ISBN 80-7179-552-6.
21. POLČÁK, R. *Internet a proměny práva.* Praha: Auditorium, 2012. 388 s. ISBN 978-80-87284-22-3.
22. SMEJKAL, V. *Internet a §§§.* Praha: Grada Publishing, 2001. 284 s. ISBN 80-247-0058-1.
23. GIBSON, W. *Neuromancer*, (přeložil Josef Rauvolf) Laser-books, 2010, ISBN 978-80-7193-318-2.
24. POLČÁK, R. *Právo na internetu, Spam a odpovědnost ISP*. Brno: Computer Press. 2007. 150 s. ISBN 978-80-251-1777-4.
25. KSHETRI, N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives.* Greensboro, Springer-Verlag Berlin Heidelberg, 2010. 135s. ISBN 978-3-642-11521-9.
26. ŠTĚDROŇ, B. LUDVÍK, M. *Právo v informačních technologiích.* Kralice na Hané: Computer Media, 2008. ISBN 978-80-86686-36-3.
27. VANÍČEK, Z. MARCHAL, S. PROKEŠ, J.ŠTĚDROŇ, B. *Právní aspekty eGovermentu v ČR*, Praha: Linde Praha, 2011, 200s. ISBN 978-80-7201-855-0.
28. BAINBRIDGE,D. *Introduction to Computer Law,* 4. vydání, Harlow: Pearson Education Limited, 2000, 480s. ISBN0-582-42334-1.
29. SIEBER, U. LEDERMAN, E. *Conceptualizing Informational Law. In Law, Information and Information Technology.* The Hague: Kluwer Law International, 2001. 429s. ISBN 90-411-1675-3.
30. OECD. Computer Viruses and Other Malicious Software: A Threat to the Internet Economy. 2009, 244s. ISBN: 978-92-64-05650-3.
31. LIDINSKÝ, V. ŠVARCOVÁ, I. BUDIŠ, P. LOEBL, Z. PROCHÁZKOVÁ, B. *eGoverment bezpečně.* Praha: Grada Publishing, 2008.145s. ISBN978-80-247-2462-1.
32. LESSIG, L. *Code V. 2*. New York: Basic Books, 2006.
33. HOLLÄNDER, P. *Filosofie práva.* Plzeň: Aleš Čeněk, 2006.
34. WEBSTER, F. *Theories of the Information Society*. 3. vydání. New York: Routledge, rok?
35. WIENER, N. *Cybernetics: Or the Control and Communication in the Animal and the Machine*. Cambridge: MIT Press, 1961.
36. HUME, D. *A Treatise on Human Nature*. Project Gutenberg, 2003.

37. DUDLEY, A. BRAMAN, J. VINCENTI, G. *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices.* Hershey USA: IGI Global, 2012.
38. BOSWORTH, S. KABAY, M. E. *Computer Security Handbook.* 5. Vydání, část první Hoboken: John Wiley & Sons, 2009. ISBN 978-0-470-32722-7.
39. Viz. HOLT, T. J. SCHELL, B. H. Hackers and Hacking: A Reference Handbook (Contemporary World Issues) California, USA, 2013, ABC-CLIO, LLC. 354 s. ISBN-13: 978-1610692762.
40. LEVY, S. Hackers: Heroes of the Computer Revolution 1. vyd. Sebastopol, CA: O'Reilly Media. ISBN 978-1449388393.

Online zdroje

1. Evropská komise. *Nové Evropské centrum pro boj proti kyberkriminalitě bude potírat internetový zločin a chránit spotřebitele* (online) © Evropská unie, 1995–2015, dostupné z: http://ec.europa.eu/ceskarepublika/press/press_releases/12_317_cs.htm
2. KOŠATA, B. *Hacker? Kdo to je?* 1. 11. 2000, © 1998 – 2015 Root.cz (online) ISSN 1212-8309, dostupné z: http://www.root.cz/clanky/hacker-kdo-to-je/
3. ERBEN, L. *Příchod hackerů – TMRC: hackeři modelových železnic* 20. 8. 2013, © 1998 – 2015 Root.cz (online) ISSN 1212-8309, dostupné z: http://www.root.cz/clanky/prichod-hackeru-tmrc-hackeri-modelovych-zeleznic/
4. ERBEN, L. *Příchod hackerů – červ Roberta Morrise.* 18. 2. 2014, © 1998 – 2015 Root.cz (online) ISSN 1212-8309, dostupné z: http://www.root.cz/clanky/prichod-hackeru-cerv-roberta-morrise/
5. BARLOW, J. P. *Deklarace nezávislosti Kyberprostoru*. Davos, 1996. Electronic Frontier Foundation, (překlad Jakub Friedl) dostupné z: http://svetylko.blog.cz/1206/deklarace-nezavislosti-kyberprostoru
6. BOŘÁNEK, R. *Electronic Frontier Foundation: neziskovka, která jde po krku NSA.* F. 4. 7. 2014, © 1998 – 2015 Root.cz (online) ISSN 1212-8309, dostupné z: http://www.root.cz/clanky/electronic-frontier-foundation-neziskovka-ktera-jde-po-krku-nsa/
7. Česká justice, *Případů kyberútoků prý přibude, terčem budou třeba ledničky nebo toastery*, 21. 9. 2014, © 2014 Česká justice (online), dostupné z: http://www.ceska-justice.cz/2014/09/pripadu-kyberutoku-pry-pribude-tercem-budou-treba-lednicky-nebo-toastery/
8. Nadřevo.cz. *Život ve virtualitě* (online) © 2012. Nadřevo.cz, dostupné z: http://nadrevo.blogspot.cz/2010/01/zivot-ve-virtualite.html
9. JANOUŠEK, M. *Kyberterorismus: terorismus informační společnosti. In Obrana a strategie* (online). 2007. dostupné z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=6513.
10. DENNING, D. E. *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. (online), dostupné z: http://130.154.3.14/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

11. HARAŠTA, J. *Geers, Kenneth. Strategic Cyber Security*. Brno: Masarykova univerzita, 2014. In Revue pro právo a technologie, 2014, roč. 5, č. 9, ISSN 1805-2797 , dostupné z: http://revue.law.muni.cz/dokumenty/27315
12. HARAŠTA, J. *Cyber security in young democracies.* In Jurisprudence, Mykolas Romeris University, 2013, ISSN 2029–2058. s. 1457–1472. dostupné z: https://www3.mruni.eu/ojs/jurisprudence/article/view/1854/1696
13. GEERS, K. *Strategic Cyber Security*. Tallinn: CCD COE Publication, 2011, 169 s. ISBN 978-9949-9040-7-5 (pdf), dostupné z: https://ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF
14. Internet pro všechny. Za 14 evropských miliard do NGA máme mít všichni internet alespoň 30 Mb/s (online). © 2002 – 2015 Internet pro všechny, o. s ISSN 1801-1160, dostupné z: http://www.internetprovsechny.cz/za-14-evropskych-miliard-do-nga-mame-mit-vsichni-internet-alespon-30-mbs/
15. HARAŠTA, J. *Právní aspekty kybernetické bezpečnosti ČR. In Revue pro právo a technologie*, 2013, roč. 4, č. 8, s. 66-93. ISSN 1804-5383, dostupné z: http://revue.law.muni.cz/dokumenty/25809
16. KLIMEK, Libor. Combating Attacks Against Information Systems: EU Legislation and its Development. Masaryk University Journal of Law and Technology.2012, roč. 6, č. 1, s. 87-100. ISSN 1802-5943, dostupné z: https://mujlt.law.muni.cz/storage/1373984084_sb_06-klimek.pdf
17. Natoaktual.cz. NATO: *Kyber terorismus je celosvětovou hrozbou*.(online) 6. 3. 2008. © Jagello 2000, dostupné z: http://www.natoaktual.cz/nato-kyber-terorismus-je-celosvetovou-hrozbou-frv-/na_media.aspx?c=A080306_155324_na_media_m00
18. Sdělovací technika červen 2014. *Úvodník: Kyberbezpečnost v Internetu věcí* (online) © 2015 Sdělovací technika, dostupné z: http://www.stech.cz/e-casopis/nahled/2014/6.aspx
19. POLČÁK, R. *Legislativa v České republice.* (online) Pracovní příručka bezpečnostního manažera, ISBN: 978-80-7251-364-2. © 2010 - 2015,CyberSecurity.cz, dostupné z: http://www.cybersecurity.cz/law.html
20. CyberSecurity.cz. *Cyber Security (Kybernetická bezpečnost),* (online). © 2010 - 2015, CyberSecurity.cz, dostupné z: http://www.cybersecurity.cz/basic.html
21. FLÍDR, T. *Mezinárodní právo kyberprostoru a Tallinnský manuál.* (online) 22. 11. 2013. Kyberbezpečnost © Menier s.r.o. dostupné z: http://www.kyberbezpecnost.cz/?p=198
22. AC24.cz. OSN chce úplnou kontrolu nad Internetem. (online) © 2011 - 2013 AC24.cz, překlad Miroslav Pavlíček, dostupné z: http://www.ac24.cz/zpravy-ze-sveta/642-osn-chce-uplnou-kontrolu-nad-internetem
23. KUŽEL, S. Kybernetická kriminalita V: Cyberwar už není Sci-Fi. (online) ©2011-2015 BusinessIT.cz, ISSN 1805-0522, dostupné z: http://www.businessit.cz/cz/kyberneticka-kriminalita-v-cyberwar-uz-neni-sci-fi.php
24. Informační centrum OSN v Praze. *Kongres OSN o prevenci kriminality a trestním soudnictví přijal závěrečnou deklaraci.* (online) 20. 4. 2010 © 2005 UNIC Praha, dostupné z: http://www.osn.cz/zpravodajstvi/zpravy/zprava.php?id=1599

25. OECD. Computer Viruses and Other Malicious Software: A Threat to the Internet Economy. 2009, 244s. ISBN: 978-92-64-05650-3, dostupné z: http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/computer-viruses-and-other-malicious-software_9789264056510-en#page1
26. GERCKE, M. „Understanding cybercrime: A Guide for Developing Countries“, (online) 2. vydání © ITU 2011 493s., dostupné z: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf
27. Vláda ČR. Členové vlád České republiky a Státu Izrael společně jednali v Jeruzalémě (online) 25. 11. 2014, © 2009-2014 Vláda ČR, dostupné z: http://www.vlada.cz/cz/media-centrum/aktualne/clenove-vlad-ceske-republiky-a-statu-izrael-spolecne-jednali-v-jeruzaleme-124757/
28. CYBERCRIME LAW. *International and regional organizations.* (online) © Cybercrimedata AS, dostupné z: http://www.cybercrimelaw.net/International_organizations.html
29. České noviny.cz . Útvar proti kyberkriminalitě by měl fungovat od příštího roku. (online) 23. 1. 2015 © 2015 ČTK, ISSN: 1213-5003, dostupné z: http://www.ceskenoviny.cz/zpravy/utvar-proti-kyberkriminalite-by-mel-fungovat-od-pristiho-roku/1172499
30. Francie v České republice. Francouzsko-české fórum kybernetické bezpečnosti (online) 19. 1. 2015, dostupné z: http://www.france.cz/Francouzsko-ceske-forum
31. HELP NET SECURITY. *UK to host global cybersecurity centre* (online) 9. 4. 2013 © 1998-2015 HELP NET SECURITY, dostupné z: http://www.net-security.org/secworld.php?id=14724
32. Global Cyber Security Capacity Centre. *Our aim is to understand how to deliver effective cyber security both within the UK and internationally* (online) © University of Oxford, 2015, dostupné z: http://www.oxfordmartin.ox.ac.uk/cybersecurity/
33. europa.eu. Jak funguje Evropská unie (online) © Evropská unie, 1995-2015, dostupné z: http://europa.eu/about-eu/index_cs.htm
34. Ministerstvo vnitra České republiky. Obecně k agendám EU (online) © 2015 Ministerstvo vnitra České republiky, dostupné z: http://www.mvcr.cz/clanek/obecne-k-agendam-eu-461106.aspx?q=Y2hudW09Mw%3D%3D
35. European Commission. *Digitální agenda pro Evropu: klíčové iniciativy* (online) © European Union, 1995-2015, dostupné z: http://europa.eu/rapid/press-release_MEMO-10-200_cs.htm?locale=EN
36. European Commission, EU *Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive* (online) European Union, 1995-2015, dostupné z: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
37. SPĚŠNÝ, J. OBOR PROPOJÍ LEGISLATIVU A KYBERBEZPEČNOST (online) NAVUT.CZ. 20. 3. 2015 2015, ©VUT v Brně, dostupné z: http://www.vutbr.cz/zivot-na-

vut/fakta-o-vut/vut-v-mediich/vut-a-media-f19526/obor-propoji-legislativu-a-kyberbezpecnost-d100653

38. SLANINA, J. *PRÁVO BÝT ZAPOMENUT A DALŠÍ DOPADY ROZSUDKU SDEU C-131/12 GOOGLE SPAIN* (online) © epravo.cz, a.s. 1999-2015, ISSN 1213-189X, dostupné z: http://www.epravo.cz/top/clanky/pravo-byt-zapomenut-a-dalsi-dopady-rozsudku-sdeu-c-13112-google-spain-94498.html
39. CAFOURKOVÁ, T. *Cena za kybernetickou bezpečnost* (online) © © epravo.cz, a.s. 1999-2015, ISSN 1213-189X, dostupné z: http://www.epravo.cz/top/clanky/cena-za-kybernetickou-bezpecnost-92586.html
40. Evropská komise, zastoupení v české republice. *Nové Evropské centrum pro boj proti kyberkriminalitě bude potírat internetový zločin a chránit spotřebitele* (online) 28. 3. 2012. © Evropská unie, 1995–2015, dostupné z: http://ec.europa.eu/ceskarepublika/press/press_releases/12_317_cs.htm
41. European Commission. *NIS Platform - Kick-off meeting of the the Working Groups* (online) 27. 9. 2013 © European Union, 1995-2015, dostupné z: http://ec.europa.eu/digital-agenda/en/news/nis-platform-kick-meeting-working-groups
42. Ministerstvo vnitra České republiky. *Interoperability Solutions for European Public Administrations - ISA* (online) © 2015 Ministerstvo vnitra České republiky, dostupné z: http://www.mvcr.cz/clanek/interoperability-solutions-for-european-public-administrations-isa.aspx
43. VOBOŘIL, J. JAKÉ BUDOU DOPADY ZRUŠENÍ SMĚRNICE O DATA RETENTION? (online) © epravo.cz, a.s. 1999-2015, ISSN 1213-189X, dostupné z: http://www.epravo.cz/top/clanky/jake-budou-dopady-zruseni-smernice-o-data-retention-94415.html
44. *Zákon o kybernetické bezpečnosti.Vše podstatné k tomu, co přináší nový zákon platný od 1. 1. 2015* (online) © 2014 AutoCont CZ a.s., dostupné z: http://www.kybernetickyzakon.cz/
45. KROPÁČKOVÁ, A. *CERT/CSIRT týmy a jejich role* (online) Root.cz 6. 5. 2013© 1998 – 2015 Internet Info, s.r.o., dostupné z: http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/
46. CIO. *Většina úřadů v ČR nevyhoví nárokům na kyberbezpečnost* (online) 8. 10. 2014, © IDG Czech Republic, a. s., dostupné z: http://businessworld.cz/bezpecnost/vetsina-uradu-v-cr-nevyhovi-narokum-na-kyberbezpecnost-11935
47. KRÁTKÝ, P. *Zákon o kybernetické bezpečnosti v praxi* (online) © 2001 - 2015 CCB spol. s r.o. ISSN 1802-615X, dostupné z: http://www.systemonline.cz/clanky/zakon-o-kyberneticke-bezpecnosti-v-praxi.htm

Judikatura a předpisy

1. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 16. 5. 2011, dostupné z: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

2. *Všeobecné deklarace lidských práv*, 10. 12. 1948, dostupné z http://www.osn.cz/dokumenty-osn/soubory/vseobecna-deklarace-lidskych-prav.pdf
3. *Mezinárodní pakt o občanských a politických právech. New York*, 19. 12. 1966, dostupné z: http://www.osn.cz/dokumenty-osn/soubory/mezinar.pakt-obc.a.polit.prava.pdf
4. NIST SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems*(online) 1996 National Institute of Standards and Thchnology Gaithersburg, MD 20899-0001, dostupné z: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
5. NIST SP 800-12 *An Introduction to Computer Security* (online). 1995, National Institute of Standards and Technology, dostupné z: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
6. MAURER, T. Cyber norm emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-security; Discussion Paper #2011-11. (online) Cambridge © 2011 President and Fellows of Harvard College, dostupné z: http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf
7. Ženevská úmluva o zlepšení osudu raněných a nemocných příslušníků ozbrojených sil v poli

   Ženevská úmluva o zlepšení osudu raněných, nemocných a trosečníků ozbrojených sil na moři

   Ženevská úmluva o zacházení s válečnými zajatci

   Ženevská úmluva o ochraně civilních osob za války

   Dodatkový protokol k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí mezinárodních ozbrojených konfliktů (Protokol I)

   Dodatkový protokol k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí ozbrojených konfliktů nemajících mezinárodní charakter (Protokol II)

   dostupné z: http://www.cervenykriz.eu/cz/mhp_knihovna/zenevske_umluvy.pdf
8. Charta Organizace spojených národů a Statut mezinárodního soudního dvora, 24. 1945, dostupné z: http://www.osn.cz/dokumenty-osn/soubory/charta-organizace-spojenych-narodu-a-statut-mezinarodniho-soudniho-dvora.pdf
9. INTERNATIONAL TELECOMMUNICATION REGULATIONS, Dubai, 2012. dostupné z: http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf
10. CETS No.: 185 Convention on Cybercrime. Budapest, 23. 11. 2001, dostupné z: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
11. UN Security Council Resolution 1624 (2005), dostupné z: http://www.mofa.go.kr/mofat/htm/issue/policyplanning/UNSCR_1624.pdf
12. Resolution adopted by the General Assembly on 18 December 2013 [on the report of the Third Committee (A/68/456/Add.2)] 68/167. *The right to privacy in the digital age*, dostupné z: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167
13. Resolution adopted by the General Assembly [on the report of the Third Committee (A/55/593)] 55/63. *Combating the criminal misuse of information technologies*. dostupné z: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

14. NÁLEZ Ústavního soudu Pl.ÚS 24/10 ze dne 22. 3. 2011, 94/2011 Sb., N 52/60 SbNU 625 Shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu, dostupné z: http://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-24-10_1 © 2006 AutoCont CZ, a.s.
15. General Assembly resolution 65/230 Twelfth United Nations Congress on Crime Prevention and Criminal Justice, dostupné z: http://www.unodc.org/documents/justice-and-prison-reform/AGMs/General_Assembly_resolution_65-230_E.pdf
16. Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, dostupné z: http://www.unodc.org/documents/justice-and-prison reform/AGMs/General_Assembly_resolution_65-230_E.pdf
17. DEAUVILLE G8 DECLARATION; RENEWED COMMITMENT FOR FREEDOM AND DEMOCRACY. dostupné z: http://ec.europa.eu/archives/commission_2010-2014/president/news/speeches-statements/pdf/deauville-g8-declaration_en.pdf
18. International review of criminal policy - *United Nations Manual on the prevention and control of computer-related crime,* dostupné z: http://www.uncjin.org/Documents/EighthCongress.html
19. CETS No.: 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Štrasburk 28. 1. 2003, dostupné z: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm
20. SMLOUVA O EVROPSKÉ UNII (92/C 191/01), dostupné z: http://www.euroskop.cz/gallery/2/758-smlouva_o_eu_puvodni_verze.pdf © 2005-15 Vláda České republiky
21. Lisabonská smlouva pozměňující smlouvu o Evropské unii a smlouvu o založení Evropské unie CIG 14/07, dostupné z: http://www.euroskop.cz/gallery/2/738-lisabonska_smlouva.pdf © 2005-15 Vláda České republiky
22. The Internet Organised Crime Threat Assessment 29. 9. 2014, dostupné z: https://www.europol.europa.eu/iocta/2014/toc.html
23. ROZSUDEK SOUDNÍHO DVORA (velkého senátu) ze dne 13. května 2014 ve věci C-131/12, Google Spain SL,Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González, dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=484073
24. Rozsudek Soudního dvora (velkého senátu) ze dne 8. dubna 2014 (žádosti o rozhodnutí o předběžné otázce High Court of Ireland, Verfassungsgerichtshof - Irsko, Rakousko) Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl a další (C-594/12) v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General (Spojené věci C-293/12 a C-594/12), dostupné z:

http://curia.europa.eu/juris/document/document.jsf?text=&docid=153045&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=484318

25. ZÁKON ze dne 22. února 2005 č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), dostupné z: http://www.zakonyprolidi.cz/cs/2005-127#cast1 © AION CS 2010-2015
26. ÚSTAVNÍ ZÁKON ze dne 22. dubna 1998 č. 110/1998 Sb., o bezpečnosti České republiky, dostupné z: http://www.zakonyprolidi.cz/cs/1998-110 © AION CS 2010-2015
27. ZÁKON ze dne 28. června 2000 č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), dostupné z: http://www.zakonyprolidi.cz/cs/2000-240 © AION CS 2010-2015
28. VYHLÁŠKA č. 316/2014 Sb. ze dne 15. prosince 2014 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), dostupné z: http://www.epravo.cz/top/zakony/sbirka-zakonu/vyhlaska-ze-dne-15-prosince-2014-o-bezpecnostnich-opatrenich-kybernetickych-bezpecnostnich-incidentech-reaktivnich-opatrenich-a-o-stanoveni-nalezitosti-podani-v-oblasti-kyberneticke-bezpecnosti-vyhlaska-o-kyberneticke-bezpecnosti-20344.html © epravo.cz, a.s. 1999-2015, ISSN 1213-189X
29. VYHLÁŠKA 317/2014 Sb. ze dne 15. prosince 2014 o významných informačních systémech a jejich určujících kritériích, dostupné z: http://www.epravo.cz/top/zakony/sbirka-zakonu/vyhlaska-ze-dne-15-prosince-2014-o-vyznamnych-informacnich-systemech-a-jejich-urcujicich-kriteriich-20345.html © epravo.cz, a.s. 1999-2015, ISSN 1213-189X
30. ZÁKON č. 181/2014 Sb. ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), dostupné z: http://www.zakonyprolidi.cz/cs/2014-181 © AION CS 2010-2015

Ostatní

1. *Worldometers* (online), © Worldometers.info dostupné z: http://www.worldometers.info/
2. *Find a professional hacker*.(online) © 2015 Hacker's List, dostupné z: https://hackerslist.com/
3. Ministerstvo vnitra ČR. *Pojmy- Bezpečnost* © 2015 Ministerstvo vnitra České republiky, dostupné z: http://www.mvcr.cz/clanek/pojmy-bezpecnost.aspx
4. http://www.un.org/en/ecosoc/ © United Nations 2015
5. http://www.unodc.org/ ©2015 UNODC
6. http://www.unicri.it/ ©2015 UNICRI
7. http://www.unidir.org/ © UNIDIR 2015
8. http://www.un.org/en/terrorism/ctitf/ © United Nations 2015
9. http://www.itu.int/en/Pages/default.aspx © ITU 2015
10. http://www.impact-alliance.org/home/index.html © 2015 IMPACT
11. GLOBAL CYBER LAW DATABASE (online) © 2010 - 2015 ASIAN SCHOOL OF CYBER LAWS, dostupné z: http://www.cyberlawdb.com/gcld/

12. http://www.coe.int/en/web/portal/home © Council of Europe 2014
13. terena © GÉANT Association, dostupné z: https://www.terena.org/activities/tf-csirt/
14. FIRST, Improving security together © 1995 - 2015 by FIRST.org, Inc., dostupné z: http://www.first.org/
15. EGC Group © 2006-2014 EGC, dostupné z: http://www.egc-group.org/
16. AFCEA © AFCEA, dostupné z: http://afcea.cz/ceska-pobocka-afcea/
17. EUROPOL. European Cybercrime Centre (EC3) © 2015 Europol, dostupné z: https://www.europol.europa.eu/content/megamenu/european-cybercrime-centre-ec3-1837
18. ENISA ©2013 European Union Agency for Network and Information Security, dostupné z: https://www.enisa.europa.eu/about-enisa
19. ICSPA. ©2014 International Cyber Security Protection Alliance – ICSPA, dostupné z: https://www.icspa.org/about-us/
20. CERT, SEI. ©2015 Carnegie Mellon University, dostupné z: https://www.cert.org/about/
21. NIST. © National Institute of Standards and Technology (NIST), dostupné z: http://www.nist.gov/
22. NCKB © Národní bezpečnostní úřad, dostupné z: http://www.govcert.cz/cs/
23. CZ. NIC, Správce domény CZ © 2015 CZ. NIC, z. s. p. o., dostupné z: https://www.nic.cz/
24. Statistické přehledy kriminality za rok 2014 © 2015 Policie ČR, dostupné z: http://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2014.aspx
25. ČIMIB. © 2013 ČIMIB, dostupné z: http://www.cimib.cz/stranka/24-o-nas
26. Conceptica. AKADEMIE KYBERNETICKÉ BEZPEČNOSTI (online) © CONCEPTICA S.R.O., dostupné z: http://www.conceptica.cz/akreditovane-kurzy/akademie-kyberneticke-bezpecnosti/