BACKGROUND REPORT

PRAGUE**PRAŽSKÝ**
STUDENT**STUDENTSKÝ**
SUMMIT

DISEC

Rozvoj informačních a komunikačních technologií

Autor: Šárka Tesařová
Imprimatur: Martin Mezenský, Filip Jelínek
Jazyková úprava: Jakub Kopřiva, Judita Zelbová
Grafická úprava: Jan Hlaváček

Model OSN

Vydala Asociace pro mezinárodní otázky (AMO) pro potřeby XXI. ročníku Pražského studentského summitu.

Asociace pro mezinárodní otázky (AMO)
Žitná 27, 110 00 Praha 1
Tel.: +420 224 813 460, e-mail: summit@amo.cz
IČ: 65 99 95 33

www.amo.cz

www.studentsummit.cz

1 Úvod

Informační a komunikační technologie (dále „ICT") v čele s internetem patří bezpochyby k přelomovým vynálezům 20. století. Ve svém prvopočátku byly počítačové technologie dostupné pouze několika málo vědecko-výzkumným ústavům, vojákům či nejbohatším korporacím, ovšem díky jejich miniaturizaci a zlevnění se postupně staly nepostradatelnou součástí našeho života. V souvislosti s expanzí a stále intenzivnějším využíváním ICT se proměnil i charakter lidské společnosti, a tak je možné 21. století charakterizovat jako století informační, kdy ICT spolu s kybernetickým prostorem a množstvím dostupných informací ovlivňují celou společnost. Avšak další pokrok v oblasti ICT s sebou přináší jak nové neuvěřitelné možnosti, tak i nové problémy. ICT mají civilní i vojenské využití při udržování mezinárodní stability a bezpečnosti, jsou zárukou inovací a jsou důležité pro rozvoj národních ekonomik. Na druhou stranu existuje několik způsobů, jak se ICT mohou stát bezpečnostní hrozbou, kupříkladu mohou být využity ke zničení informačních zdrojů, mohou být užívané zločineckými skupinami ke komunikaci nebo mohou být prostředkem k narušení hospodářských institucí.

2 Informační a komunikační technologie

Informační a komunikační technologie (anglicky *Information and Communication Technologies*) představují nejdynamičtěji se rozvíjející odvětví lidské tvorby a jsou zastřešujícím pojmem zahrnujícím technologie používané pro komunikaci a práci s informacemi v praktickém smyslu.[1]

ICT se dají rozdělit do čtyř oblastí:

a) hardware = technické zázemí IT (počítače, servery);
b) software = programové vybavení IT (operační systémy, síťové protokoly, internetové vyhledávače);
c) netware = počítačové sítě;
d) telekomunikace = sdělovací technika (rozhlas, televize, telegraf).

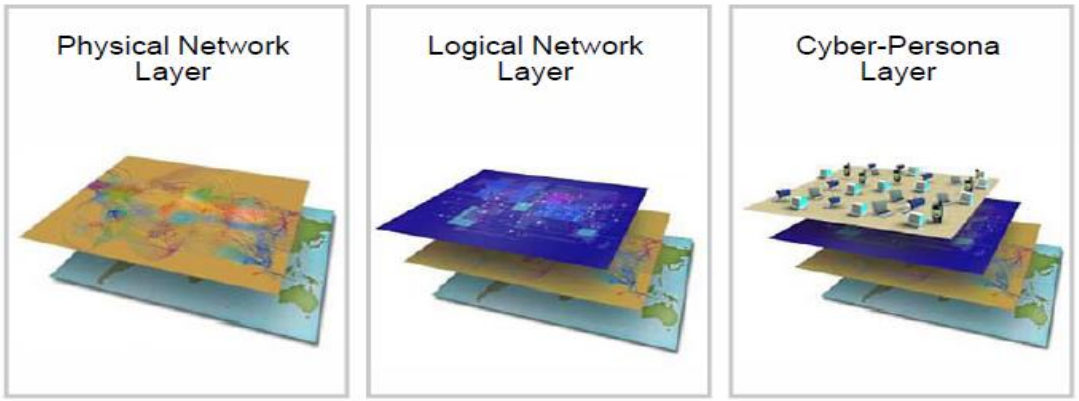
[1] Information and Communications Technology (ICT). *Technopedia* [online]. [cit. 2015-09-19]. Dostupné z: http://www.techopedia.com/definition/24152/information-and-communications-technology-ict

3 Kybernetický prostor

Vzhledem k předmětu této práce je nejprve nutné vymezit klíčový pojem kybernetický prostor[2] (anglicky *cyberspace*). Na základě různých definic existuje celá řada možných výkladů, ale vědci se dosud neshodli na žádné univerzálně platné definici – tzn. takové, která by zahrnovala vše podstatné a kterou by bylo možné jednotně používat. Jediné, v čem se většina definic shoduje[3], je chápání kybernetického prostoru jako metaforického vyjádření jakéhosi nefyzického místa, kde se nacházíme během komunikace zprostředkované počítačem či telefonem.[4] Pro účely této práce budeme tedy kybernetickým prostorem rozumět „*virtuální svět vytvořený moderními technologickými prostředky*"[5], jehož smyslem je „*vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, používat či vymazávat informace*".[6]

Jeho vlastnosti jsou: množství informací, všudypřítomnost, neohraničitelnost, decentralita, interaktivní prostřední, rychlost, otevřenost širokému okruhu uživatelů a anonymita. Je možné ho popsat ve třech provázaných vrstvách (fyzická, logická/informační a kognitivní/sociální) a pěti složkách (geografické sítě, fyzické sítě, logické sítě, lidé na síti a lidé).[7]

Obrázek 1: Vrstvy a složky kybernetického prostoru[8]



[2] Tento pojem poprvé použil v roce 1982 americko-kanadský spisovatel William Gibson (zakladatel kyberpunku) ve své povídce „Burning Chrome" a o 2 roky později ve svém sci-fi románu „Neuromancer".
[3] Viz definice českého slovníku kybernetické bezpečnosti, Joint Terminology for Cyberspace Operations, Barlowova.
[4] HRŮZA, P; PITAŠ J; BRECHTA, B. aj. *Kybernetická bezpečnost II*. Brno: Univerzita obrany, 2013. 1. vydání. 100 s. ISBN 978-80-7231-931-2. s. 10.
[5] Tamtéž.
[6] MAYER, M; MARTINO, L; MAZURIER, P. How would you define Cyberspace? *Academia.edu* [online]. 2014.[cit. 2015-09-19]. Dostupné z: https://www.academia.edu/7096442/How_would_you_define_Cyberspace
[7] *Cyberspace Operations* [online]. 2013. 70 pp. [cit. 2015-09-19]. Dostupné z: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf
[8] Tamtéž.

Přestože kybernetický prostor je imaginárním prostorem, je řízen svými uživateli a závisí na reálném světě – kybernetické infrastruktuře. Ta se skládá z jednotlivých počítačů, počítačových sítí používajících TCP/IP protokol[9], vzájemně propojených databází, síťových serverů, telefonů, telekomunikačních sítí, směrovačů a přepínačů aj.

Kybernetický prostor představuje prozatím nepříliš probádanou sféru, kde je vysoká pravděpodobnost vzniku kybernetických hrozeb a rizik.

4 Kybernetické útoky

Kybernetický útok (anglicky *cyber attack*) představuje záměrné aktivní provedení kybernetické hrozby. Je to prostředek k dosažení určitého cíle, kdy dochází k pokusu o narušení kybernetické bezpečnosti různých subjektů.[10] Naopak kybernetické incidenty nechtěně zapříčiněné, jako například nehoda či nedbalost, za ně považovány nejsou. Velké kybernetické útoky jsou většinou mezinárodního charakteru, na druhou stranu ztráty dat u soukromých společností jsou ponejvíce způsobovány samotnými zaměstnanci, kteří mají k datům přístup. Téměř anonymní prostředí kybernetického prostoru totiž nahrává přeshraničním zločinům, kde se střetávají jurisdikce rozdílných států a hrozba dopadení původce útoku se úměrně snižuje. Nicméně při dostatečné ochotě spolupracovat stále lze původce vypátrat.

Hacking coby soubor využitelných metod sloužících k proniknutí do počítačového systému jiným než standardním způsobem (tedy zpravidla obejitím či prolomením jeho bezpečnostního systému) v sobě zahrnuje metody a nástroje jako: malware,[11] některé metody sociálního inženýrství,[12] pharming,[13] sniffing,[14] defacement,[15] cybersquatting,[16] DoS,[17] spamming,[18] aj. Jelikož nástrojů kybernetického útoku existuje přemnoho, útočníci mají možnost volby podle

[9] Primární přenosový protokol obsahující řadu protokolů pro komunikaci v počítačové síti a je hlavním protokolem internetu.
[10] JIRÁSEK, P.; NOVÁK, L; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie a AFCEA, 2013. 2. aktualizované vydání. 200 s. ISBN 978-80-7251-397-0. s. 105.
[11] Počítačový program určený k neoprávněnému vniknutí nebo poškození počítačového systému, zahrnuje počítačové viry a červy, trojské koně, adware, spyware.
[12] Probíhá na základě komunikace s osobou, kterou se snaží přesvědčit, aby svým chováním poškodila ochranu systému.
[13] Podvodná technika používaná na internetu k získávání citlivých údajů od obětí útoku.
[14] Technika k odposlouchávání datových paketů.
[15] Změna či přesměrování primární internetové stránky, což vede k dezorientaci uživatelů.
[16] Označení pro registraci a následné užívání doménového jména ve zlé víře na úkor obchodní značky, názvu anebo jména jiné osoby.
[17] Forma útoku, kdy je server zahlcen falešnými požadavky na poskytnutí konkrétní služby a tím znemožňuje jeho běžný chod.
[18] Jedna z nejméně nebezpečných metod, jež spočívá v rozesílání reklamních a jiných nevyžádaných zpráv.

toho, která bude k naplnění jejich cíle nejvhodnější – krádež nebo znehodnocení informací, destabilizace systému, nedostupnost služby, blokování systémových prostředků, aj.

Počet kybernetických útoků každoročně roste, protože se ukazují jako nejjednodušší a nejrychlejší alternativa k tradičním „fyzickým" vojenským útokům nebo v kombinaci s fyzickými útoky dojde ke zvětšení jejich dopadů. Kromě toho jejich použití usnadňuje absence obecně přijímaných mezinárodních pravidel a na škále donucovacích prostředků spadají mezi diplomatický tlak a použití síly.[19]

Motivy útočníků – nestátních aktérů – jsou pak většinou internetový exhibicionismus, pomsta, finanční zisk, propaganda vlastní ideologie a publicita.[20] Na základě analýzy je možné konstatovat, že pro zločince jsou kybernetické útoky výhodné kvůli rozmanitosti cílů, snadného dosažení požadovaných výsledků, rychlosti, neomezeného dosahu, provádění na dálku, možnosti utajení, anonymity a nižších nákladů na provedení. Možnými důsledky jsou oslabení protivníka skrze jeho vlastní velitelské a řídicí systémy, vynucení si politické změny, sabotáže, ekonomické škody, poškození prestiže, vyvolání strachu a paniky.[21] Je možné, že se kybernetické útoky budou postupně stávat nástrojem k prosazení vojensko-politických záměrů.[22]

Přestože kybernetické útoky jsou hojně diskutované, jejich přesná klasifikace je velmi obtížná. Ať už z důvodu, že kybernetický terorismus je považován de facto za neexistující – jednotlivé kybernetické útoky ještě nedosáhly takové intenzity –, nebo proto, že kybernetické útoky v sobě zahrnují více znaků.[23] Zařazení níže uvedených názorných příkladů je proto pouze orientační.

4.1 Kybernetická kriminalita

Kybernetická kriminalita (anglicky *cybercrime*) je dle Výkladového slovníku kybernetické bezpečnosti: „*trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší*

[19] Připravte se, bude válka. *E15* [online]. 2013. [cit. 2015-09-19]. Dostupné z: http://euro.e15.cz/archiv/pripravte-se-bude-valka-959907

[20] JANOUŠEK, M. Kyberterorismus: terorismus informační společnosti. *Obrana a strategie* [online]. 2006, (2) [cit. 2015-09-19]. DOI: 10.3849/1802-7199. ISSN 1802-7199. Dostupné z: http://www.obranaastrategie.cz/cs/archiv/rocnik-2006/2-2006/kyberterorismus-terorismus-informacni-spolecnosti.html#.VYV-VI0w-po

[21] DRMOLA, J. Konceptualizace kyberterorismu, *Vojenské rozhledy*, 2013, 22 (54), ISSN 1210-3292. Dostupné z: http://www.vojenskerozhledy.cz/kategorie/konceptualizace-kyberterorismu

[22] MINISTERSTVO OBRANY ČESKÉ REPUBLIKY. Výroční zpráva o činnosti Vojenského zpravodajství za rok 2013 [online]. 2013. 28 s. [cit. 2015-09-19]. Dostupné z: http://admin.vzcr.cz/shared/clanky/20/V%C3%BDro%C4%8Dn%C3%AD%20zpr%C3%A1va%202013.pdf

[23] Tamtéž.

množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti".[24]

Je důležité zdůraznit, že počítače obecně neumožňují páchat nový typ trestné činnosti, jen poskytují novou technologii a nové způsoby pro páchání už známých trestných činů, jako jsou finanční podvody a zpronevěry, padělání, krádeže identity, sabotáže, obecné ohrožení, vyzvědačství, vyhrožování, vydírání, pomluvy, pirátství a distribuce dětské pornografie.[25] Existují ovšem i zcela nové „počítačové" trestné činy jako neoprávněný přístup, narušování systémů, přechovávání přístupového zařízení a hesla, poškození dat a zásah do vybavení počítače z nedbalosti.[26]

Příkladem může být virus Stuxnet, což byl americkou vládou sponzorovaný projekt, který vyřadil z provozu část íránského jaderného programu.[27]

4.2 Kybernetická špionáž

Kybernetická špionáž (anglicky *cyber espionage*) je akt zisku tajných či strategicky významných informací bez svolení vlastníka za použití nezákonných metod prostřednictvím počítačových sítí.[28]

Do této kategorie je možné přiřadit ruské a čínské útoky na systémy Spojených států amerických (proniknutí do Pentagonu, ministerstva energetiky, NASA či společnosti Lockheed Martin) či Trojangate, jakožto největší zveřejněný případ kybernetické špionáže, k němuž došlo v Izraeli v roce 2005. Jako příklad korporátní kybernetické špionáže lze uvést operaci Aurora z roku 2009, která napadla sítě velkých společností jako Google, Adobe, Yahoo či Juniper Networks.[29]

---

[24] JIRÁSEK, P.; NOVÁK, L; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie a AFCEA, 2013. 2. aktualizované vydání. 200 s. ISBN 978-80-7251-397-0. s. 57.
[25] GERCKE, M. *Understanding cybercrime: phenomena, challeges and legal response* [online]. Geneva: International Telecommunication Union, 2012.[cit. 2015-09-19]. Dostupné z: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf
[26] Tamtéž.
[27] *25 Biggest Cyber Attacks In History* [online]. 2013.[cit. 2015-09-19]. Dostupné z: http://list25.com/25-biggest-cyber-attacks-in-history/5/
[28] JIRÁSEK, P.; NOVÁK, L; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie a AFCEA, 2013. 2. aktualizované vydání. 200 s. ISBN 978-80-7251-397-0. s. 58.
[29] *25 Biggest Cyber Attacks In History* [online]. 2013.[cit. 2015-09-19]. Dostupné z: http://list25.com/25-biggest-cyber-attacks-in-history/5/

4.3 Kybernetický terorismus

Kybernetický terorismus (anglicky *cyberterrorism*) představuje jednu z největších kybernetických hrozeb, jimž dnešní informační společnost čelí.

Terorismus můžeme rozdělit podle formy na letální[30] a neletální, přičemž první skupina se vyznačuje použitím běžných prostředků pro realizaci násilí (konvenční – útoky páchané pomocí běžně dostupných bojových prostředků, nekonvenční – zneužití zbraní hromadného ničení). Kybernetický terorismus je možné vnímat jako podmnožinu nekonvenční formy neletálního terorismu. Nejrozšířenější definice pochází od Dorothy E. Denningové: „*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*".[31] Cíle kybernetického terorismu se sice nacházejí ve světě virtuálním, ale většinou mají mít dopad na reálný svět. Aby se skutečně mohlo mluvit o kybernetickém terorismu, mělo by se jednat o útok vedoucí ke ztrátám na životech a měl by být veden na službu klíčovou pro fungování společnosti.

4.4 Kybernetická válka

Opravdová kybernetická válka (anglicky *cyber war*) sice zatím nevypukla, ale tento způsob vedení boje představuje jednu z možností, jak se postavit nepříteli, který má drtivou převahu vojenské i ekonomické síly.

V kybernetické válce dochází ke stavu „*rozsáhlých, často politicky či strategicky motivovaných, souvisejících a vzájemně vyvolaných organizovaných kybernetických útoků a protiútoků*".[32]

5 Kybernetická bezpečnost

Kybernetická bezpečnost (anglicky *cyber security*), někdy také známá jako informační bezpečnost, je „*souhrn právních, organizačních, technických a vzdělávacích prostředků*"[33] sloužících k posilování „*důvěry, integrity a dostupnosti*"[34] informací.

---

[30] Znamená smrtící.

[31] DENNING, D. E. Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing Foreign Policy. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND Corporation, 2001, s. 239-288, 380 s. ISBN 0-8330-3030-2.

[32] JIRÁSEK, P.; NOVÁK, L; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie a AFCEA, 2012. 1. vydání. 93 s. ISBN 978-80-7251-378-9. s. 69.

[33] JIRÁSEK, P.; NOVÁK, L; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie a AFCEA, 2013. 2. aktualizované vydání. 200 s. ISBN 978-80-7251-397-0. s. 57.

[34] JIRÁSEK, P.; NOVÁK, L; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie a AFCEA, 2013. 2. aktualizované vydání. 200 s. ISBN 978-80-7251-397-0. s. 18.

Toto odvětví se zabývá ochranou a zabezpečením dat v počítačových sítích, které se snaží identifikovat a hodnotit, řešit kybernetické hrozby a minimalizovat rizika spojená s užíváním počítače.[35] Její funkcí je monitoring kybernetických hrozeb a účinnosti protiopatření. Třebaže se původně se měla soustředit pouze primárně na prevenci, tak je dnes její zásadní součástí posilování tzv. resilience[36]. Počítačová bezpečnost dále zahrnuje: „*zabezpečení ochrany před neoprávněným manipulováním se zařízeními počítačového systému, ochranu před neoprávněnou manipulací s daty, ochranu informací před krádeží nebo poškozením, bezpečnou komunikaci a přenos dat (kryptografie), bezpečné uložení dat, dostupnost, celistvost a nepodvrhnutelnost dat*".[37] Přičemž informace musejí zůstat přístupné jeho předpokládaným uživatelům.

Z právního hlediska jsou klíčové přijaté zákony[38] upravující použití technických prostředků a určující standardní postupy řešení kybernetických útoků. Z technického hlediska je důležité zabezpečení kybernetické infrastruktury zakládat na flexibilním více úrovňovém systému, aby při vyřazení jednoho segmentu nedošlo ke kritickému selhání celku a aby poškozený segment dokázal do doby obnovy nahradit segment jiný (posilování tzv. resilience[39]).

Základní myšlenkou je, že by stát měl být schopen ochránit své vlastní zájmy před kybernetickými útoky. „*Kybernetickou bezpečnost pak vlády vyspělých států vnímají jako národní politickou záležitost, protože nezákonné použití kyberprostoru může bránit rozvoji hospodářské, ekonomické a národní bezpečnostní činnosti.*"[40]

Po dlouhou dobu byla největším úskalím kybernetické bezpečnosti skutečnost, že většinou z finančních důvodů byla bezpečnost ICT pro vývojáře až vedlejší.[41] Potíž byla a stále je zejména v koncových uživatelích, kteří na ochranu dbají méně (neaktualizované systémy, zastaralé bezpečnostní záplaty), zatímco zločinci se stávají čím dál více vynalézavými. Nicméně dnes se jí věnuje stále více pozornosti. I přes to, že většina západních států v posledních letech významně pokročila, dokonalé stoprocentní kybernetické bezpečnosti nebude možné dosáhnout. Poněvadž kybernetická bezpečnost je procesem permanentním, který probíhá

[35] JIRÁSEK, P.; NOVÁK, L; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie a AFCEA, 2013. 2. aktualizované vydání. 200 s. ISBN 978-80-7251-397-0. s. 72.
[36] Schopnost systému přestát disturbance a v průběhu proměn se přeskupovat tak, že původní funkce, struktura, identita a zpětné vazby zůstávají zachovány. Co nejrychleji po útoku by mělo dojít k obnovení standartního chodu.
[37] Tamtéž.
[38] Např. evropská„ Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace", americký „Cyber Security Framework" a „Cyberspace Policy Review", ruská kybernetická strategie, český zákon č. 181/2014 Sb., o kybernetické bezpečnosti.
[39] Schopnost systému přestát disturbance a v průběhu proměn se přeskupovat tak, že původní funkce, struktura, identita a zpětné vazby zůstávají zachovány. Co nejrychleji po útoku by mělo dojít k obnovení standartního chodu.
[40] HRŮZA, P; PITAŠ J; BRECHTA, B. aj. *Kybernetická bezpečnost II*. Brno: Univerzita obrany, 2013. 1. vydání. 100 s. ISBN 978-80-7231-931-2. s. 15.
[41] Připravte se, bude válka. *E15* [online]. 2013. [cit. 2015-09-19]. Dostupné z: http://euro.e15.cz/archiv/pripravte-se-bude-valka-959907

kontinuálně formou zdokonalování bezpečnosti, je cílem zajištění optimální úrovně kybernetické bezpečnosti, z čehož též plyne zajištění adaptace národních bezpečnostních systémů na nově vzniklé hrozby.

Kybernetické útoky budou tedy stále probíhat, otázkou avšak je, jaké procento bude úspěšné. *„Důvodů, proč k závažným útokům zatím nedochází, je hned několik:*

- *ty nejcitlivější systémy nejsou vůbec k internetu připojeny a jsou zabezpečeny pomocí tzv. air-gap*[42] *a útok by tak obvykle vyžadoval fyzickou přítomnost;*
- *sofistikované útoky na průmyslová nebo vojenská zařízení vyžadují detailní přehled o cílovém systému, dlouhou a náročnou přípravu a velmi pokročilé znalosti z oboru;*
- *elektronické útoky pro „tradiční teroristy" postrádají silný dramatický a symbolický efekt, kterého mohou dosáhnout pomocí výbušnin a excesivního násilí;*
- *elektronické útoky vyžadují informační infrastrukturu, kterou rozvojové země (obzvláště mimo města) často postrádají;*
- *„subkultura hackerů" obvykle nemá zájem, odhodlání a potřebný ideologický zápal se do těchto rozsáhlých útoků pouštět.*"[43]

Kybernetická bezpečnost se nevztahuje pouze na veřejný sektor, ale také na ten soukromý, který je vlastníkem značné části ICT infrastruktury. Z tohoto důvodu je vhodné soukromý sektor do státem plánované kybernetické bezpečnosti zapojit, neboť stát nemusí kvůli svým byrokratickým postupům být schopen rychle reagovat, zatímco soukromý sektor v duchu zásady „co není zakázáno, je dovoleno" má volnější ruce.

6 Mezinárodně-bezpečnostní a právní aspekty

6.1 Mezinárodně-bezpečnostní aspekty

Výše uvedené vlastnosti kybernetického prostoru jsou příčinou toho, proč se tento pojem jeví chaotickým a obtížně uchopitelným. Kromě toho se zde setkáváme s několika zásadními problémy, a to s otázkou vytvoření jednotné definice, rozměru (konečný x nekonečný), hranic (státy x organizace), pravomocí (kdo může internet vypnout anebo odposlouchávat) a odpovědnosti.[44] Asi nejzávažnějším problémem je skutečnost, že kybernetický prostor nemá začátek ani konec, nezná ani geografické hranice, a tak akce provedená ve státě A může mít

[42] Znamená oddělovač, nemusí byt fyzické – musí ale mít nějaké kryptografické šifrovací zařízení. Nejedná se však o nepřekonatelný problém.
[43] DRMOLA, J. Konceptualizace kyberterorismu, *Vojenské rozhledy*, 2013, 22 (54), ISSN 1210-3292. Dostupné z: http://www.vojenskerozhledy.cz/kategorie/konceptualizace-kyberterorismu
[44] HRŮZA, P; PITAŠ J; BRECHTA, B. aj. *Kybernetická bezpečnost II*. Brno: Univerzita obrany, 2013. 1. vydání. 100 s. ISBN 978-80-7231-931-2. s. 10-15.

téměř okamžitý účinek ve státě B. Falešný pocit anonymity navíc umožňuje, že za monitor se mohou schovat hackeři, aktivistické skupiny a teroristé. A tito pachatelé jsou v kybernetickém prostoru jen velmi obtížně vypátratelní.[45]

Celkový rozmach internetu a nové ICT způsobují, že se stále více jevů přesunuje z reálného světa do uměle vytvořené sféry kybernetického prostoru. Na toto reagují i některé státy tím, že začínají kybernetický prostor chápat jako strategické bojiště budoucnosti, a proto činí z kybernetického prostoru svou novou válečnou doménu[46] vedle země, moře, vzduchu a vesmíru. Nejvíce se využití kybernetického prostoru jak pro potenciální útok nebo pro obranu věnují velmoci jako Spojené státy americké, Rusko a Čína.[47] Dále lze uvést státy jako Velká Británie, Írán či Severní Korea.

Co se týče vlivu kybernetických útoků na demokratizaci a liberalizaci uzavřených politických systémů, tak analytik Asociace pro mezinárodní otázky (AMO) Tomáš Rezek se nedomnívá, že by byly nějakým způsobem nápomocné. Spíše „*můžeme očekávat, že dosud demokratické země budou cílem častějších propagandistických útoků právě za účelem zneužití demokratického systému k tomu, aby se něco stalo, nebo naopak něco nestalo*"[48]. Tedy ve výsledku demokratické státy mohou být právě díky své svobodě více ohroženy těmito útoky než státy autoritativní, protože v okamžiku, kdy lidé mají příležitost se svobodně vyjadřovat, může snáze dojít k aktivizaci společnosti a následným změnám.[49]

6.2 Právní aspekty

Během počátečních fází evoluce internetu se mnoho uživatelů domnívalo, že by internet neměl být svázán předpisy žádné národní vlády (respektive tam nebudou kvůli rozdílnosti online a offline světa fungovat) a že si kyberprostorová komunita bude sama vytvářet svá vlastní pravidla.[50] Tato utopická představa je již překonána a internet je pojímán jako prostředí, které musí být jistým způsobem regulováno a nemůže být bez pravidel, jinak hrozí jeho zneužití.

Uplatňování práva je v kybernetickém prostoru kvůli jeho povaze celkem problematické. V kybernetickém prostoru platí jeho vlastní specifické normativní systémy a vynucovací

[45] Mezinárodní pravomoc. *Základy IT gramotnosti* [online]. [cit. 2015-09-19]. Dostupné z: http://is.muni.cz/do/1492/el/sitmu/law/html/mezinarodni-pravomoc.html
[46] BASTL, M; GRUBEROVÁ, Z. Kyberprostor jako „pátá doména"?. *Vojenské rozhledy* [online]. 2013, 22 (54), ISSN 1210-3292. Dostupné z:http://www.vojenskerozhledy.cz/kategorie/kyberprostor-jako-pata-domena
[47] DRMOLA, J. Konceptualizace kyberterorismu, *Vojenské rozhledy*, 2013, 22 (54), ISSN 1210-3292. Dostupné z: http://www.vojenskerozhledy.cz/kategorie/konceptualizace-kyberterorismu
[48] GRILLINGEROVÁ, I. Odborník na kyberprostor: ČR nemá ambice regulovat internet [online]. *E-polis.cz*, 2015. [cit. 2015-09-19]. Dostupné z: http://www.e-polis.cz/clanek/odbornik-na-kyberprostor-cr-nema-ambice-regulovat-internet.html
[49] Tamtéž.
[50] Cyberspace. *Encyclopedia Britannica* [online]. [cit. 2015-09-19]. Dostupné z: http://www.britannica.com/topic/cyberspace

mechanismy – netiketa[51] nebo řešení sporů online.[52] Za základní zásadu je možné považovat tzv. síťovou neutralitu, stanovující, že „*se všemi daty bude zacházeno stejně, bez ohledu na jejich původ nebo místo určení*"[53]. Kromě toho se na kybernetický prostor taktéž vztahuje i mezinárodní právo veřejné pokoušející se řešit otázky užití síly, sebeobrany, práva ozbrojeného konfliktu, suverenity a státní zodpovědnosti. Částečně se na tyto otázky snažil odpovědět právní poradce Ministerstva zahraničí Spojených států amerických Harold Hongju Koh:[54]

1. Kybernetické aktivity mohou za určitých okolností vyústit v použití síly ve smyslu čl. 2 odst. 4 Charty OSN[55].
2. Stát má dle čl. 51 Charty OSN právo reagovat na kybernetický útok tím, že uplatní právo na sebeobranu.
3. Právo ozbrojeného konfliktu se vztahuje i na regulaci kybernetických nástrojů v bojových akcích, v kontextu ozbrojeného konfliktu musejí kybernetické útoky rozlišovat mezi vojenskými a civilními cíli a musí být dodržován princip proporcionality.
4. Státy provádějící činnosti v kybernetickém prostoru musejí brát v potaz suverenitu jiných států.
5. Státy jsou právně zodpovědné za kybernetické jednání uskutečněné skrze prostředníky, tj. soukromé subjekty, kteří tak činí na základě instrukcí daného státu.

Třebaže kybernetický prostor není úplně novým fenoménem, není jasné, podle jakých pravidel by případná kybernetická válka měla být vedena. Ženevské konvence[56] stanovující právní normy pro vedení války totiž s ohledem na vedení kybernetické války zatím nebyly novelizovány – Tallinský manuál NATO[57] se sice pokoušel Ženevské konvence na kybernetický prostor aplikovat, ale jako doporučení nemá právní hodnotu.[58] Dle AMO analytika Tomáše

[51] Sada doporučení pro slušné chování v síti.
[52] Právo a kyberprostor. *Základy IT gramotnosti* [online]. [cit. 2015-09-19]. Dostupné z: http://is.muni.cz/do/1492/el/sitmu/law/html/pravo-a-kyberprostor.html
[53] Tamtéž.
[54] SCHMITT, M. N. International Law in Cyberspace: The Koh Speech and Talinn Manual Juxtaposed. *Harvard Law Journal* [online]. 2012, (54). 25 pp. [cit. 2015-09-19]. Dostupné z: http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf
[55] „*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.*"
[56] Čtyři úmluvy + tři dodatkové protokoly, které představují základní prameny válečného práva, které musí být za všech okolností a všemi stranami konfliktu dodržovány. Hlavní zásadou je, že v případě války musí být respektována důstojnost lidské bytosti a před válkou a jejími následky musí být chráněni ti, kdo se konfliktu přímo neúčastní (civilisté) nebo jsou z bojů vyřazeni (váleční zajatci, ranění a nemocní vojáci). Viz více http://www.cervenykriz.eu/cz/mhp/konvence.htm
[57] Viz více http://issuu.com/nato_ccd_coe/docs/tallinnmanual
[58] GRILLINGEROVÁ, I. Odborník na kyberprostor: ČR nemá ambice regulovat internet [online]. *E-polis.cz*, 2015. [cit. 2015-09-19]. Dostupné z: http://www.e-polis.cz/clanek/odbornik-na-kyberprostor-cr-nema-ambice-regulovat-internet.html

Rezka dokument popisuje ideální stav, ale obecně vzato „*není mezinárodní vůle, aby zahájila nějakou formalizaci do nějakého pravidla*".[59]

I když nikdo nekontroluje všechny sítě kybernetického prostoru, tak to neznamená, že by státní moc nebylo možné v kybernetickém prostoru vykonávat, poněvadž kybernetický prostor funguje díky kybernetické infrastruktuře, a ta se v jurisdikci států nachází. Právo v kybernetickém prostoru je vynutitelné díky poskytovatelům služeb informační společnosti, kteří podléhají výkonu práva státní moci a jsou odpovědní za poskytované informace.[60]

S akty uskutečněnými v kybernetickém prostoru souvisí rovněž nevyřešené otázky právě ohledně jurisdikce, odlišných národních právních řádů a distančního deliktu. Distančním deliktem je chápána situace, kdy se pachatel fyzicky nachází ve státě A a spáchá tam nějaký čin, byť je legální, ten samý čin ale může být trestným ve státě B, kde se projevují jeho účinky, jenže tam se pachatel nenachází.[61] Obecně platí, že příslušným soudem je soud ve státě žalovaného, což by v tomto případě znamenalo, že orgán veřejné moci státu B by musel požádat o součinnost orgán veřejné moci státu A – jednak je to zdlouhavé, jednak ve státě A spáchaný čin není ani trestným. A proto jediným řešením distančních deliktů je uzavírání mezinárodních smluv zavazujících signatářské státy do jisté míry právní řády sjednotit.

7 Přístupy ke kybernetické obraně

7.1 Mezinárodní organizace

7.1.1 Organizace spojených národů

Problematika informačních a komunikačních technologií v kontextu mezinárodní bezpečnosti je na programu OSN od roku 1998, kdy na toto téma Rusko předneslo první návrh usnesení ve Výboru pro odzbrojení a mezinárodní bezpečnost, které bylo Valným shromážděním OSN přijato bez hlasování jako rezoluce č. 53/70.[62] Od té doby se Valné shromáždění OSN aktivně podílí na sledování vývoje v oblasti ICT a jejich dopadu na mezinárodní bezpečnost. Současná rezoluce č. 69/28 vyjadřuje znepokojení ohledně možného zneužití ICT a jeho negativního vlivu

[59] Tamtéž.
[60] Právo a kyberprostor. *Základy IT gramotnosti* [online]. [cit. 2015-09-19]. Dostupné z: http://is.muni.cz/do/1492/el/sitmu/law/html/pravo-a-kyberprostor.html
[61] KUŽEL, S. Kybernetická kriminalita I: Co se děje v kyberprostoru. *Business IT* [online]. 2012. [cit. 2015-09-19]. Dostupné z: http://www.businessit.cz/cz/kyberneticka-kriminalita-i-co-se-deje-v-kyberprostoru.php
[62] Rezoluce Valného shromáždění OSN A/RES/53/70: *Developments in the field of information and telecommunications in the context of international security*. (1999) Dostupné z: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70

na bezpečnost členských států, z tohoto důvodu dále členské státy vyzývá ke zvážení opatření směřujících k omezení potenciálních kybernetických hrozeb.[63]

První výbor Valného shromáždění OSN pro odzbrojení a mezinárodní bezpečnost neměl zpočátku příliš velkou důvěru při jednání o tomto tématu, ale postupem času členské státy uznaly jeho neocenitelnou roli.[64] Nyní se členské státy k tomuto tématu vyjadřují každoročně a mají rovněž za úkol informovat generálního tajemníka o dosaženém pokroku při posilování informační bezpečnosti. Do debaty se doposud zapojilo více než 50 států, klíčovými hráči a vzájemnou opozicí se staly Spojené státy americké a Rusko, společně s koalicemi podobně smýšlejících partnerů. Základní rozepře mezi Spojenými státy americkými a Ruskem spočívala v odlišných přístupech k informační bezpečnosti a definicím – ruská definice podporovala stabilitu a eliminaci hrozeb v rámci informační a komunikační infrastruktury, zatímco pro Spojené státy americké byla klíčová svoboda slova a zaměřily se výhradně na bezpečnost infrastruktury a sítí.[65] Dále Rusko považovalo informace jako takové za zbraň a prostředek k válčení, naopak Spojené státy americké tomuto vůbec nevěnovaly pozornost.[66] A v neposlední řadě Rusko zdůrazňovalo potřebu mezinárodní právní úpravy, avšak Spojené státy americké ji nepovažovaly za nezbytně nutnou.[67] Během let 2005 až 2008 dokonce byly Spojené státy americké jediným státem, který hlasoval proti přijetí rezoluce dotýkající se onoho tématu.[68]

Na základě požadavku Valného shromáždění OSN generální tajemník svolal skupinu vládních expertů, aby zvážila potenciální kybernetické hrozby a nalezla jejich možná řešení. Patnáctičlenná expertní skupina se zatím sešla čtyřikrát. Poprvé to bylo v roce 2004, ale nemohla se shodnout na tom, které nové hrozby zahrnout a zda by se diskuse měla zaměřit na informační obsah, nebo informační infrastrukturu.[69] Druhá skupina z přelomu let 2009/2010 byla poznamenána politickým napětím mezi oběťmi kybernetických útoků (Estonskem a Gruzií) a Ruskem a ve své závěrečné zprávě pouze uznává existenci kybernetických hrozeb a dále

[63] Rezoluce Valného shromáždění OSN A/RES/69/28: *Developments in the field of information and telecommunications in the context of international security*. (2014) Dostupné z: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/69/28

[64] TIKK-RINGAS, E. *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*. Geneva: ICT4Peace Publishing, 2012. 14 pp. Dostupné z: http://www.ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf

[65] Tamtéž.

[66] Tamtéž.

[67] Tamtéž.

[68] Tamtéž.

[69] UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS. *Developments in the field of information and telecommunications in the context of international security: Fact Sheet* [online]. 2014. 2 pp. [cit. 2015-09-19]. Dostupné z: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2014/10/Information-Security-Fact-Sheet-Oct2014.pdf

vyzdvihuje nutnost vymezení definic, dialogu o normách, budování důvěry a výměny informací a technologií.[70] Třetí skupina z let 2012/2013 učinila významný pokrok, když se dohodla na použitelnosti mezinárodního práva v kybernetickém prostoru a na tom, že státní suverenita se vztahuje na činnosti související s ICT a na infrastrukturu nacházející se na státním území; mimo jiné zdůrazňuje dobré úmysly při užívání ICT spolu se základními lidskými právy v souvislosti s kybernetickou bezpečností.[71] Naposledy byla skupina ustanovena v roce 2014 a její setkání probíhají v průběhu letošního roku.[72]

Kromě Prvního výboru pro odzbrojení a mezinárodní bezpečnost se tímto tématem taktéž zabývá Úřad OSN pro drogy a kriminalitu[73] a Hospodářská a sociální rada[74].

7.1.2 NATO

Jako zásadní milník se ukázal rozsáhlý kybernetický útok na Estonsko v roce 2007, který ukázal, jak je NATO nepřipravené na řešení podobných kybernetických útoků na ICT infrastrukturu. Výsledkem bylo v roce 2008 na summitu v Bukurešti ustanovení kybernetické bezpečnosti jako jedné z priorit NATO. K již existujícímu NCRIC (anglicky *NATO Computer Incident Response Capability*) zajišťující centralizovanou obranu vlastních aliančních sít, došlo k založení CDMA (*Cyber Defence Management Authority*) vytvářející středisko pro koordinaci kybernetické odpovědi členských států.[75] Vedle toho bylo vytvořeno centrum excelence NATO nacházející se v estonském Tallinu pro výzkum a vzdělávání v oblasti kybernetické bezpečnosti.[76]

7.1.3 EU

EU se problematikou ochrany kritické infrastruktury a kybernetickou kriminalitou částečně zabývalo již před kybernetickými útoky na Estonsko v roce 2007, avšak i pro EU tato událost představovala významný milník. V roce 2013 byla přijata „Strategie EU pro kybernetickou bezpečnost" stavějící na principech bezpečného, otevřeného a svobodného internetu/kybernetického prostoru. Ve strategii jsou stanoveny základní plány pro „*dosažení kybernetické odolnosti, výrazné snížení kyberkriminality, vypracování politiky a vybudování kapacit pro účely kybernetické obrany v souvislosti se společnou bezpečnostní a obrannou*

[70] Tamtéž.
[71] Tamtéž.
[72] Tamtéž.
[73] Viz více https://www.unodc.org/unodc/index.html
[74] Viz více http://www.un.org/en/ecosoc/
[75] Cyber security. *NATO* [online]. [cit. 2015-09-19]. Dostupné z: http://www.nato.int/cps/en/natohq/topics_78170.htm
[76] Viz více NATO CCDCOE [online]. [cit. 2015-09-19]. Dostupné z: https://ccdcoe.org

politikou EU, rozvoj průmyslových a technologických zdrojů pro kybernetickou bezpečnost, zavedení soudržné mezinárodní politiky EU týkající se kyberprostoru."[77]

7.1.4 Další regionální organizace

Organizace amerických států již v roce 2004 přijala rezoluci „The Inter-American Integral Strategy to Combat Threats to Cyber Security"[78] zaměřenou především na boj proti kybernetické kriminalitě. Dalším významným dokumentem je přijetí rezoluce „Declaration on Strenghtening Cyber security in Americas"[79] z roku 2012, která vyzývá členské státy k vytvoření národních strategií kybernetické bezpečnosti a zároveň by mělo dojít k posílení mezinárodní spolupráce.

Díky iniciativě Rady Evropy vstoupila v platnost v roce 2004 „Úmluva o počítačové kriminalitě",[80] která se snaží o mezinárodní harmonizaci národní právní úpravy počítačové kriminality. Její význam tkví v tom, že se jedná o jedinou úmluvu, kterou ratifikovala většina evropských států[81] spolu se Spojenými státy americkými, Kanadou, Japonskem, Austrálií, Dominikánskou republikou, Mauritiem, Panamou a Srí Lankou.[82] Prozatím jsou jejími signatářskými státy ty, které již nějaké nástroje k potírání počítačové kriminality měly. Cílem je mezinárodní spolupráce, a aby bylo dosaženo alespoň minimální úrovně harmonizace stanovené tímto dokumentem. Díky tomu by bylo možné zabránit kybernetickému útoku velkého rozsahu z oblastí, kde se pachatelé cítí bezpečně.

Africká unie se nedávno vydala ohledně kybernetické bezpečnosti obdobným směrem jako Evropská unie a v roce 2014 přijala „Convention on Cyber Security & Personal Data Protection".[83] Důvodem je hlavně to, že africké státy si přejí zlepšit přístup k širokopásmovému internetu, jenže být připojen ke zbytku světa s sebou nese rizika v podobě kybernetických

[77] Posilování kybernetické bezpečnosti v EU. *Evropská rada, Rada Evropské Unie* [online]. [cit. 2015-09-19]. Dostupné z: http://www.consilium.europa.eu/cs/policies/cyber-security/
[78] Viz více http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm
[79] Viz více https://ccdcoe.org/sites/default/files/documents/OAS-120307-DeclarationCSAmericas.pdf
[80] Viz více http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[81] Kromě Andorry, Irska, Lichtenštejnska, Monaka, Řecka, Ruska, San Marina a Švédska.
[82] Convention on Cybercrime. *Council of Europe* [online]. [cit. 2015-09-19]. Dostupné z: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185
[83] Viz více http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf

hrozeb, což si africké státy uvědomují.[84] Hlavním úkolem bylo vytvořit novou kybernetickou legislativu vycházející z potřeb kontinentu a zároveň posílit regionální spolupráci.

7.2 Státy

Na národní úrovni je kybernetická bezpečnost většinou zabezpečována pomocí týmů CERT (anglicky *Computer Emergency Response Team*) nebo CSIRT (anglicky *Computer Security Incident Response Team*), které jsou ve své stanovené působnosti zodpovědné za řešení všech bezpečnostních incidentů a pomoc při obnově systémů.[85] Celosvětově působící asociací sdružující tyto pracoviště je FIRST (anglicky *Forum for Incident Response and Security Teams*).[86]

7.3 Nevládní organizace

Výzkumný institut OSN pro otázky odzbrojení v roce 2012 publikoval předběžné hodnocení kybernetické bezpečnosti a kybernetické války. Předmětem jeho výzkumu bylo, jak se členské státy OSN zabývají kybernetickou bezpečností, zda mají vojenské velení a kybernetické vojenské doktríny, a zda usilují o získání kybernetických útočných schopností. Podle této zprávy pouze 33 členských států zahrnulo kybernetickou válku do svého vojenského plánování.[87]

8 Závěr

Žijeme ve světě řízeném počítači, což nám do jisté míry usnadňuje život, ale zároveň nás čím dál větší závislost na IT systémech činí zranitelnými. Organizované zločinecké skupiny, extremisté a teroristé patří k nejprogresivnějším uživatelům moderních ICT, protože skrze ně se dokážou dostat k tomu, co je v současnosti nejhodnotnější, tedy k informacím uchovávaným v počítačových systémech, a následně je zneužít. Rozvoj informačních a komunikačních technologií v kontextu mezinárodní bezpečnosti představuje proto jednu z nejdůležitějších a nejaktuálnějších otázek dneška. V globálním měřítku musí být kladen důraz zejména na hrozby kyberteroristických útoků a s nimi související ochranu kritické infrastruktury pro potlačování organizovaného zločinu. Vzhledem k rostoucí komplexitě hrozeb, jejich sofistikovanosti a faktu, že kybernetické útoky mohou zasáhnout kohokoliv a kdykoliv, bude

[84] Cyber security. *African Union* [online]. [cit. 2015-09-19]. Dostupné z: http://pages.au.int/infosoc/cybersecurity?q=infosoc/cybersecurity

[85] HRŮZA, P; PITAŠ J; BRECHTA, B. aj. *Kybernetická bezpečnost II*. Brno: Univerzita obrany, 2013. 1. vydání. 100 s. ISBN 978-80-7231-931-2. s. 15,

[86] JIRÁSEK, P.; NOVÁK, L; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie a AFCEA, 2013. 2. aktualizované vydání. 200 s. ISBN 978-80-7251-397-0. s. 38.

[87] UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH. The Cyber Index: International Security Trends and Realities. New York and Geneva: United Nations, 2013, 140 pp. Dostupné také z: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

proto nutné k řešení kybernetických hrozeb dosáhnout konsensu na půdě mezinárodního společenství. I posléze bude nezbytná úzká kooperace na mezinárodní úrovni. Jedině intenzivní prohloubení spolupráce je podmínkou jakéhokoliv efektivního přístupu k bezpečnému a stabilnímu kybernetickému prostoru.

Otázky k zamyšlení

- Jak je realizována kybernetická bezpečnost ve vašem státě?
- Jak se liší výzvy při zajišťování ICT bezpečnosti v rozvinutých a rozvojových zemích?
- Jakým způsobem by státy měly reagovat na kybernetický útok?
- Jaká opatření mohou být přijata mezinárodním společenstvím ke zvýšení informační bezpečnosti na globální úrovni?
- Jak mohou státy a mezinárodní společenství zdůvodnit potřebu zvýšené bezpečnosti ICT a zároveň vydělávat na přínosu ICT pro jejich rozvoj?
- Do jaké míry mohou být prostředky kybernetického terorismu nástrojem klasického terorismu?
- Jak je možné omezit fungování teroristických skupin na internetu?
- Do jaké míry mohou státy vyvíjet ICT pro vojenské a zpravodajské účely?
- Jakou roli by měl hrát soukromý sektor při zajišťování bezpečnosti ICT?
- Je důležitější soukromí nebo ochrana obyvatel?

Doporučené zdroje

ICT4Peace Foundation: www.ict4peace.org

ICT4Peace Foundation si klade za cíl zachraňovat životy a chránit lidskou důstojnost skrze ICT užívané při krizovém řízení a humanitární pomoci; kybernetickou bezpečnost a mírový kybernetický prostor podporuje prostřednictvím mezinárodních jednání s vládami, korporacemi a nestátními aktéry.

International Criminal Police Organization: www.interpol.int

INTERPOL je největší mezinárodní policejní organizace na světě, která čítá 190 členů.

International Telecommunication Union: www.itu.int

ITU je specializovaná agentura OSN, jež je zodpovědná za otázky týkající se ICT a zahrnuje v sobě členy jak z veřejné, tak i ze soukromé sféry.

NATO CCD COE: https://ccdcoe.org

NATO CCD COE je jedním z center excelence NATO nacházející se v estonském Tallinu, jejímž úkolem je zlepšit spolupráci a sdílení informací mezi NATO a jeho členskými státy v oblasti kybernetické bezpečnosti.

United Nations Institute for Disarmament Research: www.unidir.org

UNIDIR představuje autonomní institut v rámci OSN, jehož posláním je pomoci mezinárodnímu společenství k prosperujícímu mírovému světu prostřednictvím hledání a realizací řešení pro odzbrojení a nové bezpečnostní výzvy.

United Nations Office for Disarmament Affairs: www.un.org/disarmament

UNODA je úřad Sekretariátu OSN podporující preventivní odzbrojovací opatření.

Použité zdroje

25 Biggest Cyber Attacks In History [online]. 2013. [cit. 2015-09-19]. Dostupné z: http://list25.com/25-biggest-cyber-attacks-in-history/5/

ARQUILLA, J; RONFELDT, D. (eds.). *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND Corporation, 2001. 380 pp. ISBN 0-8330-3030-2.

BASTL, M; GRUBEROVÁ, Z. Kyberprostor jako „pátá doména"?. *Vojenské rozhledy* [online]. 2013, 22 (54), ISSN 1210-3292. Dostupné z:http://www.vojenskerozhledy.cz/kategorie/kyberprostor-jako-pata-domena

Convention on Cybercrime. *Council of Europe* [online]. [cit. 2015-09-19]. Dostupné z: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185

Cyberspace Operations [online]. 2013. 70 pp. [cit. 2015-09-19]. Dostupné z: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

Cyberspace. *Encyclopedia Britannica* [online]. [cit. 2015-09-19]. Dostupné z: http://www.britannica.com/topic/cyberspace

Cyber security. *African Union* [online]. [cit. 2015-09-19]. Dostupné z: http://pages.au.int/infosoc/cybersecurity?q=infosoc/cybersecurity

Cyber security. *NATO* [online]. [cit. 2015-09-19]. Dostupné z: http://www.nato.int/cps/en/natohq/topics_78170.htm

Developments in the field of information and telecommunications in the context of international security. *United Nations Office for Disarmament Affairs* [online]. [cit. 2015-09-19]. Dostupné z: http://www.un.org/disarmament/topics/informationsecurity/

DOGRUL, M; ASLAN, A; CELIK, E. *Developing an International Cooperation on Cyber Defense and Deterrence against Cyberterrorism* [online]. 2011. [cit. 2015-09-19]. Dostupné z: https://ccdcoe.org/ICCC/materials/proceedings/dogrul_aslan_celik.pdf

DRMOLA, J. Konceptualizace kyberterorismu, *Vojenské rozhledy*, 2013, 22 (54), ISSN 1210-3292. Dostupné z: http://www.vojenskerozhledy.cz/kategorie/konceptualizace-kyberterorismu

GERCKE, M. *Understanding cybercrime: phenomena, challeges and legal response* [online]. Geneva: International Telecommunication Union, 2012. [cit. 2015-09-19]. Dostupné z: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

GRILLINGEROVÁ, I. Odborník na kyberprostor: ČR nemá ambice regulovat internet [online]. *E-polis.cz*, 2015. [cit. 2015-09-19]. Dostupné z: http://www.e-polis.cz/clanek/odbornik-na-kyberprostor-cr-nema-ambice-regulovat-internet.html

HRŮZA, P; PITAŠ J; BRECHTA, B. aj. *Kybernetická bezpečnost II*. Brno: Univerzita obrany, 2013. 1. vydání. 100 s. ISBN 978-80-7231-931-2.

Information and Communications Technology (ICT). *Technopedia* [online]. [cit. 2015-09-19]. Dostupné z: http://www.techopedia.com/definition/24152/information-and-communications-technology-ict

JANOUŠEK, M. Kyberterorismus: terorismus informační společnosti. *Obrana a strategie* [online]. 2006, (2) [cit. 2015-09-19]. DOI: 10.3849/1802-7199. ISSN 1802-7199. Dostupné z: http://www.obranaastrategie.cz/cs/archiv/rocnik-2006/2-2006/kyberterorismus-terorismus-informacni-spolecnosti.html#.VYV-VI0w-po

JIRÁSEK, P.; NOVÁK, L; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie a AFCEA, 2013. 2. aktualizované vydání. 200 s. ISBN 978-80-7251-397-0.

Joint Chiefs of Staff. *Joint Terminology for Cyberspace Operations*. [online] 2010. 16 pp. [cit. 2015-09-19] Dostupné z: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf

KUŽEL, S. Kybernetická kriminalita I: Co se děje v kyberprostoru. *Business IT* [online]. 2012. [cit. 2015-09-19]. Dostupné z: http://www.businessit.cz/cz/kyberneticka-kriminalita-i-co-se-deje-v-kyberprostoru.php

MAYER, M; MARTINO, L; MAZURIER, P. How would you define Cyberspace? *Academia.edu* [online]. 2014. [cit. 2015-09-19]. Dostupné z: https://www.academia.edu/7096442/How_would_you_define_Cyberspace

MINISTERSTVO OBRANY ČESKÉ REPUBLIKY. *Výroční zpráva o činnosti Vojenského zpravodajství za rok 2013* [online]. 2013. 28 s. [cit. 2015-09-19]. Dostupné z: http://admin.vzcr.cz/shared/clanky/20/V%C3%BDro%C4%8Dn%C3%AD%20zpr%C3%A1va%202013.pdf

NATO CCDCOE [online]. Dostupné z: https://ccdcoe.org

Note by the Secretary-General A/68/98: *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. (2013). Dostupné z: http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-

information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf

Organization of American States [online]. Dostupné z: http://www.oas.org/

Posilování kybernetické bezpečnosti v EU. *Evropská rada, Rada Evropské Unie* [online]. [cit. 2015-09-19]. Dostupné z: http://www.consilium.europa.eu/cs/policies/cyber-security/

POŽÁR, J. *Některé trendy informační války, počítačové kriminality a kyberterorismu*. Dostupné z: http://www.files.sves.webnode.cz/200004808-c759bc94a4/sbornik.pdf

Připravte se, bude válka. *E15* [online]. 2013. [cit. 2015-09-19]. Dostupné z: http://euro.e15.cz/archiv/pripravte-se-bude-valka-959907

Rezoluce Valného shromáždění OSN A/RES/53/70: *Developments in the field of information and telecommunications in the context of international security*. (1999) Dostupné z: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70

Rezoluce Valného shromáždění OSN A/RES/69/28: *Developments in the field of information and telecommunications in the context of international security*. (2014) Dostupné z: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/69/28

SCHMIDT, N. Kyberprostor bude strategickým místem budoucnosti. *Natoaktual.cz* [online]. 2014. [cit. 2015-09-19]. Dostupné z: http://www.natoaktual.cz/kyberprostor-bude-strategickym-mistem-budoucnosti-fyl/na_analyzy.aspx?c=A140630_135804_na_analyzy_m02

SCHMITT, M. N. International Law in Cyberspace: The Koh Speech and Talinn Manual Juxtaposed. *Harvard Law Journal* [online]. 2012, (54). 25 pp. [cit. 2015-09-19]. Dostupné z: http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf

THEOHARY, C. A.; ROLLINS, J. W. Cyberwarfare and Cyberterrorism: In Brief. *Congressional Research Service* [online]. 2015. 15 pp. [cit. 2015-09-19]. Dostupné z: http://fas.org/sgp/crs/natsec/R43955.pdf

TIKK-RINGAS, E. *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*. Geneva: ICT4Peace Publishing, 2012. 14 pp. Dostupné z: http://www.ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf

United Nations Economic and Social Council [online]. Dostupné z: http://www.un.org/en/ecosoc/

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH. *The Cyber Index: International Security Trends and Realities*. New York and Geneva: United Nations, 2013,

140 pp. Dostupné také z: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS. *Developments in the field of information and telecommunications in the context of international security: Fact Sheet* [online]. 2014. 2 pp. [cit. 2015-09-19]. Dostupné z: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2014/10/Information-Security-Fact-Sheet-Oct2014.pdf

United Nations Office on Drugs and Crime [online]. Dostupné z: https://www.unodc.org/unodc/index.html

United Nations. *Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: UN, 2011. Disarmament: Study series, 33. ISBN 978-92-1-142281-8.

WEIMANN, G. Cyberterrorism: How real is the threat? *United States Institute of Peace* [online]. [cit. 2015-09-19]. 12 pp. Dostupné z:http://www.usip.org/sites/default/files/sr119.pdf

WOLTER, D. The UN Takes a Big Step Forward on Cybersecurity. *Arms Control Association* [online]. 2013. [cit. 2015-09-19]. Dostupné z: https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity

Základy IT gramotnosti [online]. [cit. 2015-09-19]. Dostupné z: http://is.muni.cz/do/1492/el/sitmu/law/html/index.html

Top partneři

Generální partner
Pražského studentskeho summitu

The Kellner Family Foundation

Hlavní partner
Modelu OSN

G2 OD KOMERČNÍ BANKY

Hlavní partner Modelu NATO

Ministerstvo zahraničních věcí České republiky

Univerzitní partner

VŠE Vysoká škola ekonomická v Praze

Hlavní partner Modelu EU

Evropská komise

Partner jednání

KONGRESOVÉ CENTRUM PRAHA

Partner zahájení

interhotel AMBASSADOR ZLATÁ HUSA *****

Partneři Modelů

Embassy of Canada
Ambassade du Canada

US embassy

NATO OTAN

Visegrad Fund

Česko-německý fond budoucnosti
Deutsch-tschechischer Zukunftsfonds

Mediální partneři

Hlavní mediální partner

HOSPODÁŘSKÉ NOVINY

Hlavní mediální partner

IHNED.cz

Mediální partner

RESPEKT

Partner Chronicle

METROPOLITNÍ UNIVERZITA PRAHA

Za podpory

PRAHA PRAGUE PRAGA PRAG

MĚSTSKÁ ČÁST PRAHA 3

AUTO ZRUCKÝ DEALER NISSAN

Informační centrum o NATO
NATO Information Center

SCIO

Asociace pro mezinárodní otázky
Association for International Affairs

Pražský studentský summit
projekt Asociace pro mezinárodní otázky