Univerzita Karlova v Praze
Právnická fakulta

Z(a)traceni v kyberprostoru: Státy, online-útoky a mezinárodní právo

Studentská vědecká a odborná činnost

Kategorie: magisterské studium

2014
VII. ročník SVOČ

Autor: Bc. Tomáš Bruner, 3. ročník
Konzultant: JUDr. Ján Matejka, Ph.D.

Čestné prohlášení a souhlas s publikací práce

Prohlašuji, že jsem práci předkládanou do VII. ročníku Studentské vědecké a odborné činnosti (SVOČ) vypracoval samostatně za použití literatury a zdrojů v ní uvedených. Dále prohlašuji, že práce nebyla ani jako celek, ani z podstatné části dříve publikována, obhájena jako součást bakalářské, diplomové, rigorózní nebo jiné studentské kvalifikační práce a nebyla přihlášena do předchozích ročníků SVOČ či jiné soutěže.

Souhlasím s užitím této práce rozšiřováním, rozmnožováním a sdělováním veřejnosti v neomezeném rozsahu pro účely publikace a prezentace PF UK, včetně užití třetími osobami.

V Praze dne 11. dubna 2014

……. ……
Tomáš Bruner

Poděkování

Tímto bych chtěl poděkovat JUDr. Jánu Matejkovi, Ph.D., za vstřícnost, s níž se ujal konzultací mé práce, za podnětné připomínky a za doporučení ohledně relevantní literatury, která zásadním způsobem rozšířila mé obzory. Za doporučení děkuji také doc. JUDr. Vladimíru Balašovi, CSc. V neposlední řadě zaslouží velký dík Mgr. Nikola Schmidt, bez jehož vydatné pomoci a kurzu *Cybersecurity and International Relations* bych jen stěží získával řadu relevantních informací a materiálů.

Obsah:

„Lawyers don’t win wars.

But can they lose a war? We’re likely to find out, and soon.
Lawyers across the government have raised so many
showstopping legal questions about cyberwar
that they’ve left our military unable to fight,
or even plan for, a war in cyberspace.“

Stewart Baker[1], 2012

[1] BAKER, Stewart A. DUNLAP, Charles J. What is the role of lawyers in cyber warfare? *ABA Journal*. 2012, roč. 98, č. 5. Str. 1.

Úvodem

Česká republika se v loňském roce 2013 dvakrát stala cílem rozsáhlého útoku ze zahraničí. Konkrétněji řečeno, určité cíle v České republice čelily internetovému útoku ve formě tzv. *Distributed Denial of Service (DDoS)*. Takovýto útok má vyřadit napadený informační systém z provozu nebo snížit jeho výkonnost. Útok spočívá v záměrném přetížení napadeného serveru pomocí opakujících se požadavků na tento server[2]. Po praktické stránce se pachatel napojí na velké množství různých počítačů, které se slangovou formou označují jako „botnet" nebo „zombie", a těm poté bez vědomí jejich skutečných uživatelů přikáže, aby zahltily cílový server požadavky. „Systém napadený DDoS útokem se projevuje zejména neobvyklým zpomalením služby, nedostupností části nebo celých webových stránek, extrémním nárůstem spamu apod."[3]

V únoru a březnu 2013 směřovaly takovéto DDoS útoky na servery českých bank, ale také na zpravodajské webové portály. Mimo provoz se octly dokonce i platební terminály. Útok zaznamenaly například Česká spořitelna, Fio Banka, ČSOB, Raiffeisen Bank, ale také Burza cenných papírů v Praze. Dotazy z počítačů, k nimž neznámí útočníci získali přístup, přehltily i nejstarší český webový vyhledávač[4].

V listopadu poté zasáhl čtyřdenní útok server Rádia Svobodná Evropa. Tento útok nepřerušil vysílání rádia, ale výrazně zpomalil nahrávání nových zpráv, fotek a videí na jeho webové stránky. Osmdesát procent útočících „zombie" počítačů pocházelo z území Číny a zbylé množství z Ruska.[5]

Česká republika má vlastní Strategii pro oblast kybernetické bezpečnosti na období 2012 – 2015[6], projednává se přijetí zákona o kybernetické bezpečnosti a Národní bezpečnostní úřad zřídil Národní centrum kybernetické bezpečnosti. Takovéto skutečnosti dokládají, že se i Česká republika stala součástí toho, co mnozí s větší či menší mírou

---

[2] VOLEVECKÝ, Petr. Kybernetické hrozby a jejich trestněprávní kvalifikace. *Trestní právo*. 2011, roč. 15, č. 1, 2011. Str. 12 – 13.
[3] Ibid. str. 13.
[4] *Kybernetické útoky dnes pokračovaly. Terčem byly servery českých bank.* Technet. Idnes.cz. Dostupný online [22.3.2014]. URL: < http://technet.idnes.cz/vypadek-serveru-bank-0r8-/sw_internet.aspx?c=A130306_094423_sw_internet_jw >. *Weby českých bank ochromil DDoS útok. NBÚ žádá od postižených data*. Lupa.cz. Dostupný online [22.3.2014]. URL: < http://www.lupa.cz/clanky/web-ceske-sporitelny-neni-dostupny-vcetne-online-sluzeb-servis24/ >
[5] *Rádio Svobodná Evropa se stalo terčem hackerů*. Deník. 18/11/2013. Dostupný online [22.3.2014]. URL: < http://www.denik.cz/z_domova/radio-svobodna-evropa-se-stalo-tercem-utoku-hackeru-20131118.html > *US-funded Radio Free Europe hit by cyberattack*. The Huffington Post. 19/11/2013. Dostupný online [22.3.2014]. URL: < http://www.huffingtonpost.com/huff-wires/20131119/eu-czech-radio-free-europe/?utm_hp_ref=travel&ir=travel
[6] Dostupný online [22.3.2014]. URL: < www.govcert.cz/download/nodeid-727 / >

přesnosti či nadsázky označují jako kybernetická válka[7] nebo její postupná předehra.

Záměrně necháváme stranou diskuzi, nakolik je pojem *kybernetická válka* adekvátní a použitelný, nebo nakolik tato „válka“ naplňuje kritéria definice ozbrojeného konfliktu, kterou poskytl Mezinárodní trestní tribunál pro bývalou Jugoslávii v případu Tadič. Nicméně nelze přehlédnout, že na celém světě v nedávné minulosti proběhla řada událostí naznačující, že se kybernetický prostor[8] může stát spíše *anarchickým*[9] bojištěm nežli místem, ve kterém se státy i nestátní aktéři řídí psanými či nepsanými pravidly *společenské smlouvy* o pokojném soužití. Čím více společnost spoléhá na informační systémy, tím větší je pravděpodobnost, že se tyto systémy stanou cílem útoku[10]. Vybrané příklady masivní kybernetické agresivity můžeme krátce připomenout.

V květnu 2007 čelilo Estonsko velmi intenzivním DDoS útokům, které zablokovaly servery tamní vlády, bank i řady dalších institucí. Pravděpodobně se jednalo o odplatu ruských hackerů za to, že Estonsko odstranilo sochu sovětského vojáka z centra Talinnu. Některé zdroje uvádějí, že útoky probíhaly na popud ruské vlády. Ministr obrany Estonska tehdy formuloval klíčový otazník mezinárodního práva v přirovnání, jaký je rozdíl mezi takto masivním DDoS útokem a vojenskou blokádou přístavu[11]. Ať už může být odpověď jakkoli provokativní, společný článek 5 Smlouvy Severoatlantické aliance (NATO) se neuplatnil.

Kybernetické útoky se využívají i při klasických vojenských misích. Jedním příkladem je operace Orchard. V září 2007 Izrael kybernetickým útokem úspěšně vyřadil syrskou protileteckou obranu a následně letecky zaútočil na domnělé syrské jaderné zařízení. Izraelský software v tomto případě pronikl do počítačů syrských obránců a zaznamenal hodnoty, které pak ve smyčce pouštěl během útoku. Ačkoli izraelské letectvo překročilo hranice a blížilo se k cíli, monitory syrským obráncům ukazovaly údaje z okamžiků, kdy byla obloha nad jejich hlavami prázdná. O dva roky později se naopak stal cílem Izrael. V průběhu ofenzivy v pásmu

---

[7] FARWELL, James P. ROHOZINSKI, Rafal. The New Reality of Cyber War. *Survival: Global Politics and Strategy*. 2012, roč. 54, č. 4. 2012. Dostupný online [22.3.2014]. URL: < http://www.tandfonline.com/loi/tsur20 >
STONE, John. Cyberwar will take place! Journal of Strategic Studies. 2013, roč. 36, č. 1. Dostupný online [22.3.2014]. URL: < http://www.tandfonline.com/loi/fjss20 >.
LIFF Adam P. The Proliferation of Cyberwarfare Capabilites and Interstate War, Redux: Liff Responds to Junio. *Journal of Strategic Studies*. 2013, roč. 36, č. 1. Dostupný online [22.3.2014]. URL: < http://dx.doi.org/10.1080/01402390.2012.733312 >. LIFLAND, Amy. Cyberwar. The Future Conflict. *Harward International Review*. Spring 2012. **Řada autorů naopak tvrdí, že kybernetická válka nikdy nebude, a bude-li, nebude to válka.**

[8] Definice použitých termínů čtenář nalezne v následující kapitole.

[9] Srov. DAVID G. Post, Against "Against Cyberanarchy“. *Berkeley Technical Law Journal.*2002, roč. 17, č. 1365.

[10] HARAŠTA, Jakub. Právní aspekty kybernetické bezpečnosti ČR – Hrozby a nástroje. *Revue pro právo a technologie*. Roč. 4, č. 8, 2013. Str. 76 – 82.

[11] Digital Fears Emerge After Data Siege in Estonia. The New York Times. Dostupný online [22.3.2014]. URL: < http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 >

Gazy zaútočilo na infrastrukturu izraelské internetové sítě na 5 milionů zneužitých počítačů. Podle izraelského vyjádření šlo o útok kriminální organizace na území bývalého Sovětského svazu, které zaplatilo hnutí Hamas nebo Hizballah.[12] Další kybernetické útoky podporující vojenskou operaci probíhali např. v Gruzii v roce 2008[13].

Mezi nejznámější kybernetické útoky posledních let patří úder směřovaný proti íránskému jadernému programu. V říjnu 2010 byl odhalen počítačový kód Stuxnet, který se šířil po Internetu a napadal vybrané přístroje Siemens. V íránském jaderném zařízení Natanz virus postupně manipuloval s ovládáním centrifug na obohacování uranu. Takovouto sabotáží některé centrifugy zničil a způsobil tak hmotnou škodu. Ačkoli se původ viru nepodařilo dohledat, existují dohady, že za jeho vypuštěním stojí USA s Izraelem, které tak chtěly ukázat, že existují vysoce sofistikované nástroje na omezení íránského jaderného programu[14].

Spekuluje se o tom, že íránskou odvetou za Stuxnet byl útok na počítačovou síť ropné společnosti Saudi Aramco. Virus nakazil na 30 000 počítačů, snížil cenu akcií společnosti a přesvědčil Spojené státy americké a Saudskou Arábii, že plynulost dodávek ropy je nutné chránit nejen proti fyzickým útokům. Ačkoli samotná korporace disponuje značným kapitálem, trvalo ji přes týden, než se s následky útoku plně vyrovnala.[15]

Tím výčet *protiprávních* aktivit v kybernetickém prostoru nekončí. V roce 2013 přinesla společnost Mandiant zprávu o výzkumu, jímž stopovala rozsáhlé špionážní aktivity spočívající především v neoprávněném získávání přístupu k chráněnému a utajovanému obsahu na Internetu. Společnost zjistila, že tato špionáž probíhá pod kontrolou čínské vlády, která tak získala data od více než 140 organizací[16].

Zde zmíněné příklady představují pouze špičku narůstajícího ledovce. V bohatém kazuistickém výčtu bychom mohli pokračovat až do 80. let minulého století, kdy údajně CIA nastražila past na sovětské špióny – dovolila KGB, aby získala průmyslový software, který

---

[12] Significant Cyber Incidents since 2006. Centre for Strategic and International Studies. Dostupný online [22.3.2014]. URL: < https://csis.org/files/publication/120504_Significant_Cyber_Incidents_Since_2006.pdf >. K dalším útokům tamtéž.

[13] MCGAVRAN, Wolfgang. Intended Consequences: Regulating Cyber Attacks. *Tulane Journal of Technology and Intellectual Property*. 2009. Str. 265 Dostupný online [22.3.2014]. URL: < https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=12+Tul.+J.+Tech.+%26+Intell.+Prop.+259&srctype=smi&srcid=3B15&key=0f2fef5a9d4661701cc02d5b5bc5be35>

[14] COLLINS, Sean. McCombie, Stephen. Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*. 2012, roč. 7, č. 1. Dostupný online [22.3.2014]. URL: < http://www.tandfonline.com/loi/rpic20 >
FARWELL, James. P., ROHOZINSKI, Rafal. Stuxnet and the Future of Cyber War. *Survival: Global Politics and Strategy*. 2011, roč. 53, č. 1. Dostupný online [22.3.2014]. URL: < http://dx.doi.org/10.1080/00396338.2011.555586 >

[15] BRONK, Christopher. TIKK-RINGAS, Eneken. The Cyber Attack on Saudi Aramco. *Survival. Global Politics and Strategy*. 2013, roč. 55, č. 2, Str. 81 – 96.

[16] *APT1 Exposing One of China's Espionage Units*. Mandiant. Dostupný online [22.3.2014]. URL: < http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf >

byl záměrně pozměněn, aby poničil zařízení, v němž měl být nainstalován. V důsledku toho vybouchl sovětský plynovod na Sibiři[17].

Každá další kybernetická operace se odráží v teoretické diskuzi o mezinárodním právu veřejném, kterou prostupují následující otázky: Co je to kybernetický útok a kybernetický prostor? Za jakých podmínek znamená takovýto útok použití síly podle čl. 2, odst. 4 Charty OSN? Kdy zakládá kybernetický útok právo státu na sebeobranu? Jak se vypořádat s faktem, že přičitatelnost je v případě kybernetických útoků velmi obtížná? *A lze vůbec aplikovat mezinárodní právo na kybernetický prostor?* Poslední otázka je přitom z našeho pohledu zásadní pro zodpovězení těch ostatních a více či méně prostupuje celou touto prací.

Tato práce ji, ani otázky předešlé, pochopitelně nemůže vyčerpávajícím způsobem zodpovědět. Místo toho si klade za cíl a na konkrétním případě ukázat úskalí této problematiky a tak spíše dílčím způsobem přispět k probíhající debatě o (mezinárodním) právu v kyberprostoru. Práce si pokládá následující otázku: **Jakého práva a vůči komu se má stát dovolávat, když chce čelit kybernetickým hrozbám ze zahraničí?** Jako příklad státu v tomto případě můžeme používat Českou republiku a za příklad kybernetické hrozby lze vzít DDoS útok. Nicméně práce tohoto konkrétního příkladu využívá i k řadě abstraktnějších úvah a dílčím způsobem hypoteticky řeší i jiné situace. Na teoretické rovině prací prostupují dvě zásadní vzájemně propojené teze. Zaprvé, vnitrostátní ani regionální právní úprava nepostačuje k efektivnímu řešení problémů, které se v kybernetickém prostoru vyskytují. Bude nutné, aby kybernetický prostor reflektovalo mezinárodní právo veřejné v co nejširší podobě. Zadruhé, současné mezinárodní právo veřejné lze na kybernetický prostor aplikovat pouze se značnými obtížemi, důvodem jsou specifika kybernetického prostoru, zejména omezená přičitatelnost chování.

Struktura práce je následující. První kapitola uvádí definice některých pojmů, s nimiž práce operuje, a zamýšlí se obecně nad aplikovatelností práva na kybernetický prostor. Druhá kapitola hledá právo použitelné na kybernetické útoky. Třetí kapitola se týká přičitatelnosti kybernetických útoků, a tudíž odpovědnosti jednotlivce a státu. Specifikuje tedy, vůči komu případné právo uplatňovat. Zároveň se zamýšlí nad některými širšími důsledky, které přináší kybernetický prostor pro mezinárodní odpovědnost států. V závěru čtenář krom shrnutí problematiky nalezne také teoretické zamyšlení nad možnostmi reálné obrany proti kybernetickým hrozbám a jejího právního zdůvodnění. Pro větší přehlednost je problematika shrnuta také v tabulce v příloze této práce.

[17] HARAŠTA, op. cit. Str. 76 – 82.

1. Obecně k terminologii a aplikaci práva na kybernetický prostor

Nejprve je nutné podotknout, že tato práce s jistou mírou samozřejmosti používá pojmy jako Internet, kybernetický prostor a kybernetický útok. Níže uvádíme některé pracovní definice. Práce poté používá i některé pojmy další, vyčerpávající výklad veškerých termínů by bohužel dalece přesáhl její rámec a v mnoha případech by byl nemožný, neboť shody ohledně definic nebylo vůbec dosaženo. Proto si autor práce v termínech, jejichž definice není explicitně uvedena, dovolí odkázat na jejich obvyklý význam v odborném diskurzu.

Rovněž je na místě poznamenat, že cílem této práce není postihnout technické aspekty problematiky, nýbrž stránku (mezinárodně)právní. Proto se práce v případech, kdy by technicky zaměřená publikace poskytla podrobné vysvětlení, spokojí se zjednodušeným konstatováním stávajícího stavu a zahrnuje pouze ty technické záležitosti, které jsou absolutně nezbytné pro pochopení právního rozměru věci.

Klíčový pojem **kybernetický prostor** nemá univerzálně přijímanou definici. Obvykle se vymezuje jako síť vytvořená pomocí telekomunikací zahrnující především Internet, což je velmi zjednodušeně řečeno síť počítačů navzájem propojených určitým protokolem. Jednotlivé počítače spolu v tomto prostředí kooperují, vytvářejí propojený systém výměny dat, který existuje odděleně od hmotného světa, a tím umožňují spojení mezi jednotlivými uživateli.[18]

Obvykle citovanou definicí **kybernetického útoku** je poté popis amerického Oddělení obrany (*Department of Defense*). Podle něj termín kybernetický útok označuje akce užívající počítačové sítě za účelem přerušení, upření, zhoršení kvality, potlačení nebo zničení informací v počítačích nebo počítačových sítích, nebo zničení samotných počítačů či počítačových sítí.[19] V této práci ale víceméně vycházíme ze stejné konceptualizace kybernetického útoku jako Harašta[20]: „Bezpečnostní incidenty jsou často označované jako kybernetické útoky, což v právním prostředí vzbuzuje určitou terminologickou nepříjemnost. Útok jako takový je totiž předmětem mezinárodního práva a předpokládá vojenský konflikt, což zdánlivě diskvalifikuje jeho použití jako zobecňujícího pojmu. Podle některých autorů je tento problém ale pouze virtuální a pojem kybernetický útok se ujal jako generální pojem

[18] SCHAAP, Maroj Arie J. Cyber Warfare operations: Development and use under International Law. *Air Force Law Review*. 2009, roč. 69. Str. 125 – 126.
[19] THE JOINT CHIEFS OF STAFF, JOINT PUB. NO. 3-13, JOINT DOCTRINE FOR INFORMATION. OPERATIONS 1-9 (Oct. 9, 1998), Dostupný online [22.3.2014]. URL: < http://www.dtic.il/dotrine/jel/new-pubs/p3_13.pdf >
[20] HARAŠTA, Jakub. op. cit. Str. 76.

veškerých kybernetických hrozeb namířených proti informačním systémům.[21]“ Tak také bude na následujících řádcích tento termín používán.

Nyní se již zaměřme na otázku použití práva na kybernetický prostor. Vhodný úvod k této problematice poskytuje teoretický spor Easterbrook versus Lessig[22]. Jednu stranu tohoto sporu reprezentoval americký soudce Frank Easterbrook, který tvrdil, že „psát o právu kyberprostoru je, jakoby se psalo o právu koňském, s tím, že ‚koňské právo' samozřejmě neexistuje (…) Technologie by měla prostě přijmout právo, které jsme pro ni vymysleli.“[23] Podle tohoto pohledu by se tak kybernetický prostor měl plně přizpůsobit současným normám. Praxe ale dala za pravdu jeho oponentovi Lawrenci Lessigovi, který tvrdil, specifičnost kyberprostoru pozmění právo, namísto toho, aby právo pozměnilo kyberprostor[24].

Konkrétní verzi tohoto sporu reflektuje i Horowitz[25]. Ten uvádí, že stále zuří debata mezi „exceptionalisty“ a „neexceptionalisty“. Podle prvých si výjimečný charakter kybernetického prostoru vytváří svá vlastní pravidla. Ti druzí tvrdí podobně jako soudce Easterbrook pravý opak – současná pravidla teritoriality a reálného světa jsou plně aplikovatelná na kybernetický prostor. Horowitz poté doplňuje třetí rozměr – pravidla kyberprostoru vytvoří až jeho uživatelé v jisté společenské smlouvě.

Spor se odráží rovněž v ryze mezinárodněprávní diskuzi. Na straně jedné např. Mezinárodní strategie USA pro kybernetický prostor tvrdí, že tento prostor plně ovládají letité zásady mezinárodního práva, jejichž fungování může být jen drobně obměněno. Na straně druhé řada teoretiků tento názor vyvrací a dokládá jeho nedostatky[26].

Vraťme se ale ještě k Lessigově[27] analýze kyberprostoru. Tento autor uvádí, že právo je pouze jedním ze způsobů regulace chování. Mimo něj regulují chování také obecné normy, trh, ale také *architektura*. Právě ta je pro kybernetický prostor zásadní. Lessig[28] vzhledem k maximální decentralizaci kyberprostoru uvádí: „Cyberspace has no nature; it has no

---

[21] Kybernetický útok ovšem může směřovat i proti jinému cíli a tím pádem jeho charakter určuje, že je uskutečněn *prostřednictvím* počítačové sítě.
[22] Převzato z MATEJKA, Ján. *Internet jako objekt práva*. Praha: CZ.NIC, 2013. ISBN 978-80-904248-7-6. Str. 26 – 27.
[23] Ibid.
[24] Ibid.
[25] HOROWITZ, Steven J. As Boundaries Fade: The Social Contract In Cyberspace. Temple University Libraries. 2006. Dostupný online: [22.3.2014]. URL: < http://digital.library.temple.edu/cdm/ref/collection/p15037coll12/id/1617 >
[26] SCHMITT, Michael N. International Law in Cyberspace: The Koch Speech and Tallinn Manual Juxtaposed. Harward International Law Journal. 2012, roč. 54. Dostupný online: [22.3.2014]. URL: < http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf >
[27] LESSIG, Lawrence. The Law of the Horse: What Cyberlaw Might Teach. *Harward Law Review*. 1999. Dostupný online: [22.3.2014]. URL: < http://cyber.law.harvard.edu/works/lessig/LNC_Q_D2.PDF >
[28] Ibid. Str. 6.

particular architecture to be changed. It's code."[29] Právo tak vlastně nemá na kybernetickém prostoru co měnit. Ba právě naopak, kybernetický prostor – kód – omezuje aplikovatelnost práva a tím způsobuje, že právo reguluje jiným způsobem.[30] V reálném prostoru je například snadné zjištění a ověření identity. O jedinci lze získat hodnověrné údaje za relativně nízkých nákladů (například pouhým pohledem). To v kybernetickém prostoru neplatí. Necháme-li stranou podrobnou technickou analýzu, můžeme vyjít z konstatování, že jediné, co lze o jedinci v kyberprostoru zjistit, je IP adresa počítače, který používá[31]. Ovšem je možné více či méně protiprávně sledovat, jaké stránky počítač navštěvuje, nebo prostřednictvím špionážního softwaru zaznamenávat údery na jeho klávesnici. V normálním prostoru by jedinec obvykle záhy zjistil, že někdo (*konkrétní*) sleduje místa, která navštěvuje, a zaznamenává jeho komunikaci. V kyberprostoru se opět primárně dopátrá pouze IP adresy.

Problém identifikace – a obecně charakter či *architektura* Internetu – má zásadní vliv na přičitatelnost chování v kybernetickém prostoru a tím i otázku, vůči komu uplatňovat určité právo. Otázkou přičitatelnosti se zabývá 3. kapitola; nejprve se totiž zaměříme na identifikaci právní úpravy, kterou můžeme na kybernetické útoky použít.

2. Problémy *de lege lata*

Po obecném vstupu do problematiky usiluje tato kapitola o nalezení právní úpravy, kterou lze v daném případě aplikovat a na jejímž základě by se stát – v našem případě Česká republika – mohl dovolávat ochrany před kybernetickým útokem. Kapitola začíná stručným exkurzem do vnitrostátního práva, který nad rámec ukazuje, že i vnitrostátně-právní úprava je na tuto situaci aplikovatelná s obtížemi. Následně již kapitola řeší mezinárodněprávní úpravu.

2.1 Vnitrostátní úprava

Vrátíme-li se k našemu případ DDoS útoků proti cílům v České republice, můžeme se krátce zastavit nad jejich trestněprávní kvalifikací. Dle našeho vnitrostátního práva by takovéto jednání mělo být považováno za trestný čin podle § 230 zák. č. 40/2009 Sb., trestní zákoník, který popisuje neoprávněný přístup k počítačovému systému a nosiči informací. Podle prvního odstavce tohoto paragrafu by bylo možné kvalifikovat získávání jednotlivých „zombie" počítačů pro vlastní útok. Ovšem tyto jednotlivé počítače se nacházely v Rusku a v Číně, tudíž nelze tento odstavec použít. V úvahu by přicházel odstavec druhý, písm. b), kde

[29] „Kybernetický prostor nemá charakter; nemá architekturu. Je to kód."
[30] Ibid. 24.
[31] I tu lze ovšem v některých případech zamaskovat, například tzv. cloudovým útokem.

se stanoví:

„Kdo získá přístup k počítačovému systému nebo k nosiči informací a data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“

Vezměme třeba případ útoku na Rádio Svobodná Evropa a identifikujme překážky, které brání tomu, aby mohla být naplněna definice tohoto trestného činu a založena působnost orgánů činných v trestním řízení. Zaprvé, pachatel v tomto případě *nezískal přístup k počítačovému systému ani k nosiči informací* v ČR. Získal přístup pouze k ruským a čínským počítačům (české právo se neaplikuje), které následně donutil, aby se připojily na server Rádia Svobodná Evropa a tím ho zahltily. Pokud by české právo platilo v Číně a Rusku, byl by tam pachatel postižitelný podle § 230, odst. 1 trestního zákoníku. Nicméně do České republiky, na stránky Radia Svobodná Evropa směřovalo pouze velké množství požadavků z jednotlivých „zombie“ počítačů. V tomto případě nelze *a priori* odlišit, který počítač se na server připojuje v rámci úmyslu pachatele server zablokovat a který počítač tak činí bez tohoto úmyslu. Samotné připojení na server není a nemůže být trestným činem. Zadruhé lze uvažovat o tom, nakolik se jednalo o *data uložená v počítačovém systému nebo na nosiči informací* – útok zpomaloval nahrávání dat (novinek, zpráv, fotografií) na server, tzn. data ještě nebyla uložena v počítačovém systému, ačkoli už mohla být uložena na nosiči informací, z něhož tam byla nahrávána. Zatřetí, *data nebyla vymazána, zničena ani poškozena*, v podstatě ani nebyla učiněna neupotřebitelnými *stricto sensu*. Pouze bylo zpomaleno jejich nahrávání na webové stránky[32].

Také Gřivna[33] podřazuje DDoS útok pod § 230, odst. 2, písm. b). Uvádí, že „[p]otlačením dat jsou případy, kdy data dále existují beze změny, ale pachatel s nimi naložil tak, že je nelze dohledat na jejich původním umístění.“[34] DDoS útok se tedy pohybuje na pomezí potlačení dat a snížení jejich upotřebitelnosti. Obojí je ovšem jen částečné. V úvahu ještě přichází pojetí, že pachatel získal neoprávněně přístup k počítačovému systému v zahraničí, který využil k potlačení a snížení upotřebitelnosti dat jiného počítačového

[32] Ještě lze uvažovat o kvalifikaci podle § 230, odst. 2, písm. d) TZ. Nakolik ovšem pachatel učinil zásah do programového nebo technického vybavení počítače, když se pouze připojil na server?
[33] GŘIVNA, Tomáš. § 230 Neoprávněný přístup k počítačovému systému a nosiči informací. IN Šámal a kol. *Trestní zákoník II: Zvláštní část (§ 140 – 421)*. 2. vydání. Praha: C. H. Beck, 2012. ISBN 978-80-7400-428-5. Str. 2311.
[34] Ibid. 2309.

systému v ČR. Následek tedy nastal v ČR[35]. Mějme ovšem na paměti, že sám Gřivna rozlišuje počítačový systém, který je chráněný zmíněným paragrafem, a počítačovou síť, jejíž ochranu zákon nespecifikuje[36]. Otázkou tedy zůstává, nakolik se ochrana zákonem poskytnutá počítačovému systému vztahuje také na propojení těchto systémů, tedy na *síť*.

Systematický výklad a zařazení trestného činu podle § 230 mezi trestné činy proti majetku také příliš nápovědy, jak situaci vyřešit, neskýtá. *Architektura* kybernetického prostoru tak výrazně komplikuje aplikaci práva.

Skeptický závěr potvrzuje ve své analýze Volevecký, který zdůrazňuje, že kvalifikace DDoS útoku je v českém právu obtížná. Pachatel totiž nezískává přístup k napadeným počítačům. Jednání je možné kvalifikovat podle § 228 trestního zákoníku jako poškození cizí věci. Ovšem bylo by nutné fakticky poškodit věc a způsobit škodu nikoli nepatrnou[37]. Samotné vyčíslení škody v případě útoku na Rádio Svobodná Evropa představuje problém (ačkoli např. při zablokování platebních terminálů v březnu 2013 už o něm lze uvažovat).

I za předpokladu, že by se podařilo DDoS útok proti Svobodné Evropě subsumovat pod některý z paragrafů českého trestního zákoníku, sama Česká republika by situaci vyřešit nemohla už z toho důvodu, že pachatel by se pravděpodobně nacházel v zahraničí, nebo by situaci v zahraničí bylo nutné vyšetřovat, což platí i pro řadu dalších trestných činů spáchaných v kyberprostoru[38]. Identifikace mezinárodněprávní úpravy aplikovatelné při dané situaci tedy zůstává zásadní.

Samozřejmě se nabízí teoretická otázka, zdali je vůbec žádoucí, aby jednala zrovna Česká republika. Nejedná-li se o trestný čin, nemělo by zůstat na jednotlivých subjektech – Rádiu Svobodná Evropa či jednotlivých institucích, aby zabezpečily své stránky a hledaly vhodná protiopatření? Zde lze obecně zmínit argument Lewise[39], který tvrdí, že vlády států by si měly obhájit a zajistit v kybernetickém prostoru svou suverenitu. Podobně jako soukromé aerolinie nechrání vzdušný prostor nad státy, kde operují, nelze po soukromoprávních právnických osobách požadovat, aby si plně zajistily ochranu v kybernetickém prostoru.[40]

---

[35] Srov. § 230, odst. 3, písm. b) TZ a § 4, odst. 2, písm. b) TZ.
[36] Ibid. 2306.
[37] VOLEVECKÝ, Petr. Kybernetické hrozby a jejich trestněprávní kvalifikace. *Trestní právo*. 2011, roč. 15, č. 1. Str. 16 – 17.
[38] Dále k tématu vnitrostátní právní úpravy např. SOKOL, Tomáš. SMEJKAL, Vladimír. Postih počítačové kriminality podle nového trestního zákoníku. *Právní rádce*. 23.7.2009. Dostupný online [22.3.2014]. URL: < http://pravniradce.ihned.cz/c1-37865090-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona >. VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo*. 2010, roč. 14, č. 7-8. Str. 26 – 38.
[39] LEWIS, James A. Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs*. 2010, roč. 16, č. 2.
[40] Jedna z mnoha analogií, která se v odborné literatuře na kybernetický prostor aplikuje. Tato nutně vede k teritorializaci kybernetického prostoru ve smyslu fyzického prostoru. Takovéto *zhmotnění nehmotného* ale

2.2 Mezinárodní právo – regionální smluvní a komunitární úprava

Jedinou mezinárodní smlouvou, která řeší kybernetické útoky, je Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. Listopadu 2001 (dále jako „Budapešťská úmluva"). Článek 5 této smlouvy popisuje opatření proti zásahům do počítačových systémů a stanoví povinnost států takovýmto zásahům zabránit: „Každá smluvní strana přijme legislativní a jiná opatření nezbytná k tomu, aby podle vnitrostátního práva bylo trestným činem jednání spočívající v úmyslném závažném protiprávním narušení fungování počítačového systému vložením, přenesením, poškozením, vymazáním, zhoršením kvality, změnou nebo potlačením počítačových dat."

Česká republika tuto úmluvu podepsala v roce 2005 a ratifikovala v roce 2013. Na jejím základě by tedy mohla upozornit stát, že na jeho území byly počítače zneužity k přehlcení českého serveru, a tím v jeho jurisdikci došlo – slovy českého trestního zákoníku – k získání neoprávněného přístupu k počítačovému systému. Stát by tento trestný čin, implementovaný podle čl. 5 Budapešťské konvence, poté začal v součinnosti s ČR vyšetřovat[41]. Předpokladem ovšem je, že tento stát ratifikoval Budapešťskou konvenci. Pokud se vrátíme k případu DDoS útoku na Rádio Svobodná Evropa, shledáme, že státy, kde se nacházely zneužité „zombie" počítače, k Budapešťské konvenci nepřistoupily.

Harašta zmiňuje dělení kybernetických hrozeb na „kyberkriminalitu, hacktivismus, kybernetickou válku [příp. kyberterorismus] a kybernetickou špionáž"[42]. Podle závažnosti porušení a porušených norem pak Harašta zavádí dělení na „porušení vnitřních nařízení; porušení právní povinnosti; kybernetickou kriminalitu; kybernetický terorismus; kybernetickou válku"[43]. Námi rozebírané DDoS útoky leží na pomezí kybernetické kriminality, terorismu a války. Nicméně z teoretického hlediska nelze nechat bez povšimnutí, že Budapešťská konvence vnímá kybernetický prostor jako místo, kde může probíhat právě ona *kybernetická kriminalita,* případně *hacktivismus* či *špionáž*. Otázkou zůstává, proč členské státy kybernetický prostor doposud nevnímaly a nevnímají také jako prostor, kde

---

může narážet na řadu problémů. Posílí kompetence států (na úkor svobody Internetu?) a případně ujasní otázku odpovědnosti států, nezmění ale architekturu Internetu a staré potíže se mohou vrátit v novém kabátě (zneužití přičitatelnosti apod.).

[41] Úmluva zavádí odpovědnost právnických osob za kybernetické trestné činy, a to i nedbalostní odpovědnost. Otázkou zůstává, nakolik by bylo možné samotný stát považovat za právnickou osobu. Má-li se v budoucích letech vyvinout jistý mezinárodní právní režim kybernetické bezpečnosti, mohou mít ustanovení této úmluvy symbolický význam.

[42] Kyberkriminalita směřuje k obohacení pachatele, hacktivismus má přitáhnout pozornost, kdežto kybernetická válka u státních a kyberterorismus u nestátních aktérů jsou taktiky boje s nepřítelem. Harašta, Jakub. Právní aspekty kybernetické bezpečnosti ČR – Hrozby a nástroje. *Revue pro právo a technologie*. Roč. 4, č. 8, 2013. Str. 76.

[43] Ibid.

může probíhat konflikt v podobě *kybernetické války* nebo *terorismu*.[44]

Určitého stupně relevance nabývají i některé dokumenty Evropské unie[45], například:

- Rozhodnutí Rady 92/242/EHS ze dne 31. 3. 1992 o bezpečnosti informačních systémů;
- Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům;
- Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů – Boj proti spamu a špionážnímu (spyware) a škodlivému softwaru (malicious software) ze dne 15. 11. 2006;
- Sdělení Komise Evropskému Parlamentu, Radě a Evropskému výboru regionů k obecné politice v boji proti počítačové kriminalitě ze dne 22. 5. 2007;
- 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.

Můžeme zobecnit, že tyto dokumenty harmonizují jak právní úpravu, tak i rámcově upravují a stanovují některé faktické postupy členských států při přípravě na kybernetické hrozby nebo jejich odvracení. Obsahují již přesnější vymezení jednotlivých útoků a rozlišují mezi útoky spáchanými prostřednictvím počítačového systému a proti samotnému počítačovému systému.[46] Stran našeho konkrétního příkladu ale bohužel opět nemají pražádný vliv na to, jak se k DDoS útokům postaví Rusko nebo Čína. Dokumenty neupravují, jak vystupovat vůči třetím státům. Kolektivní postup států EU proti státům, z jejichž území vyvstávají kybernetické útoky, by nejspíše – hypoteticky – spadal pod společnou zahraniční a bezpečnostní politiku EU a vyvíjel by se v jednotlivých případech.

V našem případě počítačů útočících z Ruska a Číny, stejně jako v mnoha dalších, si tedy nevystačíme ani s komunitární ani s regionální úpravou. Volevecký trefně podotýká, že „[d]íky rozvoji počítačových a informačních technologií, které udávají mezinárodní charakter kybernetických trestných činů, je efektivní ochrana počítačových dat nemyslitelná bez existence mezinárodního, resp. nadnárodního právního rámce, a to nejen mezi členskými státy

[44] Jak už bylo naznačeno výše, autor práce si je vědom neostré definice těchto termínů, nicméně považoval za vhodné upozornit jejich prostřednictvím na tento zajímavý jev.
[45] Stávající výčet sestaven podle VOLEVECKÝ, P. Kybernetická trestná činnost v mezinárodních dokumentech a v dokumentech ES/EU. *Trestní právo*. 2009, roč. 14, č. 7-8.
[46] Blíže ke komunitární úpravě srov. GŘIVNA, Tomáš. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. *Acta Universitatis Caroline-Iuridica*. 2008, č. 4.

Evropské unie, ale i v **celosvětovém měřítku**."[47] Musíme tedy sáhnout do nejobecnější úpravy mezinárodního práva veřejného. Následující podkapitola se tudíž zaměří na to, co tvoří zmíněný současný nadnárodní právní rámec.

2.3 Mezinárodní právo – obecná úprava

Stran pramenů mezinárodního práva na jeho nejobecnější úrovni se lze dovolávat zejména Charty OSN a obyčejového práva. Ovšem zásadní je, jak jsou tyto dokumenty vykládány a aplikovány na kybernetický prostor. V tomto ohledu se následující řádky opírají zejména o doktrinální výklad[48], který shrnují a kriticky zkoumají.

První a nejzásadnější otázka, kterou je nutné výkladem zodpovědět, zní: Kdy je kybernetický útok použitím síly podle čl. 2, odst. 4 Charty OSN? S trochou nadsázky můžeme odpovědět *téměř nikdy*. Doposud nejvýznamnější výstup doktríny v této oblasti, Talinský manuál o aplikovatelnosti mezinárodní právana kybernetické válčení[49], ve svém pravidlu 10 s jasným odkazem na čl. 2, odst. 4 Charty OSN stanoví: **„**A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."[50] Potíže zde může činit samotné určení, kdy použití síly směřuje proti územní celistvosti a politické nezávislosti státu nebo je uskutečněné způsobem odporujícím cílům OSN. Hned v pravidle následujícím Talinský manuál definuje, kdy je kybernetický útok použitím síly: „A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.**"**[51]

V obou pravidlech vychází Talinský manuál z Charty OSN a nadále odkazuje na případ Mezinárodního soudního dvora Nikaragua[52]. Z komentáře v manuálu lze usoudit, že tento dokument určitý software, například počítačové viry, vnímá jako *zbraň*, čímž dává základ pro aplikaci článku 51 Charty OSN o obraně proti *ozbrojenému* útoku. Jak je ale patrné

[47] VOLEVECKÝ, P. Kybernetická trestná činnost v mezinárodních dokumentech a v dokumentech ES/EU. *Trestní právo*. Roč. 14, č. 7-8, 2009. Zvýraznil autor práce. Str. 27.
[48] Jak čtenář pozná z bibliografie, tématu se velmi intenzivně věnují především americké právní žurnály. Vztah mezi národností pisatelů článků a pohledem na problematiku by jistě stál za samostatný výzkum.
[49] CCDCOE, SCHMITT, Michael N. (ed.) *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York:. Cambridge University Press, 2013. Warfare je se dá také přeložit jako vedení boje.
[50] „Kybernetická operace, která zakládá hrozbu silou nebo použití síly proti územní celistvosti nebo politické nezávislosti státu, nebo která je jiným způsobem neslučitelná s cíli Spojených národů, je protiprávní." Překlady v poznámkách pod čarou provedl autor práce, není-li uvedeno jinak.
[51] „Kybernetická operace zakládá použití síly, když jsou její rozsah a účinky srovnatelné s nekybernetickou operací dosahující úrovně použití síly."
[52] Rozsudek Mezinárodního soudního dvora ze dne 27. června 1986.Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America). Dostupný online [22.3.2014]. URL: < http://www.icj-cij.org/docket/files/70/6503.pdf >.

z výše uvedených citací, samotnou otázku použití síly manuál řeší nejasnou analogií s jakýmsi konvenčním (*non-cyber*) použitím síly. Pro posouzení, zdali je určité jednání v kyberprostoru použitím síly, je tedy nutné posoudit rozsah takového jednání a jeho důsledky („scale and effects"). Tudíž jednání, které má zničit nebo poškodit objekt nebo zabít člověka, je podle Talinského manuálu bezesporu použití síly. Podle tohoto právního výkladu by ovšem útok prostřednictvím viru Stuxnet znamenal použití síly, a tudíž založil právo Iránu na sebeobranu, neboť hmatatelně došlo ke škodám. Útoky na Estonsko v roce 2007 zůstávají v tomto světle na sporné hranici, kde na jedné straně zůstává argument, že nikdo nebyl zraněn a hmotné škody lze obtížně vyčíslit. Na straně druhé leží srovnání DDoS útoku s vojenskou blokádou přístavu. Nicméně mezinárodní společenství výklad, že v Estonsku a v Iránu došlo k použití síly, nepřijalo. Ani napadené státy neuplatnily právo na sebeobranu. *A maiori ad minus* tak jako použití síly nekvalifikujeme ani DDoS útoky proti České republice. Nad rámec řečeného lze poznamenat, že Talinský manuál je obecně velmi restriktivní, co se týče aplikace *ius ad bellum* na kybernetický prostor, zatímco ohledně *ius in bello* dochází k řadě hmatatelných závěrů[53].

Většina výstupů doktríny se víceméně ztotožňuje nebo doplňuje se závěry Talinského manuálu. Řada autorů[54] při klasifikaci kybernetického útoku jako použití síly používá tzv. Schmittova kritéria[55], podle nichž lze některé útoky klasifikovat jako použití síly, jiné tohoto prahu nedosahují a jsou potom pouhým ekonomickým a politickým donucením[56]. Schmitt jako tato kritéria určil závažnost (*severity*), bezprostřednost (*immediacy*), přímost (*directness*), míru narušení či agresivitu (*invasiveness*) a měřitelnost následků (*measurability*). Samotná kritéria ale v tomto případě mohou být předmětem výkladu a rozdílného vnímání. Jaký útok tedy je a jaký není použitím síly, zůstává spornou otázkou.

Jensen[57] podotýká, že rozvoj mezinárodního práva musí ještě pokročit, aby byl kybernetický útok rozeznáván jako použití síly a *ozbrojený* útok, který zakládá právo na

[53] I doktrína souhlasí, že ius in bello lze lépe aplikovat na kybernetické útoky. „Rozdíly mezi konvenčním a kybernetickým válečnictvím spočívají v intenzitě, nikoli v druhovém určení. Takže režim mezinárodního humanitárního práva, který upravuje konvenční válečnictví, může být efektivně aplikován na kybernetické útoky." GERVAIS, Michael. Cyber Attacks and the Laws of War. *Berkeley Journal of International Law*. 2012, roč. 30, č. 2. Str. 579.

[54] GŘIVNA, Tomáš. POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4. Str. 57 – 61. REMUS, Titiriga. Cyber-attacks and International law of armed conflicts; a "jus ad bellum" perspective. *Journal of International Commercial Law and Technology*. 2013, roč. 8, č. 3. Str. 179 – 189.

[55] SCHMITT, Michael. N. Computer Network Attack: The Normative Software. IN *Yearbook of International Humanitarian Law*. Roč. 4. Haag: TMC Asser Press, 2001. Str. 53 – 85.

[56] Přeformulujme otázku Talinských útoků z roku 2007 (pro který se vžil slangový název „eStonia") – Je blokáda přístavu politickým nebo ekonomickým donucením?

[57] JENSEN, Eric Talbot. Computer Attacks on National Infrastructure: A Use of Force Invoking the Right of Self-Defense. *Stanford Journal of International Law*. 2002, roč. 28. Str. 207 – 240.

sebeobranu. Obecně volá po tom, aby státy získaly právo na sebeobranu proti kybernetickému útoku nehledě na to, jestli je takovýto útok použitím síly nebo nikoli: „Whether initiated by an enemy's military, a terrorist organization, or an individual, CNAs [Computer Network Attacks] will be a serious and destabilizing force unless states are given the right to protect themselves with a proportionate response in selfdefense, including anticipatory self-defense, even if the attack does not constitute an armed attack."[58] K totožnému závěru dospívá DeLuca[59].

Podobně Hoisington poznamenává, že se kybernetické útoky odehrávají do jisté míry v právním vakuu. Výklad samotného čl. 2, odst. 4 Charty OSN, která byla napsaná dlouho před vznikem Internetu, je nejasný a kybernetické útoky jen přilévají pověstný olej do ohně. Ve výsledku tak podle něj bude nutné, aby státy rozšířily výklad daného ustanovení Charty, nebo přijaly nové (právní) prostředky, jak čelit těmto hrozbám.[60]

Waxman[61] dále poznamenává, že výklad Charty, včetně výkladu čl. 2, odst. 4, vždy podléhal mocenským vlivům, což se obzvlášť intenzivně projevovalo za studené války. Podle něj kybernetický prostor zůstane velmi nejistým právním terénem a výklad právních norem, které na něj lze aplikovat, se tak jako za studené války může podrobit potřebám velmocí. Bude záležet na tom, jaké stanovisko k útokům v tomto prostředí zaujmou Spojené státy americké a další hegemonické státy a jak na toto stanovisko zareaguje zbytek mezinárodního společenství. [62] K velmi podobné úvaze vede názor, že by kybernetické útoky mohly být za takovouto hrozbu označeny Radou bezpečnosti OSN podle čl. 39 Charty OSN. Rada bezpečnosti prakticky může označit za hrozbu cokoli, a tudíž záleží na jejích (stálých) členech – opět více či méně hegemonických státech[63].

McGavran se opírá o článek 36 prvního Dodatkového protokolu k Ženevským úmluvám a stanoví povinnost smluvních stran zvážit, jestli nově vyvinuté druhy zbraní nejsou

[58] „Ať už zosnované nepřátelskou armádou, teroristickou skupinou nebo jednotlivcem, útoky na počítačovou síť budou závažnou a destabilizující silou, pokud státy nezískají právo bránit se proti nim přiměřenou sebeobrannou reakcí, včetně předstižné obrany, i když útok neobnáší ozbrojený útok."
[59] DELUCA, Christopher D. The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors. *Pace International Law Review Online Companion*. 2013, roč. 3, č. 9. 2013. Str. 315.
[60] HOISINGTON, Mathew. Cyberwarfare and the Use of Force Giving Rise to the Right of Selfdefense. *Boston Colledge International and Comparative Law Review*. 2009, roč. 32, č. 2. Str. 439 – 454.
[61] WAXMAN, Mathew C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). *The Yale Journal of International Law*. 2011, roč. 36, č. 2. Str. 458.
[62] V akademickém prostředí probíhá debata o tzv. dvojsečném státním zájmu. Státy na jednu stranu potřebují kybernetický prostor bezpečný a maximálně kontrolovaný, na druhou stranu jim vyhovuje jeho svobodný charakter, protože zde mohou podnikat těžko odhalitelné výpady proti svým rivalům. Jaký model převáží bude nejspíše záležet
[63] GŘIVNA, Tomáš. POLČÁK, Radim (eds.). op. cit. Str. 60.

za určitých okolností zakázány Protokolem nebo jinou normou mezinárodního práva.[64] Dle názoru autora této práce se jedná o vyjádření Martensovy klauzule, které je ovšem z podstaty věci normou *in bello* (respektive normou odzbrojení), nikoli *ad bellum*. Jistá vodítka však nabízí – zejména pokud by kybernetický útok způsoboval nadměrné utrpení nebo měl (pravděpodobněji) nediskriminační charakter, mohl by být zakázán, a to jak *in bello*, tak jako prostředek zahájení války.

Shrňme tedy dvěma závěry. Zaprvé, ***teoreticky*** lze kvalifikovat kybernetický útok jako použití síly podle čl. 2, odst. 4 Charty OSN jen v malém množství případů, kdy výsledek daného jednání odpovídá výsledku použití konvenční síly (ačkoli ani samotné konvenční použití síly a jeho výsledek nejsou jasně definovány). Zadruhé, ***prakticky*** se tak nikdy nestalo. Výstižný je proto následující názor[65]: „The law of war, for example, provides a useful framework for only the very small number of cyber-attacks that amount to an armed attack or that take place in the context of an ongoing armed conflict.“[66]

Právo na obranu proti ozbrojenému útoku podle Charty OSN se tedy pravděpodobně nepoužije. Po jakém jiném právu by tedy měl napadený stát sáhnout? Talinský manuál opět používá případ Nikaragua a pracuje s obyčejovou zásadou neintervenovat ve věcech cizího státu. Pokud tedy není kybernetický útok použitím síly, měl by být označen jako protiprávní intervence ve věcech cizího státu, případně také jako narušení suverenity.[67] Zásada neintervenovat ve věcech cizího státu vyvstává jako nutný důsledek rovnosti a nezávislosti suverénních států a musí být považována za jeden ze základních principů mezinárodního práva[68]. Kybernetický útok je podle ní protiprávní a postižený stát se může na základě této zásady dovolávat toho, aby okamžitě ustal. Postižený stát by se tak mohl uchýlit k retorzím nebo neozbrojeným represáliím. Ovšem ani pod porušení suverenity nelze podřadit všechny kybernetické útoky. Jak uvádí Talinský manuál[69]: “Group of Experts could achieve no consensus as to whether the placement of malware that causes no physical damage (as with

[64] MCGAVRAN, Wolfgang. op. cit. Str. 269.
[65] HATHAWAY, Oona A. (et al). *The Law of Cyber-Attack. California Law Review*. 2012, roč. 100, č. 817. 2012. Str. 817.
[66] „Například válečné právo [zde 1. *ad bellum* i 2. *in bello*] poskytuje použitelný rámec pro malé množství kybernetických útoků, které [1.] dosahují intenzity ozbrojeného útoku, nebo které [2.] probíhají za ozbrojeného konfliktu.“ Poznámky vložit autor práce.
[67] Mezi zastánce tohoto názoru patří BUCHAN, Russel. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict & Security Law*. 2012, roč. 17, č. 2. Str. 212. Srov. také výstup setkání Cyber Security and International Law. London: Chantam House. Dostupný online [22.3.2014]. URL: < http://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf >
[68] JOYER, Christopher C. *International Law in the 21st Century: Rules for Global Governance*. London: Rowman and Littlefield, 2005. ISBN 0742500098. Str. 54
[69] Op. cit. str. 26.

malware used to monitor activities) constitutes a violation of sovereignty."[70]

Úvahy ohledně suverenity nadále rozvíjí Shackelford[71]. Navrhuje dvě možná řešení stávajících komplikací s kyberprostorem. Zaprvé na úrovni jednotlivce lze použít doktrínu v USA známou jako *effects principle*. Tato doktrína určuje, že stát, v němž se nachází oběť určitého protiprávního jednání, může podle svého práva soudit pachatele tohoto protiprávního jednání, ačkoli se tento pachatel nachází v zahraničí.[72] Druhou možností je pohlížet na kybernetický prostor jako na společné dědictví lidstva a mezinárodní prostor, podobně jako je tomu u Antarktidy, hlubokomořského dna nebo vnějšího vesmíru. Státy by jistě mohly tyto možnosti využít. V prvním případě ovšem nastává problém s přičitatelností jednání, odpovědností a povinností cizího státu vyšetřit zločin a vydat pachatele, o čemž bude pojednáno v následující kapitole. Ve druhém případě by státy musely na takovouto volbu nejprve přistoupit, nehledě na to, že režimy mezinárodních prostor fungují také v mnoha ohledech problematicky.

Pokud by kybernetickým útokem vznikla škoda, kterou by se podařilo dokázat a vyčíslit, jistě by poškozený stát (případně formou diplomatické ochrany) mohl vystoupit proti pachateli. S trochou kreativity a s – v této sféře nesmírně populárním – využitím analogie se dá odkázat na případ Slévárny v Trailu[73]. Kybernetický útok by tak mohl být hodnocen podobně jako kouř pronikající z území jednoho státu na území druhého státu, kde působí škodu. Tím už se ale fakticky dostáváme k obsahu následující kapitoly. Vyvstává totiž otázka, kdo je za kybernetické útoky odpovědný, komu jsou přičitatelné. Jinými slovy vůči komu lze vlastně uplatňovat právo na sebeobranu, právo na to, aby nedocházelo k intervenci a narušení suverenity, nebo právo na náhradu škody? Tyto otázky se pokusíme zodpovědět v následující kapitole.

3. Otázka přičitatelnosti

Většina autorů zmíněných v této práci jedním dechem spojuje právní kvalifikaci kybernetického útoku s přičitatelností tohoto útoku. Bez samotné přičitatelnosti – tedy možnosti zjistit pachatele nebo toho, kdo je za útok *nedbalostně* zodpovědný – totiž

[70] „Skupina expertů se neshodla na tom, jestli umístění malwaru, který nezpůsobuje fyzickou škodu (jako malware, který monitoruje aktivity), znamená porušení suverenity." Zde se pro změnu otevírá otázka kybernetické špionáže, na jejíž zpracování by bylo třeba nejméně samostatné práce.
[71] SHACKELFORD, Scott J. From Nuclear War to Net War: Analogizing Cyber Attacks in Intemational Law . *Berkeley Journal of International Law*. 2009, roč. 27, č. 1. Str. 212 – 216.
[72] Srov. § 4, odst. 2, písm b.) českého trestního zákoníku: „Trestný čin se považuje za spáchaný na území České republiky, porušil-li nebo ohrozil-li tu pachatel zájem chráněný trestním zákonem nebo měl-li tu alespoň zčásti takový následek nastat, i když se jednání dopustil v cizině."
[73] Trail Smelter Case (United States v. Canada). Dostupný online [22.3.2014]. URL: < http://legal.un.org/riaa/cases/vol_III/1905-1982.pdf >

neexistuje reálná možnost domoci se svého práva.

Jak jsme uvedli v první kapitole, v kybernetickém prostoru lze obvykle zjistit IP adresy cizích počítačů[74]. V našem případě DDoS útoku tak zjistíme IP adresy jednotlivých „zombie“ počítačů a za určitých podmínek se dopátráme i IP adresy počítače, který jednotlivé „zombie“ k útoku zneužil. Tedy pachatelova počítače. Pokud útok pochází ze zahraničí, jako je tomu v naprosté většině případů, je ke zjištění, kdo daný počítač použil, obvykle potřeba součinnosti cizího státu. Na jednu stranu by sice bylo možné založit individuální odpovědnost podle domácí právní úpravy na základě doktríny *effects principle*. Na straně druhé bez pomoci zahraničního státu, z jehož území útok pochází, se pachatele nikdy nepodaří vypátrat. Primárního významu tak nabývají mezistátní (právní) vztahy.

Zodpovězme si nejprve následující otázku: Kdy je samotný stát přímo zodpovědný za určitý kybernetický útok? Návrh článků o odpovědnosti států za mezinárodně protiprávní chování[75] uvádí, že odpovědnost za určité chování je podmíněna přičitatelností tohoto chování určitému státu. Talinský manuál, který zásadu přičitatelnosti aplikuje na kybernetický prostor, poté v pravidlu 6 uvádí: „A State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation.“[76] Hned v následujícím pravidle poté Manuál upřesňuje: „The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State but is an indication that the State in question is associated with the operation.“[77] To, že útoky pocházejí z území určitého státu, například Ruska nebo Číny, tedy nestačí, aby za ně tyto státy odpovídaly. Státy za ně nebudou podle manuálu přímo zodpovědné dokonce ani v případě, že by útoky pocházely přímo ze státních počítačů (například ve vojenském zařízení). Manuál správně tvrdí, že tento fakt značí pouhé spojení státu s útokem, ovšem o jaké spojení se jedná, již není jasné. Logika za tímto pojetím je jasná. Pokud opět použijeme náš příklad DDoS útoků na Svobodnou Evropu, můžeme konstatovat následující. Útočící „zombie“ počítače byly v Rusku a Číně. Pachatel ale mohl tyto počítače fakticky ovládnout z jakéhokoli státu od Afghánistánu po Zimbabwe. Opět nám tedy do hry vstupuje *architektura* kybernetického prostoru, která fakticky znemožňuje

[74] Čtenář opět promine, že se omezujeme na zjednodušené konstatování namísto technického popisu.
[75] INTERNATIONAL LAW COMMISSION. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. 2001. Dostupný online [22.3.2014]. URL: < http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf >.
[76] Stát nese mezinárodní právní odpovědnost za kybernetickou operaci jemu přičitatelnou, která zakládá porušení mezinárodních závazků.
[77] Pouhý fakt, že byla kybernetická operace spuštěna nebo jinak pocházela z vládní kybernetické struktury je nedostatečným důkazem pro přičitatelnost operace danému státu, ale je indikátorem, že je dotčený stát spojený s operací.

přičitatelnost. Talinský manuál tudíž vychází z pravidla efektivní kontroly, vysloveného opět v případu MSD Nikaragua. Kybernetický útok je přičitatelný státu, pokud měl stát nad útočníky tzv. *efektivní* kontrolu[78]. Břímě dokazování takové skutečnosti poté z podstaty věci leží na napadeném státu. Úspěch takovéhoto dokazování bude pravděpodobně pochybný.

De facto tak cizí stát, byť by třeba útok nařídil, neponese podle současného mezinárodního práva přímou odpovědnost téměř nikdy. Nezbývá než uvažovat o jakési nepřímé odpovědnosti, tedy o odpovědnosti za nečinnost či nedbalost.

Pravidlo 5 Talinského manuálu v tomto ohledu stanoví: „A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.“ Manuál zde odkazuje na precedent Slévárny v Trailu, podle nějž stát nemůže vědomě dopustit, aby na jeho teritoriu docházelo k jednání, které způsobí jinému státu škodu. V případu Korfský průliv[79] poté MSD dovodil, že stát musí varovat ostatní státy, pokud na jeho území vyvstává hrozba pro tyto státy. V neposlední řadě v případu Teherán[80] MSD určil povinnost státu neschválit výsledek protiprávního jednání a zabezpečit, aby na území státu byly dodržovány určité normy. Pokud stát dopustí, aby takovéto normy byly na jeho území porušeny, měl by nahradit škodu[81]. Vzhledem k těmto argumentům tedy můžeme potvrdit pojetí, z něhož vychází Shaw[82] s odkazem na poradní stanovisko MSD v případu Namibia[83]: “Physical control of a territory and not sovereignty or legitimacy of title, is the basis of state liability for acts affecting other states.”[84] Pokud aplikujeme tato pravidla na zmíněný DDoS útok, otevře se pro Českou republiku následující možnost obrany. Vyrozumět Rusko a Čínu, že z jejich území probíhá kybernetický útok. Zároveň je vyzvat, aby podle výše zmíněných norem tomuto útoky zamezily a veřejně ho odsoudily. Rusko a Čína by poté v ideálním případě kybernetický útok vyšetřily a pomohly při odhalení viníka, nebo doložily, že se tento viník

[78] Mezinárodní trestní tribunál pro bývalou Jugoslávii využíval širší termín obecná kontrola, Manuál ale používá termínu efektivní kontroly.
[79] Rozsudek Mezinárodního soudního dvora z 9. května 1949. The Corfu Channel Case. Dostupný online [22.3.2014]. URL: < http://www.icj-cij.org/docket/files/1/1645.pdf >
[80] Rozsudek Mezinárodního soudního dvora z 24. Června 1980. *Case* Concerning United States Diplomatic and Consular Staff in *Tehran.* Dostupný online [22.3.2014]. URL: < http://www.icj-cij.org/docket/files/64/6291.pdf >
[81] Srov. např. případ Chorzówské továrny. Rozsudek Stálého dvora mezinárodní spravedlnosti ze dne 13. září 1928. The factory at Chorozow (Germany v. Poland). Dostupný online [22.3.2014]. URL: < http://www.worldcourts.com/pcij/eng/decisions/1928.09.13_chorzow1.htm >.
[82] SHAW, Malcolm, N. *International Law*. 6th edition. Cambridge: Cambridge University Press, 2008. ISBN 978-0-521-72814-0. Str. 790.
[83] Poradní stanovisko Mezinárodního soudního dvora z 21. června 1971. Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970). Dostupný online [22.3.2014]. URL: < http://www.icj-cij.org/docket/files/53/5595.pdf >
[84] Právě fyzická kontrola nad určitým územím, a nikoli suverenita nebo legitimita důvodu, určuje státní odpovědnost za činy ovlivňující jiné státy.“

nachází na území jiného státu, proti kterému by šlo uplatnit podobná práva. Odmítnou-li tyto státy spolupracovat, budou povinné nahradit škodu.

Opět ale vyvstávají problémy. Zaprvé lze zpochybňovat, nakolik DDoS útok působí škodu. Zadruhé je sporná samotná otázka teritoriality. Jinými slovy, počítače (hardware) jsou sice na území určitých států, kybernetický prostor, tedy síť těchto počítačů, je ovšem bez hranic a omezení. Lze se bez výhrady řídit jen umístěním počítačů? Zatřetí, cizí stát může „na oko" slíbit maximální spolupráci, fakticky ale neudělá vůbec nic. Tyto otazníky opět nahlodávají vratkou jistotu mezinárodního práva.

Ostatně sporné jsou i možnosti, jak jednat v případě, že cizí stát na výzvy a upozornění prostě dlouhodobě nereaguje. V roce 1871 Adolf Lasson tvrdil, že suverénní stát se nemusí nikomu a z ničeho zodpovídat[85]. Jakkoli se od té doby rozvinuly *ius cogens* mezinárodního práva, architektura kybernetického prostoru omezuje jejich aplikovatelnost. Tím pádem se na pořad dne opět dostává starší názor, že suverenita popírá odpovědnost[86]. Do jaké míry lze tedy právo vynutit, když protistrana nespolupracuje? Není jasné, zdali má poškozený stát zůstat u retorzí a neozbrojených represálií, nebo jestli může po čase provést kybernetický protiútok nebo jinak *silově* donutit druhý stát, aby jednal a útoku ze svého území zamezil.

Jistou systematiku do problematiky vnáší Healey[87] ve svém spektru národní odpovědnosti za kybernetické útoky. Healey navrhuje ustoupit od přílišné fixace na přičitatelnost. Místo ní předestírá deset stupňů odpovědnosti státu za kybernetické útoky a následný postup poškozeného státu:

1. Útok je státem, ze kterého pochází, zakázaný. Tento stát tedy dostojí své mezinárodní odpovědnost i vnitrostátní povinnosti asistovat při zastavení útoku.
2. Útok je státem, ze kterého pochází, zakázaný, ale vnitrostátní právní úprava nebo postup daného státu není zcela adekvátní.
3. Útok je státem, ze kterého pochází, zcela ignorovaný. Stát je za něj tedy *nedbalostně* odpovědný.
4. Útok je státem, ze kterého pochází, povzbuzovaný (např. v tisku, v prohlášeních, náznaky).
5. Útok je státem, ze kterého pochází, formovaný. Útok sice řídí třetí osoby, ale stát

[85] KOSKENNIEMI, Martti. Doctrines of State Responsibility. IN Crawford, James, Pellet, Alain, Olleson, Simom. *The Law of International Responsibility*. New York, Oxford University Press: 2010. Str. 45. ISBN 978-0-19929697-2.

[86] Na místo moderního názoru, že suverenita bezpodmínečně znamená odpovědnost k ostatním členům mezinárodní komunity (podle Charty OSN) a vlastním občanům (lidská práva, R2P - „*sovereignty is not a licence to kill*".)

[87] HEALEY, Jason. The Spectrum of National Responsibility for Cyber Attacks. *Brown Journal of World Affairs*. 2011, roč. 18, č. 1.2011. p. 57 – 71.

jim poskytuje podporu či zázemí.

6. Útok je státem, ze kterého pochází, koordinovaný.
7. Útok je státem, ze kterého pochází, přímo přikázaný. Ačkoli ho nevykonávají přímo státní orgány.
8. Útok je státem, ze kterého pochází, přikázaný a částečně také vykonaný (např. armádou). Částečně znamená, že je útok vykonaný za účasti státních složek, nebo bez vědomí nejvyššího velení.
9. Útok je státem, ze kterého pochází, přikázaný a vykonaný.
10. Útok je státem, ze kterého pochází, integrovaný. To znamená uznaný a schválený.

Podle Healeyho takto lze kategorizovat jednotlivé útoky. Čím vyšší je kategorie útoku, tím jasnější je přičitatelnost a tím více se uplatní přímá odpovědnost státu a případné právo na sebeobranu. Čím nižší je kategorie, tím více se uplatní jakási nedbalostní odpovědnost, nebo bude v ideálním případě cizí stát spolupracovat v kategorii 1 či 2. Healey navrhuje neřešit jednotlivé útoky, ale spíše se orientovat na politická jednání se státem, ze kterého pocházejí. Kombinací odstrašení a motivace, tedy metodou „cukru a biče“, by se poté mělo docílit toho, že se cizí stát přesune do kategorie 1 a útok náležitě vyšetří.

Toto spektrum má ale řadu nevýhod. Zaprvé jsou hranice mezi kategoriemi neostré. Zadruhé je spektrum orientované spíše na politický *decision making* než na využití samotné právní úpravy. Dokazování a prokazování, jestli útok spadá do té či oné kategorie, by se často muselo odehrávat na bázi dohadů, vyvratitelných domněnek a indicií. Vezměme opět DDoS útok na Rádio Svobodná Evropa. Hypoteticky (a optimisticky) ho zkusme dále rozvíjet. Rusko a Čína, z jejichž území útoky pocházejí, prohlásí, že s nimi nemají nic společného. Budou tvrdit, že nemohou zajistit několik tisíc „zombie“ počítačů, které na servery rádia útočí. Zároveň přednesou, že přístup k těmto počítačům získal počítač s IP adresou nacházející se v Jemenu. Slíbí se s útoky dále zabývat, navzdory tomu budou ale útoky pokračovat. Nakolik detailně musí Rusko a Čína podle těchto pravidel podložit své závěry? Mohou tak úspěšně zamaskovat, že útok koordinovaly nebo nařídily? A co když neudělají i přes veškerou diplomatickou snahu ČR vůbec nic? Na to již Healeyho spektrum neodpovídá.

Problematiku shrnuje pesimistický závěr, že stávající právní úprava ani její případné rozšíření healeyovským způsobem rozhodně neumožní napadenému státu rychlé řešení situace, po kterém volá Jensen: „Due to the instantaneous nature of CNAs [computer network attacks], the right to respond must accrue immediately, despite the traditional obstacles of attribution (determining the attacker’s identity), characterization (determining the attacker’s

intent), and the inviolability of neutrals."[88]

Teoreticky se tedy pro napadený stát může jevit výhodnější anonymně provést kybernetický protiútok nebo odvetný úder, nepřihlásit se k němu a zahladit po sobě stopy.

Po právní stránce se tak kybernetický prostor může stát prostorem nedokonalých právních domněnek a neefektivních konstrukcí legality a legitimity, ačkoli po praktické stránce bude probíhat konflikt utajovaných, domnělých, podvržených a poloznámých všech proti všem.

Závěr: Legální a legitimní obrana proti kybernetickým hrozbám a návrat staršího typu odpovědnosti

Na kybernetický prostor se bezesporu vztahuje řada ustanovení stávající právní úpravy či právních režimů. Harašta[89] odkazuje na současná pravidla NATO pro bezpečný kybernetický prostor: „teritorialitu, odpovědnost, spolupráci, sebeobranu, ochranu dat, řádnou péči, včasnou výstrahu, přístup k informacím, kriminalizaci a jasný mandát." Fungování těchto pravidel koncentruje v následujících větách: „Pokud byl z informačních sítí státu veden útok na stát jiný, existuje nejenom odpovědnost, ale zároveň i povinnost asistovat poškozenému při napravování a odhalování škod. Pravidlo sebeobrany, umožňující tzv. hack-back, funguje jako ultima ratio v případě kybernetického útoku."[90] Tato slova jsou ovšem spíše přáním nežli popisem reálného stavu. Soudce Easterbrook, který tvrdil, že stávající právo lze bez potíží aplikovat na jakoukoli technologii, by s tímto výrokem zajisté souhlasil. Nicméně tato práce musí opět dát za pravdu Lawrenci Lewissovi a jeho tvrzení, že architektura Internetu – jeho kód – omezuje a mění působení práva.

Vzhledem ke specifičnosti tohoto prostředí a velmi obtížné přičitatelnosti chování, je velmi složité zajistit faktickou a efektivní vymahatelnost práva a odpovědnost za jeho porušení. V tabulce v příloze 1 této práce čtenář nalezne, kterého práva se může poškozený stát dovolávat a za jakých podmínek. Zásadním faktem ale zůstává, že tyto podmínky zdaleka nemusí být a nebudou vždy naplněny. Zároveň nejsou těmito normami pokryty všechny typy kybernetických útoků. V některých případech pak postižený stát obvykle nemá žádné právní možnosti, jak se útoku bránit.

Fakticky mu tak zůstávají následující kroky. Zaprvé preventivně budovat přiměřenou kybernetickou odolnost své počítačové sítě (*cyber resilience*), případně dodržovat určitou

[88] JENSEN, Eric Talbot. op. cit. Str. 240.
[89] HARAŠTA, Jakub. op. cit. Str. 81.
[90] Ibid.

kybernetickou hygienu. Zadruhé, jak navrhuje Healey, vstoupit v jednání se státem, z jehož území útok pochází, a pokusit se ho motivovat a odstrašit do té míry, aby útoku – ať již činěnému z jeho vůle nebo bez ní – zabránil. Zatřetí, přiměřeným způsobem útoku zamezit svépomocí, například ve formě kybernetického protiútoku[91], na právo přitom příliš nehledě. Zde se ovšem navracejí totožné otázky – je tento protiútok sebeobrana nebo samostatné použití síly? Narušuje suverenitu státu, ze kterého původní útok pochází?

Vraťme se v tomto bodě k našemu modelovému příkladu. Představme si, že by Česká republika po detekování DDoS útoků postupovala výše uvedeným způsobem. Nejprve by vyzvala Čínu a Rusko, aby útokům podle vlastní jurisdikce zamezily. Tyto státy by nereagovaly, nebo by slíbily útoky prošetřit, nicméně by se nic nedělo a nežádoucí stav by pokračoval. Proto by Česká republika kybernetickým protiútokem odpojila „zombie" počítače, které na ni útočí. Pokud by DDoS útok byl trestným činem, musí být tento protiútok proporcionální v rámci institutu krajní nouze (§ 28 TZ). Záleželo by tedy mimo jiné, jestli „zombie" počítače odpojené protiútokem patří hráčům počítačových her, nebo jsou to systémy, které řídí například provoz nemocnice. Lze toto technicky zjistit? Velmi obtížně. Mimoto DDoS útok nejspíše trestným činem v ČR doposud není. Otázka legality protiútoku je tedy stejně komplikovaná, jako otázka ilegality samotného prvotního kybernetického útoku. Při nedostatku použitelné právní úpravy tak vstupuje do hry otázka ospravedlnění, tedy legitimity takovýchto protiútoků. A s ní přichází obecně značná právní nejistota. Vzhledem k architektuře kybernetického prostoru není problém vytvořit falešný prvotní útok a následně drtivě zasáhnout nevinný stát – domnělého pachatele – protiútokem.

Vzhledem k těžkopádné aplikaci mezinárodních norem na kybernetický prostor se tak fakticky vrací starší forma mezinárodní odpovědnosti států (*liability*) z doby premoderního mezinárodního práva. Místo právní odpovědnosti (*responsibility*) vůči mezinárodnímu společenství podle Charty OSN a vůči svým občanům podle práva lidských práv je stát v kyberprostoru odpovědný (*liable*) pouze a jedině druhé straně – jinému státu ve vzájemných vztazích. Čepelka a Šturma[92] uvádějí:

> "Na *porušitele* právní normy se dříve hledělo, jako kdyby projevil *nezájem* o existující právní úpravu. Proto se i *poškozená strana* mohla cítit vyvázanou z daného právního poměru a napříště pokládat sebe za oprávněnou k mimoprávnímu či volnostnímu jednání (*freedom of action*) vůči porušiteli práva. (…) Tradiční obecně platné právo nemělo totiž pravidel, jež by

[91] Do jisté míry analogická situace nastala, když byl v Somálsku po útocích z 11/9 2011 odpojen Internet, neboť existovalo nebezpečí, že ho používá Al Kaida. US shuts down Somalia Internet. BBC News. London. 23. 11. 2001. Dostupný online [22.3.2014]. URL: < http://news.bbc.co.uk/2/hi/africa/1672220.stm >

[92] ČEPELKA, Čestmír, ŠTURMA, Pavel. *Mezinárodní právo veřejné*. 2. vydání. Praha: CH Beck, 2008. ISBN 978-80-7179-728-9. Str. 574 – 575.

ukládala státům povinnost odčinit újmu způsobenou deliktem.“

Jelikož v kybernetickém právu se takováto náhrada újmy fakticky také neuplatní, bohužel tedy záleží pouze na (kybernetické) síle a faktické schopnosti státu vynutit si respekt vůči sobě sama ve vztahu k ostatním státům[93].

Otázkou zůstává, zdali tento stav přetrvá nebo státy své vzájemné vztahy v kyberprostoru více zregulují tak, aby zamezily jeho zneužívání. Vyvstane mezi státy a uživateli Internetu (či šířeji kyberprostoru) nová společenská smlouva tak, jak o tom píše Horowitz a přestane hobbesovská kybernetická anarchie? Neomezí ale tato regulace příliš „leviathansky“ svobodu jednotlivce v zájmu posílení státu? A co je podmínkou toho, aby státy takovouto regulaci přijaly? Odborná veřejnost diskutuje o tom, zdali si společnost všechna nebezpeční této kybernetické anarchie neuvědomí příliš pozdě. Tedy až poté, co přijde *kybernetický Pearl Harbour*, *kybernetická Hirošima* nebo nastane jiný *Cybergeddon*.

[93] Kyberprostor tedy přináší návrat staršího typu bilaterální, vertikální odpovědnosti vůči druhému státy (*liability*), který zatlačuje novější typ komunitární, horizontální odpovědnosti (*responsibility*) vůči lidu a mezinárodnímu společností. Autor této práce připravuje samostatnou podrobnou analýzu této problematiky, která bude dostupná v létě tohoto roku pod Bruner, Tomáš. States in Cyber-Space: Perspectives of Responsibility beyond Attribution. ECPR Conference Paper. Léto 2014.

Literatura a zdroje:

Primární prameny:

CCDCOE, SCHMITT, Michael N. (ed.) *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York:. Cambridge University Press, 2013.

INTERNATIONAL LAW COMMISSION. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. 2001. Dostupný online [22.3.2014]. URL: < http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf >.

Organizace spojených národů. Charta OSN. 1945. Dostupný online [22.3.2014]. URL: < http://www.osn.cz/dokumenty-osn/soubory/charta-organizace-spojenych-narodu-a-statut-mezinarodniho-soudniho-dvora.pdf >.

Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. Listopadu 2001. Dostupný online [22.3.2014]. URL: < http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm >

Zák. č. 40/2009 Sb., trestní zákoník, v platném znění, ze dne 8. ledna 2009, přijatý Parlamentem České republiky.

Judikatura:

Rozsudek Mezinárodního soudního dvora z 9. května 1949. The Corfu Channel Case. Dostupný online [22.3.2014]. URL: < http://www.icj-cij.org/docket/files/1/1645.pdf >

Rozsudek Mezinárodního soudního dvora ze dne 27. června 1986.Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America). Dostupný online [22.3.2014]. URL: < http://www.icj-cij.org/docket/files/70/6503.pdf >.

Rozsudek Stálého dvora mezinárodní spravedlnosti ze dne 13. září 1928. The factory at Chorozow (Germany v. Poland). Dostupný online [22.3.2014]. URL: < http://www.worldcourts.com/pcij/eng/decisions/1928.09.13_chorzow1.htm >.

Rozsudek Mezinárodního soudního dvora z 24. Června 1980. *Case* Concerning United States Diplomatic and Consular Staff in *Tehran.* Dostupný online [22.3.2014]. URL: < http://www.icj-cij.org/docket/files/64/6291.pdf >

Poradní stanovisko Mezinárodního soudního dvora z 21. června 1971. Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970). Dostupný online [22.3.2014]. URL: < http://www.icj-cij.org/docket/files/53/5595.pdf >

Trail Smelter Case (United States v. Canada). Dostupný online [22.3.2014]. URL: < http://legal.un.org/riaa/cases/vol_III/1905-1982.pdf >

Vybrané dokumenty komunitárního práva:

Rozhodnutí Rady 92/242/EHS ze dne 31. 3. 1992 o bezpečnosti informačních systémů;

Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům;

Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů – Boj proti spamu a špionážnímu (spyware) a škodlivému softwaru (malicious software) ze dne 15. 11. 2006;

Sdělení Komise Evropskému Parlamentu, Radě a Evropskému výboru regionů k obecné politice v boji proti počítačové kriminalitě ze dne 22. 5. 2007;

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.

Zpravodajské články:

Digital Fears Emerge After Data Siege in Estonia. The New York Times. Dostupný online [22.3.2014]. URL: < http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 >

Kybernetické útoky dnes pokračovaly. Terčem byly servery českých bank. Technet. Idnes.cz. Dostupný online [22.3.2014]. URL: < http://technet.idnes.cz/vypadek-serveru-bank-0r8-/sw_internet.aspx?c=A130306_094423_sw_internet_jw >.

Rádio Svobodná Evropa se stalo terčem hackerů. Deník. 18/11/2013. Dostupný online [22.3.2014]. URL: < http://www.denik.cz/z_domova/radio-svobodna-evropa-se-stalo-tercem-utoku-hackeru-20131118.html >

US-funded Radio Free Europe hit by cyberattack. The Huffington Post. 19/11/2013. Dostupný online [22.3.2014]. URL: < http://www.huffingtonpost.com/huff-wires/20131119/eu-czech-radio-free-europe/?utm_hp_ref=travel&ir=travel >

US shuts down Somalia Internet. BBC News. London. 23. 11. 2001. Dostupný online [22.3.2014]. URL: < http://news.bbc.co.uk/2/hi/africa/1672220.stm >

Weby českých bank ochromil DDoS útok. NBÚ žádá od postižených data. Lupa.cz. Dostupný online [22.3.2014]. URL: < http://www.lupa.cz/clanky/web-ceske-sporitelny-neni-dostupny-vcetne-online-sluzeb-servis24/

Sekundární prameny:

APT1 Exposing One of China's Espionage Units. Mandiant. Dostupný online [22.3.2014]. URL: < http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf >

BAKER, Stewart A. DUNLAP, Charles J. What is the role of lawyers in cyber warfare? *ABA*

Journal. 2012, roč. 98, č. 5.

BRONK, Christopher. TIKK-RINGAS, Eneken. The Cyber Attack on Saudi Aramco. *Survival. Global Politics and Strategy*. 2013, roč. 55, č. 2.

BUCHAN, Russel. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict & Security Law*. 2012, roč. 17, č. 2.

COLLINS, Sean. McCombie, Stephen. Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*. 2012, roč. 7, č. 1. Dostupný online [22.3.2014]. URL: < http://www.tandfonline.com/loi/rpic20 >

Cyber Security and International Law. London: Chantam House. Dostupný online [22.3.2014]. URL: < http://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf >

ČEPELKA, Čestmír, ŠTURMA, Pavel. *Mezinárodní právo veřejné*. 2. vydání. Praha: CH Beck, 2008. ISBN 978-80-7179-728-9. Str. 574 – 575.

DAVID G. Post, Against "Against Cyberanarchy". *Berkeley Technical Law Journal*. 2002, roč. 17, č. 1365. 2002.

DELUCA, Christopher D. The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors. *Pace International Law Review Online Companion*. 2013, roč. 3, č. 9. 2013. Str. 278 – 315.

FARWELL, James P. ROHOZINSKI, Rafal. The New Reality of Cyber War. *Survival: Global Politics and Strategy*. 2012, roč. 54, č. 4. Dostupný online [22.3.2014]. URL: < http://www.tandfonline.com/loi/tsur20 >

FARWELL, James. P., ROHOZINSKI, Rafal. Stuxnet and the Future of Cyber War. *Survival: Global Politics and Strategy*. 2011, roč. 53, č. 1. Dostupný online [22.3.2014]. URL: < http://dx.doi.org/10.1080/00396338.2011.555586 >

GERVAIS, Michael. Cyber Attacks and the Laws of War. *Berkeley Journal of International Law*. 2012, roč. 30, č. 2, 2012. Str. 527 – 579.

GŘIVNA, Tomáš. POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.

GŘIVNA, Tomáš. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. *Acta Universitatis Caroline-Iuridica*. 2008, č. 4.

GŘIVNA, Tomáš. § 230 Neoprávněný přístup k počítačovému systému a nosiči informací. IN Šámal a kol. *Trestní zákoník II: Zvláštní část (§ 140 – 421)*. 2. vydání. Praha: C. H. Beck, 2012. ISBN 978-80-7400-428-5.

HARAŠTA, Jakub. Právní aspekty kybernetické bezpečnosti ČR – Hrozby a nástroje. *Revue pro právo a technologie*. 2013, roč. 4, č. 8.

HATHAWAY, Oona A. (et al). *The Law of Cyber-Attack. California Law Review*. 2012, roč. 100, č. 817. 2012. Str. 817- 885.

HEALEY, Jason. The Spectrum of National Responsibility for Cyber Attacks. *Brown Journal of World Affairs*. 2011, roč. 18, č. 1. Str. 57 – 71.

HOISINGTON, Mathew. Cyberwarfare and the Use of Force Giving Rise to the Right of Selfdefense. *Boston Colledge International and Comparative Law Review*. 2009, roč. 32, č. 2. Str. 439 – 454.

HOROWITZ, Steven J. As Boundaries Fade: The Social Contract In Cyberspace. Temple University Libraries. 2006. Dostupný online: [22.3.2014]. URL: < http://digital.library.temple.edu/cdm/ref/collection/p15037coll12/id/1617 >

JENSEN, Eric Talbot. Computer Attacks on National Infrastructure: A Use of Force Invoking the Right of Self-Defense. *Stanford Journal of International Law*. 2002, roč. 28.

JOYER, Christopher C. *International Law in the 21st Century: Rules for Global Governance*. London: Rowman and Littlefield, 2005. ISBN 0742500098.

KOSKENNIEMI, Martti. Doctrines of State Responsibility. IN Crawford, James, Pellet, Alain, Olleson, Simom. *The Law of International Responsibility*. New York, Oxford University Press: 2010. ISBN 978-0-19929697-2.

LEWIS, James A. Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs*. 2010, roč. 16, č. 2.

LESSIG, Lawrence. The Law of the Horse: What Cyberlaw Might Teach. Harward Law Review. 1999. Dostupný online: [22.3.2014]. URL: < http://cyber.law.harvard.edu/works/lessig/LNC_Q_D2.PDF >

LIFF Adam P. The Proliferation of Cyberwarfare Capabilites and Interstate War, Redux: Liff Responds to Junio. *Journal of Strategic Studies*. 2013, roč. 36, č. 1. Dostupný online [22.3.2014]. URL: < http://dx.doi.org/10.1080/01402390.2012.733312 >.

LIFLAND, Amy. Cyberwar. The Future Conflict. *Harward International Review*. Jaro 2012.

MATEJKA, Ján. *Internet jako objekt práva*. Praha: CZ.NIC, 2013. ISBN 978-80-904248-7-6.

MCGAVRAN, Wolfgang. Intended Consequences: Regulating Cyber Attacks. *Tulane Journal of Technology and Intellectual Property*. 2009. Str. 259 – 272. Dostupný online [22.3.2014]. URL: < https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=12+Tul.+J.+Tech.+%26+Intell.+Prop.+259&srctype=smi&srcid=3B15&key=0f2fef5a9d4661701cc02d5b5bc5be35>

REMUS, Titiriga. Cyber-attacks and International law of armed conflicts; a “jus ad bellum” perspective. *Journal of International Commercial Law and Technology*. 2013, roč. 8, č. 3.

SCHAAP, Maroj Arie J. Cyber Warfare operations: Development and use under International Law. *Air Force Law Review*. 2009, roč. 69.

SHACKELFORD, Scott J. From Nuclear War to Net War: Analogizing Cyber Attacks in Intemational Law . *Berkeley Journal of International Law*. 2009, roč. 27, č. 1. Str. 193 – 251.

SHAW, Malcolm, N. *International Law*. 6. vydání. Cambridge: Cambridge University Press, 2008. ISBN 978-0-521-72814-0

SCHMITT, Michael. N. Computer Network Attack: The Normative Software. IN *Yearbook of International Humanitarian Law*. Roč. 4. Haag: TMC Asser Press, 2001.

SCHMITT, Michael N. International Law in Cyberspace: The Koch Speech and Tallinn Manual Juxtaposed. *Harward International Law Journal*. 2012, roč. 54. Dostupný online: [22.3.2014]. URL: < http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf >

Significant Cyber Incidents since 2006. Centre for Strategic and International Studies. Dostupný online [22.3.2014]. URL: < https://csis.org/files/publication/120504_Significant_Cyber_Incidents_Since_2006.pdf >

SOKOL, Tomáš. SMEJKAL, Vladimír. Postih počítačové kriminality podle nového trestního zákoníku. *Právní rádce*. 23.7.2009. Dostupný online [22.3.2014]. URL: < http://pravniradce.ihned.cz/c1-37865090-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona >.

STONE, John. Cyberwar will take place! Journal of Strategic Studies. 2013, roč. 36, č. 1. Dostupný online [22.3.2014]. URL: < http://www.tandfonline.com/loi/fjss20 >.

Strategie pro oblast kybernetické bezpečnosti na období 2012 – 2015. Česká republika. Dostupný online [22.3.2014]. URL: < www.govcert.cz/download/nodeid-727 / >

THE JOINT CHIEFS OF STAFF, JOINT PUB. NO. 3-13, JOINT DOCTRINE FOR INFORMATION. OPERATIONS 1-9 (Oct. 9, 1998), Dostupný online [22.3.2014]. URL: < http://www.dtic.il/dotrine/jel/new-pubs/p3_13.pdf >

VOLEVECKÝ, Petr. Kybernetické hrozby a jejich trestněprávní kvalifikace. *Trestní právo*. 2011, roč. 15, č. 1. Str. 11 – 18.

VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo*. 2010, roč. 14, č. 7-8. Str. 26 – 38.

VOLEVECKÝ, P. Kybernetická trestná činnost v mezinárodních dokumentech a v dokumentech ES/EU. *Trestní právo*. 2009, roč. 14, č. 7-8, 2009.

WAXMAN, Mathew C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). *The Yale Journal of International Law*. 2011, roč. 36, č. 2. Str. 421- 458.