Tomáš Bruner

O MOŽNOSTECH PRÁVNÍ OCHRANY PŘED KYBERNETICKÝM ÚTOKEM ZE ZAHRANIČÍ PODLE MEZINÁRODNÍHO PRÁVA VEŘEJNÉHO

Abstrakt: *Příspěvek řeší výzkumnou otázku, jak má stát využít mezinárodního práva veřejného, když chce čelit kybernetickým útokům ze zahraničí. Jako modelový příklad používá DDoS útoky uskutečněné v minulosti na cíle v České republice. Nejdříve se zabývá kvalifikací kybernetického útoku jako mezinárodně protiprávního chování. Zkoumá možný objektivní prvek (porušení práva) takovéhoto chování a ověřuje, za jakých podmínek představuje kybernetický útok použití síly zakázané Chartou OSN a kdy je narušením suverenity státu. Následně se zaměřuje na subjektivní prvek protiprávního chování, tzn. na přičitatelnost kybernetického útoku státu. Ve třetí části se zabývá častými situacemi, kdy není zcela prokazatelně přítomen subjektivní prvek (přičitatelnost) kybernetického útoku jako mezinárodně protiprávního chování. V této souvislosti uvažuje o odpovědnosti státu za útoky pocházející z jeho území a o dalších možných alternativách.*

Klíčová slova: *mezinárodní právo veřejné, kybernetický útok, mezinárodně protiprávní chování, použití síly, narušení suverenity, přičitatelnost, DDoS*

ÚVODEM

V posledních letech vzrostl počet kybernetických útoků natolik, že podnítil diskuse o kybernetické válce.[1] Útoky přitom zasahují i cíle v České republice. Příkladem může být rozsáhlý útok typu DDoS z února a března 2013, který mj. vyřadil z provozu platební terminály českých bank, nebo obdobný DDoS útok z října téhož roku směřovaný proti serveru Rádia Svobodná Evropa. Následující příspěvek se zabývá otázkou, jakých norem mezinárodního práva veřejného využít pro ochranu před kybernetickými útoky a co brání efektivní aplikaci těchto norem. Po praktické stránce tedy příspěvek zkoumá, jakého práva se může dovolat napadený stát, nebo stát, pod jehož jurisdikci spadá cíl útoku.

Po stručném vymezení terminologie příspěvek nejprve zdůvodňuje, proč danou problematiku řeší právě na úrovni mezinárodního práva veřejného. Následně klasifikuje kybernetický útok jako mezinárodně protiprávní chování. Zaměřuje se na problémy, které tento postup přináší, a jejich možná řešení. Jako prototyp kybernetického útoku příspěvek používá útok typu DDoS, ačkoli odkazuje i na jiné druhy kybernetických útoků.[2]

---

[1] Záměrně necháváme stranou diskusi, 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. Blíže např. FARWELL, James P. – ROHOZINSKI, Rafal. The New Reality of Cyber War. *Survival: Global Politics and Strategy*. 2012, roč. 54, č. 4. Dostupné z: <http://www.tandfonline.com/loi/tsur20>, [2014-03-22]. STONE, John. Cyberwar will take place! *Journal of Strategic Studies*. 2013, roč. 36, č. 1. Dostupné z: <http://www.tandfonline.com/loi/fjss20>, [2014-03-22].

[2] Tam, kde lze zobecnit závěry úvah ohledně DDoS i pro jiné útoky, příspěvek hovoří o kybernetických útocích obecně.

1. K TERMINOLOGII A ZAMĚŘENÍ PŘÍSPĚVKU NA MEZINÁRODNÍ PRÁVO VEŘEJNÉ

Klíčový pojem tohoto příspěvku, kybernetický útok, nemá definici právní, ani univerzálně přijímanou definici obecnou. Americké Oddělení obrany (*Department of Defense*) kybernetický útok popisuje prostřednictvím jeho cílů jako operaci 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.[3] Označení takovýchto „bezpečnostních incidentů" za útoky pak může být vnímáno jako nepřesné, neboť mezinárodní právo veřejné spojuje útok s ozbrojeným konfliktem.[4] Přesto se termín kybernetický útok obvykle používá pro napadení informačních systémů, případně pro jejich zneužití za výše uvedeným účelem. Vlastní cíl útoku může ležet mimo informační systém, avšak zasažením systému dojde minimálně k ovlivnění cíle. Kybernetické útoky využívají provázanost informačních systémů, které tvoří síť telekomunikací, v níž spolu jednotlivé počítače a další součásti výpočetní techniky kooperují, směňují data a umožňují spojení mezi jejich uživateli. Tato síť technických zařízení a telekomunikací, včetně probíhající interakce, komunikace a její obsahové složky, bývá označována jako kybernetický prostor.[5]

Mezi kybernetické útoky patří útok typu *Distributed Denial of Service* (DDoS). Ten má vyřadit napadený informační systém z provozu nebo snížit jeho výkonnost. Útok spočívá v záměrném přetížení napadeného informačního systému, konkrétně jeho části – serveru, pomocí opakujících se požadavků.[6] Pachatel se napojí na velké množství různých počítačů, které se slangově 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.*"[7]

V únoru a březnu 2013 směřovaly takovéto DDoS útoky na servery českých bank, ale také na zpravodajské webové portály. Útok zaznamenaly například Česká spořitelna, Fio Banka, ČSOB, Raiffeisen Bank, ale také Burza cenných papírů v Praze.[8] V listopadu poté zasáhl čtyřdenní útok server Rádia Svobodná Evropa. Ačkoli nepřerušil vysílání, výrazně zpomalil nahrávání nových zpráv, fotek a videí na webové stránky rádia. Osmdesát procent útočících „*zombie*" počítačů pocházelo z území Číny a zbylé množství z Ruska.[9]

---

3 The Joint Chiefs of Staff, joint pub. No. 3–13, Joint Doctrine for Information. Operations 1–9 (Oct. 9, 1998). Dostupné z: <http://www.dtic.il/dotrine/jel/new-pubs/p3_13.pdf>, [2014-03-22].

4 HARAŠTA, Jakub. Právní aspekty kybernetické bezpečnosti ČR – Hrozby a nástroje. *Revue pro právo a technologie*. 2013, roč. 4, č. 8, s. 76.

5 SCHAAP, Maroj Arie J. Cyber Warfare operations: Development and use under International Law. *Air Force Law Review*. 2009, roč. 69, s. 125–126.

6 VOLEVECKÝ, Petr. Kybernetické hrozby a jejich trestněprávní kvalifikace. *Trestní právo*. 2011, roč. 15, č. 1, s. 12–13.

7 Ibidem, s. 13.

8 Kybernetické útoky dnes pokračovaly. Terčem byly servery českých bank. In: *Technet. Idnes.cz* [online]. 6. 3. 2013. Dostupné z: <http://technet.idnes.cz/vypadek-serveru-bank-0r8-/sw_internet.aspx?c=A130306_094423_sw_internet_jw>, [2014-03-22]. Weby českých bank ochromil DDoS útok. NBÚ žádá od postižených data. *Lupa.cz* [online]. 6. 3. 2013. Dostupný z: <http://www.lupa.cz/clanky/web-ceske-sporitelny-neni-dostupny-vcetne-online-sluzeb-servis24/>, [2014-03-22].

9 Rádio Svobodná Evropa se stalo terčem hackerů. *Deník* [online]. 18. 11. 2013. Dostupné z: <http://www.denik.cz/z_domova/radio-svobodna-evropa-se-stalo-tercem-utoku-hackeru-20131118.html>, [2014-03-22].

Většina kybernetických útoků přesahuje hranice státu. DDoS útok je trestným činem podle českého práva, konkrétně dle § 230 z. č. 40/2009 Sb., trestní zákoník,[10] ačkoli lze takovéto podřazení do určité míry problematizovat.[11] Nicméně pachatel se s největší pravděpodobností nachází v zahraničí. K řešení situace[12] tak bude třeba součinnosti cizího státu.[13] U řady kybernetických útoků se navíc spekuluje o tom, zdali nejsou nařízené či podporované přímo cizími státy. Právě z tohoto důvodu je nutné zabývat se mezinárodněprávní úpravou.

Jedinou mezinárodní smlouvou, která částečně upravuje 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, tedy zajistit, *„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"*. Budapešťská úmluva ovšem vyžaduje implementaci a není přímo aplikovatelná. V daném případě DDoS útoků pocházelo největší množství útočících počítačů z území Ruska a Číny – tyto státy k Budapešťské úmluvě nepřistoupily, tudíž nelze tohoto smluvního dokumentu využít.[14] Příspěvek se proto zabývá mezinárodním právem na jeho nejobecnější úrovni.

Charakter mezinárodního práva veřejného předurčuje klíčovou, téměř výhradní roli státům. Soukromí aktéři – v konkrétním případě DDoS útoku na ČR poškozené banky a rozhlasová stanice – postrádají dostatečnou mezinárodněprávní subjektivitu, aby se

US-funded Radio Free Europe hit by cyberattack. *The Huffington Post* [online]. 19. 11. 2013. Dostupné z: <http://www.huffingtonpost.com/huff-wires/20131119/eu-czech-radio-free-europe/?utm_hp_ref=travel&ir=travel>, [2014-03-22].

[10] Blíže např. 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, s. 2311.

[11] Volenecký (Kybernetické hrozby a jejich trestněprávní kvalifikace, s. 16–17) zdůrazňuje, že kvalifikace DDoS útoku jako trestného činu je v českém právu problematická. Pachatel totiž nezískává přístup k napadenému počítačovému systému nebo nosiči informací v ČR podle § 230, odst. 1 TZ. Jednotlivé *„zombie"* počítače, k nimž získal přístup, se nacházejí v zahraničí (v rozebíraném případě DDoS v Rusku a Číně). Zároveň je sporné, nakolik pachatel *„data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými"* (§ 230, odst. 2, písm. b) TZ). Pachatel pouze *zpomalil nahrávání* dat na server – k jejich úplnému potlačení nedošlo. Jednání by tedy bylo nutné posuzovat jako pokus a vycházet z argumentace, že škodní následek nastal v ČR dle § 4, odst. 2 TZ. Intenzivnější DDoS útoky by bylo dle skutkových okolností a následků možné kvalifikovat také jako poškození cizí věci, teroristický útok (možnost zásahu informačního systému je zde výslovně uvedena) nebo sabotáž. Dále k tématu vnitrostátní právní úpravy např. VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo*. 2010, roč. 14, č. 7–8, s. 26–38.

[12] Autor práce záměrně neuvádí *„k odhalení pachatele"*, které je mnohdy fakticky nemožné.

[13] K možnostem bezvýhradně aplikovat personální jurisdikci poškozeného státu pomocí doktríny tzv. *effects principle* blíže např. SHACKELFORD, Scott J. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. *Berkeley Journal of International Law*. 2009, roč. 27, č. 1, s. 212–216. Přesto by však bylo nutné zajistit součinnost státu, na jehož území se pachatel nachází. Někteří autoři rozvíjejí i možnost mezinárodněprávní odpovědnosti fyzických osob za nepřátelské akty proti cizím státům. Např. GARCIA MORA, Manuel R. *International Responsibility for Hostile Acts of Private Persons Against Foreign States*. The Hague, 1962.

[14] Pokud by ovšem v budoucnu měl vzniknout mezinárodněprávní režim upravující kybernetický prostor, bude mít tato dohoda zajisté význam. V obdobné souvislosti lze vzpomenout i některé dokumenty EU, které harmonizují právní úpravu kyberprostoru a faktické postupy států, blíže VOLEVECKÝ, Petr. Kybernetická trestná činnost v mezinárodních dokumentech a v dokumentech ES/EU. *Trestní právo*. 2009, roč. 14, č. 7–8.

mohly domáhat nápravy. Role státu je zde tudíž zásadní, a to jak ve funkci zajišťovatele bezpečnosti a ochránce práv soukromých subjektů ve své jurisdikci (např. formou diplomatické ochrany), tak ve funkci toho, kdo případně odpovídá ostatním státům za porušení práva, jak bude uvedeno dále.[15]

Pachateli kybernetických útoků jsou v mnoha případech nestátní aktéři. O jejich činnosti stát, v jehož jurisdikci se nacházejí, nemusí vědět, protože je prakticky nemožné kontrolovat tisíce počítačů tvořících jeho kybernetickou infrastrukturu. Přesto je aktivita a součinnost tohoto státu s napadeným státem klíčová a tento příspěvek se zaměřuje právě na to, jak ji právně zajistit. Také z tohoto důvodu se příspěvek zabývá problematikou z veřejnoprávního pohledu.

2. KYBERNETICKÝ ÚTOK JAKO MEZINÁRODNĚ PROTIPRÁVNÍ CHOVÁNÍ – POUŽITÍ SÍLY A NARUŠENÍ SUVERENITY

Pokud by byl kybernetický útok kvalifikovaný jako mezinárodně protiprávní chování, měl by poškozený stát (stát, v jehož jurisdikci se nacházejí cíle útoku) právo dovolávat se toho, aby kybernetický útok okamžitě přestal. Zároveň by mohl požadovat restituci, kompenzaci nebo případnou satisfakci. K tomu, aby mohl být kybernetický útok označen za mezinárodně protiprávní chování, je nutné splnit následující podmínky.[16] Zaprvé, musí dojít k porušení mezinárodního práva,[17] které představuje objektivní prvek mezinárodně protiprávního chování. Zadruhé, porušení musí být podle mezinárodního práva přičitatelné danému státu, což představuje prvek subjektivní. Jsou-li tyto podmínky naplněny, zakládá mezinárodně protiprávní chování odpovědnost státu, který se ho dopustil.

Následující podkapitola 2.1 řeší objektivní prvek. Zkoumá, kdy kybernetický útok porušuje mezinárodní právo. Jako normy mezinárodního práva, které mohou být kybernetickým útokem porušeny, identifikuje zákaz použití síly a povinnost neintervenovat ve věcech (nenarušovat suverenitu) cizího státu. Podkapitola 2.2 se pak zabývá subjektivním prvkem – přičitatelností daného chování státu.

2.1 Objektivní prvek (identifikace normy porušené útokem)

2.1.1 Porušená norma: zákaz použití síly

Zákaz použití síly je zakotven v obyčejovém právu stejně jako v čl. 2, odst. 4 Charty OSN. Doposud nejvýznamnější výstup doktríny v této oblasti, Tallinnský manuál o aplikovatelnosti mezinárodní práva na kybernetické válčení,[18] ve svém pravidlu 10 s odkazem na citovaný článek Charty OSN a případ Mezinárodního soudního dvora

[15] Blíže např. LEWIS, James, A. Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs*. 2010, roč. 16, č. 2, s. 55–65.

[16] INTERNATIONAL LAW COMMISSION. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. The UN, 2001. Dostupné z: <http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf>, [2014-03-22].

[17] „Breach of an international *obligation* of a State".

[18] CCDCOE, SCHMITT, Michael N. (ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press, 2013. *Warfare* lze přeložit také jako vedení boje.

Nikaragua[19] stanoví: „*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.*“[20] V následujícím jedenáctém pravidle Tallinnský manuál definuje, kdy je kybernetický útok použitím síly: „*Kybernetická operace představuje použití síly, když jsou její rozsah a účinky srovnatelné s nekybernetickou operací dosahující úrovně použití síly.*“

Manuál sice určitý software, například počítačové viry, vnímá jako zbraň, čímž dává základ pro aplikaci článku 51 Charty OSN o obraně proti ozbrojenému útoku, ovšem samotnou otázku použití síly řeší nejasnou analogií s konvenčním (*non-cyber*) použitím síly. Pro stanovení, zdali je určité jednání v kyberprostoru použitím síly, je nutné posoudit rozsah takového jednání a jeho důsledky („*scale and effects*“). Tudíž jednání, které má zničit nebo poškodit objekt nebo zabít člověka, je podle Tallinnského manuálu bezesporu použití síly.

Většina výstupů doktríny se víceméně doplňuje se závěry Tallinnského manuálu. Řada autorů[21] při klasifikaci kybernetického útoku jako použití síly používá tzv. Schmittova kritéria,[22] podle nichž lze některé útoky klasifikovat jako použití síly, jiné tohoto prahu nedosahují a jsou potom spíše ekonomickým a politickým donucením. Schmitt jako tato kritéria určil závažnost (*severity*), bezprostřednost (*immediacy*), přímost (*directness*), míru narušení či agresivitu (*invasiveness*) a měřitelnost následků (*measurability*) kybernetického útoku. Samotná kritéria ale v tomto případě mohou být předmětem výkladu a rozdílného vnímání. Hranice mezi útokem, který představuje použití síly, a útokem, který tato kritéria nenaplňuje, není zcela jasná.

Tomuto závěru odpovídá i dosavadní faktické vnímání proběhlých kybernetických útoků mezinárodním společenstvím. 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 Tallinnu. Některé zdroje uvádějí, že útoky probíhaly na popud ruské vlády. Ministr obrany Estonska přirovnal takto masivní DDoS útok k vojenské blokádě přístavu.[23] Mezinárodní společenství ale nekvalifikovalo tento kybernetický útok jako použití síly a neuplatnil se společný článek 5 Smlouvy Severoatlantické aliance o kolektivní sebeobraně.

Podobně nebyl jako použití síly vnímán útok na íránský jaderný program virem Stuxnet. Tento kód odhalený v říjnu 2010 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

[19] Rozsudek Mezinárodního soudního dvora ze dne 27. června 1986. *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America). Dostupné z: <http://www.icj-cij.org/docket/files/70/6503.pdf>, [2014-03-22].

[20] Překlady citovaných ustanovení z anglického originálu provedl autor práce.

[21] GŘIVNA, Tomáš – POLČÁK, Radim (eds). *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 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, s. 179–189.

[22] SCHMITT, Michael N. Computer Network Attack: The Normative Software. In: *Yearbook of International Humanitarian Law*. Vol. 4. Haag: TMC Asser Press, 2001, s. 53–85.

[23] Digital Fears Emerge After Data Siege in Estonia. *The New York Times* [online]. 29. 5. 2007. Dostupné z: <http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0>, [2014-03-22].

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.[24] Jako použití síly nebyla označena ani domnělá odveta za Stuxnet – útok na počítačovou síť ropné společnosti Saudi Aramco. Při něm virus nakazil na 30 000 počítačů a snížil cenu akcií společnosti. Ačkoli samotná korporace disponuje značným kapitálem, trvalo přes týden, než se vyrovnala s následky.[25]

Přestože se v posledních dvou jmenovaných případech nejedná o DDoS útoky, lze dosažené závěry na DDoS útoky aplikovat argumentem *a maiori ad minus*. Nebyly-li jako použití síly kvalifikovány útoky, které prokazatelně způsobily škodu, neměly by tak být kvalifikovány ani útoky, u nichž škoda není jasně prokazatelná.

Nemožnost označit kybernetický útok jako použití síly kritizuje řada autorů. Jensen[26] podotýká, že rozvoj mezinárodního práva musí ještě pokročit, aby byl kybernetický útok rozeznáván jako použití síly a *ozbrojený* útok, který zakládá právo na 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. Dokud státy nezískají právo na okamžitou kybernetickou sebeobranu, včetně předstižného kybernetického úderu, tak budou tyto útoky vážně destabilizující silou. K totožnému závěru dospívá DeLuca.[27]

Podobně Hoisington[28] poznamenává, že se kybernetické útoky odehrávají do jisté míry v právním vakuu. Výklad samotného čl. 2, odst. 4 Charty OSN, která byla napsaná před vznikem Internetu, je nejasný. Tvrdí, že státy by měly rozšířit výklad daného ustanovení Charty, nebo přijmout nové (právní) prostředky, jak čelit těmto hrozbám.

Waxman[29] 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.[30] K velmi podobné úvaze vede názor, že by kyber-

[24] 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. Dostupné z: <http://www.tandfonline.com/loi/rpic20>, [2014-03-22]. FARWELL, James P. – ROHOZINSKI, Rafal. Stuxnet and the Future of Cyber War. *Survival: Global Politics and Strategy*. 2011, roč. 53, č. 1. Dostupný z: <http://dx.doi.org/10.1080/00396338.2011.555586>, [2014-03-22].

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

[26] 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, s. 207–240.

[27] 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, s. 315.

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

[29] 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, s. 458.

[30] V akademickém prostředí probíhá debata o tzv. dvojsečném státním zájmu. Státy na jednu stranu potřebují kybernetický prostor bezpečný a kontrolovaný, na druhou stranu jim vyhovuje jeho svobodný charakter, protože zde mohou podnikat těžko odhalitelné výpady proti rivalům.

netické útoky mohly být za hrozbu označeny Radou bezpečnosti OSN podle čl. 39 Charty OSN. Rada bezpečnosti může označit za hrozbu cokoli, a tudíž záleží na jejích (stálých) členech – opět více či méně hegemonických státech.[31]

McGavran[32] se opírá o článek 36 prvního Dodatkového protokolu k Ženevským úmluvám a stanoví povinnost smluvních stran zvážit, jestli nově vyvinuté druhy zbraní nejsou za určitých okolností zakázány Protokolem nebo jinou normou mezinárodního práva. Dle názoru autora tohoto příspěvku se jedná o vyjádření Martensovy klauzule, které je ovšem normou *ius in bello* (případně normou odzbrojení), nikoli *ius 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. Obecně lze poznamenat, že samotný Tallinnský manuál je restriktivní, co se týče aplikace *ius ad bellum* na kybernetický prostor, zatímco ohledně *ius in bello* dochází k řadě hmatatelných závěrů.[33] Pokud by tedy kybernetický útok probíhal za ozbrojeného konfliktu, bude podléhat normám humanitárního práva (*ius in bello*).[34]

Co se ovšem týče normy *ius contra bellum*, kybernetický útok lze jako použití síly podle čl. 2, odst. 4 Charty OSN kvalifikovat jen v malém množství případů,[35] kdy výsledek daného jednání odpovídá výsledku použití konvenční síly (ačkoli ani samotné konvenční použití síly a jeho výsledek nejsou jasně definovány). K takovéto kvalifikaci navíc prakticky ještě nikdy nedošlo.

2.1.2 Porušená norma: Povinnost neintervenovat ve věcech cizího státu

V případě, že nelze kybernetický útok označit jako použití síly a zasáhnout proti němu v sebeobraně, je možné jej vnímat jako porušení suverenity a intervenci ve věcech cizího státu.[36] Pokud by DDoS útok, tak jako doposud ve všech případech, nebyl dostatečně

---

[31] GŘIVNA, T. – POLČÁK, R. (eds). *Kyberkriminalita a právo*, s. 60.

[32] MCGAVRAN, Wolfgang. Intended Consequences: Regulating Cyber Attacks. *Tulane Journal of Technology and Intellectual Property*. 2009, s. 259–272. Dostupné z: <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>, op. cit., s. 269, [2014-03-22].

[33] 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, s. 579.

[34] Kybernetické útoky přitom při vojenských operacích v rámci tzv. informační války probíhají poměrně často. Příkladem jsou útoky z území Ruska na cíle v Gruzii v roce 2008 nebo operace Orchard. V jejím průběhu 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.

[35] Podobně např. HATHAWAY, Oona A. et al. The Law of Cyber-Attack. *California Law Review*. 2012, roč. 100, č. 4. 2012, s. 817.

[36] 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, s. 212. Srov. také výstup setkání Cyber Security and International Law. London: Chantam House [online]. 29. 5. 2012. Dostupné z: <http://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf>, [2014-03-22]. S obdobnými závěry přichází také Tallinnský manuál.

závažný, bezprostřední, přímý a agresivní jako konvenční použití síly, měl by být označen jako protiprávní intervence ve věcech cizího státu a narušení cizí státní suverenity. Zásada neintervenovat ve věcech cizího státu vyvstává jako důsledek rovnosti a nezávislosti *suverénních* států a tvoří jeden ze základních principů mezinárodního práva.[37] Její narušení přitom může mít i podobu chování, které má poškodit či ovlivnit vnitřní uspořádání cizího státu, omezit výkon jeho práv nebo mu způsobit podobné potíže.[38] Pokud nebude kybernetický útok zastaven, případně nedojde ke kompenzaci či satisfakci poškozeného státu, může se tento stát uchýlit k proporcionálním protiopatřením.

Aplikace této normy se ovšem neobejde bez (byť nevyslovené) definice státní suverenity v kyberprostoru. Suverenita bývá obvykle určena neexistencí vyšší autority, přičemž vnitřní suverenita znamená výlučnost autority suveréna na jeho území a vnější suverenita jeho nezávislost a možnost vstupovat do závazků s jinými státy. Tento koncept však prošel, a jak někteří autoři argumentují, stále prochází vývojem a výklad pojmu není přijímán jednotně.[39] Obecně přijímaný pohled vymezuje hranice suverenity právě prostřednictvím teritoria státu. Takovýto přístup bývá označován za vestfálské vnímání suverenity[40] a jeho původ spojován např. s právní zásadou *cuius regio, eius religio*.[41]

V praxi je tak dovozováno, že pokud má stát výlučnou pravomoc nad fyzickým umístěním počítačů a součástí výpočetní techniky, měl by se těšit také suverenitě v té části kybernetického prostoru, kterou tyto počítače vytvářejí. Jedná se o „teritorializaci" kyberprostoru, nebo o zásadu teritoriality v kyberprostoru. Pokud pak DDoS útok zasáhne tu část kyberprostoru, kterou utváří výpočetní technika daného státu, omezuje výlučnou autoritu tohoto státu a představuje porušení jeho suverenity.

Hardware, který vytváří kybernetickou infrastrukturu, jejíž činnost je DDoS útokem zasažena nebo ze které útok pochází, se ale často může nacházet na území více států. Uplatňovat protiopatření proti všem těmto státům přitom nemusí být efektivní. Navíc, jak uvádí Tallinnský manuál,[42] expertní skupina autorů se neshodla, jestli umístění malwaru, který nezpůsobuje fyzickou škodu, znamená porušení suverenity. Malware, který ovládá „*zombie*" počítače při DDoS útoku a nutí je zahltit cílový server oběti, fyzickou škodu bez dalšího působit nemusí.

Lze shrnout, že DDoS útok by tak sice z pohledu mezinárodního práva měl být kvalifikován spíše jako porušení suverenity a práva neintervenovat ve věcech cizího státu, nežli jako použití síly. Vždy je však nutné vzít v úvahu konkrétní rozsah a následky útoku. Ovšem i takovéto určení objektivního prvku kybernetického útoku jako mezinárodně protiprávního chování může být problematické a zpochybňované, zejména tvrzením, že části kybernetického prostoru nelze „teritorializovat" – přiřknout jednotlivým státům podle hardwaru, který se nachází v jejich jurisdikci.

---

[37] JOYER, Christopher C. *International Law in the 21st Century: Rules for Global Governance*. London: Rowman and Littlefield, 2005, s. 54.

[38] Např. VATTEL, Emmerich. *The Law of Nations*. Kniha II, kapitola I, § 18. [online]. 29. 5. 2012. Dostupné z: <http://www.constitution.org/vattel/vattel_02.htm>, [2014-03-22].

[39] Blíže např. GLANVILLE, Luke. The Myth of „Traditional" Sovereignty. *International Studies Quarterly*. 2013, roč. 57, s. 79–90. KRASNER, Stephen D. (ed.). *Problematic Sovereignty*. New York: Columbia University Press, 2001.

[40] Podrobněji ibidem.

[41] „*Čí kraj, toho náboženství*", zásada, v jejíž rozšíření vyústila třicetiletá válka a vestfálský mír. Výlučné právo suveréna rozhodovat o záležitostech (konkrétně náboženství) na jeho území.

[42] S. 26.

Aby se poškozený stát mohl dovolávat odpovědnosti cizího státu za porušení zákazu použití síly nebo narušení státní suverenity kybernetickým útokem, musí být tento útok přičitatelný státu. Jinými slovy musí být naplněn subjektivní prvek mezinárodně protiprávního chování, o němž pojednává následující podkapitola.

2.2 Subjektivní prvek (přičitatelnost útoku)

Následující podkapitola zkoumá, za jakých podmínek je kybernetický útok přičitatelný státu. U DDoS útoku lze technickou analýzou zjistit tzv. IP adresu[43] „*zombie*" počítačů, které zahlcují server, v některých případech je možné dopátrat i IP adresu počítače samotného pachatele. Tyto počítače se, jak již bylo uvedeno, obvykle nacházejí v zahraničí.

Tallinnský manuál, který zásadu přičitatelnosti aplikuje na kybernetický prostor, v pravidlu 6 uvádí, že stát nese mezinárodní právní odpovědnost za kybernetickou operaci jemu přičitatelnou, která zakládá porušení mezinárodních závazků. Hned v následujícím pravidle 7 poté Manuál upřesňuje, že 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. Samotný fakt, že DDoS útoky pocházejí z (IP adres počítačů na) území určitého státu, například Ruska nebo Číny, tedy nestačí, aby za ně tyto státy odpovídaly jako za mezinárodně protiprávní chování. Státy za ně nebudou podle manuálu přímo zodpovědné dokonce ani v případě, že by útoky pocházely přímo z vládních počítačů (například ve vojenském zařízení). Manuál tvrdí, že tento fakt značí pouhé spojení státu s útokem, pachatel totiž může využít státní počítače jako „*zombie*", aniž by o tom jejich uživatelé věděli.

Tallinnský manuál dále vychází z pravidla efektivní kontroly, vysloveného v případu *MSD Nikaragua*. Kybernetický útok je přičitatelný státu, pokud měl stát nad útočníky tzv. *efektivní* kontrolu.[44] Úspěch dokazování takovéto skutečnosti bude pravděpodobně v mnoha případech pochybný, neboť se, jak bylo uvedeno výše, podaří dopátrat např. pouze IP adresy počítačů. Označení kybernetického útoku jako mezinárodně protiprávního chování, které je přímo přičitatelné cizímu státu, tak bude v mnoha případech nemyslitelné.

3. ALTERNATIVNÍ MOŽNOSTI

Problém přičitatelnosti vnímá jako zásadní překážku v kvalifikaci mezinárodně protiprávního chování také Healey.[45] Ten navrhuje ustoupit od přílišné fixace na přičitatelnost. Jako alternativu předestírá spektrum deseti stupňů odpovědnosti státu za kybernetické útoky a zároveň navrhuje následný postup poškozeného státu:

---

[43] Jedinečný číselný kód každého počítače. Technický popis je zde uvedený v maximálně zjednodušené podobě.

[44] Mezinárodní trestní tribunál pro bývalou Jugoslávii využíval širší termín obecná kontrola, manuál ale zastává využití testu efektivní kontroly.

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

1. Útok je státem, ze kterého pochází, zakázaný. Tento stát tedy dostojí své vnitrostátní povinnosti a (na případnou výzvu poškozeného státu) asistuje při vyšetření a 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).[46]
5. Útok je státem, ze kterého pochází, formovaný. Útok sice řídí třetí osoby, ale stát jim poskytuje podporu či zázemí.[47]
6. Útok je státem, ze kterého pochází, koordinovaný.
7. Útok je státem, ze kterého pochází, přímo přikázaný. Ačkoli ho nevykonávají přímo státní orgány.[48]
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.

Healey takto jednotlivé útoky kategorizuje a tvrdí, že čím vyšší 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 by se poté cizí stát měl přesunout do kategorie 1, útok náležitě vyšetřit a zamezit jeho pokračování či opakování.

Toto spektrum má ale řadu nevýhod. Zaprvé jsou hranice mezi kategoriemi neostré. Zadruhé je spektrum orientované spíše na politické rozhodování než na právní kvalifikaci. Dokazování, jestli útok spadá do té či oné kategorie, by se často muselo odehrávat na bázi dohadů, domněnek a indicií. Státy, z jejichž území útoky pocházejí, mohou tvrdit, že s nimi nemají nic společného, a argumentovat, že fakticky nemohou zajistit několik tisíc útočících „*zombie*" počítačů, které se na jejich území nacházejí. Zároveň přednesou, že přístup k těmto počítačům získal počítač s IP adresou nacházející se ve třetím státě. Slíbí situaci řešit, navzdory tomu budou ale útoky pokračovat. Není jasné, nakolik detailně musí státy, z jejichž území útoky pocházejí, podložit své závěry. Zároveň mohou úspěšně maskovat, že útok koordinovaly nebo nařídily.

Navzdory tomu Healeyho návrh naznačuje určité možnosti, jak se vypořádat s nemožností přičitatelnosti, a to na teritoriální bázi. Podle jeho předpokladu je kybernetický útok nutné řešit se státem, z jehož území pochází. Healey už ovšem neprozrazuje, jakých

[46] Tzn. porušení povinnosti neuznat výsledky protiprávního chování. Povinnost vyslovena např. v případu MSD Teherán, jak bude uvedeno dále.
[47] Odpovědnost státu by tedy bylo nejspíše možné uplatnit při testu obecné kontroly, což platí pro body 5 a 6.
[48] Zde už je přičitatelnost jednoznačná, i podle testu efektivní kontroly.

právních norem se dovolat, aby tento stát začal jednat. Na následujících řádcích se příspěvek pokouší tyto normy obyčejového práva popsané v judikatuře a v doktríně identifikovat a rozšířit tak odpovědnost státu za hranice přímé přičitatelnosti, respektive specifikovat, jak státu přičíst nečinnost.[49]

V případu Korfský průliv[50] Mezinárodní soudní dvůr dovodil, že stát musí varovat ostatní státy, pokud na jeho území vyvstává pro tyto státy hrozba. Pokud by tedy stát věděl, že na jeho území aktuálně dochází k průnikům do informačních systémů, které mohou být zneužity proti dalším státům, má povinnost tyto další státy varovat. MSD tak dovozuje odpovědnost za nečinnost, která se vztahuje i na stát, jemuž není dané chování přímo přičitatelné. Značný problém by ale v případě DDoS útoků představovalo opět prokazování. Dokázat, že stát *a priori* věděl o kybernetickém útoku, je téměř stejně obtížné jako přičíst samotný útok tomuto státu na bázi efektivní kontroly.

Další možností je využít závěry MSD v poradním stanovisku Namibia,[51] z nichž vychází Shaw[52]: „*Právě fyzická kontrola nad určitým územím, a nikoli suverenita nebo legitimita důvodu, určuje státní odpovědnost za činy ovlivňující jiné státy.*“ Lze tedy dovodit, že faktický výkon státní moci nad určitým teritoriem, tzn. i nad hardwarem počítačů, znamená odpovědnost státu za případné protiprávní chování, které se odehraje na tomto území a ovlivní další státy. Pojmy *odpovědnost* a *protiprávní* musí být však v tomto případě do jisté míry vykládány ve světle Návrhu článků o odpovědnosti států za mezinárodně protiprávní chování,[53] kdy by pro aktivaci mezinárodní odpovědnosti musel být přítomen také subjektivní prvek protiprávního chování. Tento postup by tak znamenal návrat kruhem k problému přičitatelnosti na bázi testu efektivní kontroly nebo k podmínkám *přičitatelnosti nečinnosti* a ke klasifikaci DDoS útoků jako mezinárodně protiprávního chování.

Další možnosti nabízí analogická aplikace závěrů MSD v případu Teherán.[54] Soudní dvůr se v tomto rozsudku mimo jiné podrobněji zabýval právě odpovědností státu za neaktivitu. Stát sice není odpovědný za určité činy jednotlivců, ale bude odpovědný v případě, že neučinil všechny nezbytné kroky, aby těmto činům zabránil. Právě takováto norma by se mohla stát východiskem pro donucení státu, aby zamezil kybernetickým útokům pocházejícím z jeho území. Mezinárodní soudní dvůr dále popsal povinnost státu neschválit výsledek porušení těchto norem. V ideálním případě by tak pro stát poté, co se dozví o DDoS útoku z jeho území, vyvstala povinnost veřejně tento útok odsoudit (např. nepodporovat tak hackery v médiích) a vyvinout snahu k jeho zastavení. Pokud aplikujeme takovýto výklad na zmíněný DDoS útok na Rádio Svobodná Evropa v ČR, otevřou se následující možnosti. Zaprvé vyrozumět Rusko a Čínu, že z jejich území pro-

[49] Návrh článků o odpovědnosti státu za mezinárodně protiprávní chování také operuje s odpovědností za nečinnost (*omission*).

[50] Rozsudek Mezinárodního soudního dvora ze dne 9. května 1949. The Corfu Channel Case (United Kingdom v. People's Republic of Albania). Dostupné z: <http://www.icj-cij.org/docket/files/1/1645.pdf>, [2014-03-22].

[51] 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). Dostupné z: <http://www.icj-cij.org/docket/files/53/5595.pdf>, [2014-03-22].

[52] SHAW, Malcolm N. *International Law*. 6. vydání. Cambridge: Cambridge University Press, 2008, s. 790.

[53] Byť tento Návrh pochází z doby pozdější.

[54] Rozsudek Mezinárodního soudního dvora z 24. června 1980. *Case* Concerning United States Diplomatic and Consular Staff in *Tehran*. Dostupné z: <http://www.icj-cij.org/docket/files/64/6291.pdf>, [2014-03-22].

bíhá kybernetický útok. Zadruhé je vyzvat, aby tento útok veřejně odsoudily a podnikly kroky k jeho zastavení. Rusko a Čína by v ideálním případě útok vyšetřily a pomohly při odhalení viníka, nebo doložily, že se tento viník nachází na území jiného státu, proti kterému by byla uplatnitelná stejná práva. Odmítají-li soustavně státy, z jejichž území útok pochází, zcela spolupracovat i poté, co se o kybernetickém útoku dozvědí (např. upozorněním poškozeného státu), lze je podle tohoto výkladu obvinit z porušení mezinárodního práva nečinností a podle závažnosti útoku přistoupit k proporcionálním protiopatřením.

Takováto aplikace závěrů MSD v případu Teherán přináší také sporné body. Zaprvé není skutkově jasné, co vše musí stát učinit, aby útokům ze svého území zamezil nebo je vyšetřil, a kde jeho faktické možnosti končí v situaci, kdy očekávané opatření ani nelze zavést, např. kvůli obrovskému množství počítačů na území státu. Zadruhé, z právního hlediska došlo v případu Teherán k porušení tzv. *self-contained* režimu. Tento režim byl mezinárodním společenstvím široce uznáván, včetně ustáleného výkladu příslušných norem. DDoS útok nemusí představovat obdobně závažné porušení normy vnímané a vykládané natolik koherentně jako normy porušené v případu Teherán. Jinými slovy by bylo nutné široké přijetí výkladu, že DDoS útoky představují porušení státní suverenity, kterou lze v kyberprostoru vnímat stejně jako v prostoru fyzickém. V opačném případě nebude po právní stránce jasné, jakému porušení (porušení čeho) by vlastně měl odpovědný stát zabránit.

Zcela odlišnou variantu představuje vnímání DDoS útoků jako chování doposud nezakázaného (či lépe řečeno neupraveného) mezinárodním právem. Podle rozhodnutí v případu slévárny v Trailu[55] stát nemůže dopustit, aby na jeho teritoriu docházelo k jednání, které působí škodu jinému státu. DDoS útok by tak obrazně řečeno mohl odpovídat kouři z komína slévárny. V tomto případě by ovšem na rozdíl od případů předešlých bylo nutné prokázat, že vzniká faktická škoda.[56] Právě ta je v případě DDoS útoku často obtížně stanovitelná.

Pravidlo 5 Tallinnského manuálu rovněž vychází ze zásady teritoriality v kyberprostoru: „*Stát vědomě*[57] *nedovolí, aby byla kybernetická infrastruktura na jeho území nebo pod jeho výlučnou kontrolou použita k činům, které nepřátelsky nebo protiprávně ovlivňují jiné státy.*“ Jelikož se ale jedná pouze o výstup doktríny, bylo by nutné argumentaci opřít taktéž o výše uvedené judikáty a jejich aplikovatelnost zdůvodnit v konkrétním případě.[58] Tallinnský manuál (pravidlo 5, odstavec 5) zjevně vychází z předpokladu, že kybernetický útok porušuje suverenitu poškozeného státu. Proto stačí samotný negativní, škodlivý („*detrimental*“) efekt, aniž by musela být způsobena fyzická škoda a není nutné nahlížet na kybernetický útok jako na chování nezakázané mezinárodním právem, kde by bylo vyčíslení škody třeba.

---

[55] Trail Smelter Case (United States v. Canada). Dostupné online z: <http://legal.un.org/riaa/cases/vol_III/1905-1982.pdf>, [2014-03-22].

[56] Srov. např. případ Chorzowské továrny. Rozsudek Stálého dvora mezinárodní spravedlnosti ze dne 13. září 1928. The factory at Chorzów (Germany v. Poland). Dostupné z: <http://www.worldcourts.com/pcij/eng/decisions/1928.09.13_chorzow1.htm>, [2014-03-22].

[57] Stát o útoku musí vědět. Expertní skupina autorů Tallinnského manuálu se neshodla, zdali postačuje, aby stát o útoku měl a mohl vědět (Pravidlo 5, odst. 11).

[58] Samotný Tallinnský manuál v tomto bodě odkazuje na případ MSD Korfský průliv.

Zároveň Tallinnský manuál připouští, že se expertní skupina autorů neshodla, zdali pravidlo č. 5 platí i pro stát, z jehož území kybernetický útok nepochází, ovšem je skrz toto území (počítače na tomto území) veden. Stát, prostřednictvím jehož infrastruktury je útok veden, by ale logicky měl mít povinnost prokázat, že tento útok pochází právě z jiného státu.

Po skutkové stránce zde komplikuje situaci charakter kybernetického prostoru. Globální DDoS útok může zneužít „*zombie*" počítače na území desítek států, zároveň nemusí být jasné, kdy útok pochází přímo z dané infrastruktury a kdy je jen touto infrastrukturou směřován či veden. Stejně obtížně bude stát dopátrávat na svém území samotného pachatele. V neposlední řadě se stát, z jehož území útoky pocházejí, může uchýlit k účelovým tvrzením, slibovat či předstírat spolupráci, ačkoli fakticky neudělá nic. Vezmeme-li v úvahu dynamický charakter kybernetického prostoru, kde mohou proběhnout tisíce operací za vteřinu, nemusí být uplatňování práva výše uvedeným způsobem vůči státu (nebo vůči množství států), z jehož území útok pochází, efektivním řešením situace.

Jak bylo uvedeno výše, Jensen[59] vyžaduje, aby v případě kybernetického útoku vzniklo právo na protiútok okamžitě, a to navzdory nedostatku přičitatelnosti, neznámému záměru pachatele a nezranitelnosti neutrálních států. V současné době je kybernetický protiútok literaturou vnímán spíše jako krajní možnost,[60] při jejíž aktivaci by opět bylo nutné obezřetně zkoumat, jaká norma mezinárodního práva zakládá jeho legitimitu. Pokud by mezinárodní společenství uznalo právo poškozených států na okamžitý protiútok[61] bez ohledu na přičitatelnost nebo neutralitu, učinilo by tak krok ke zvláštní úpravě kybernetického prostoru. Shackelford[62] v tomto směru navrhuje pohlížet na kybernetický prostor jako na společné dědictví lidstva a mezinárodní prostor, podobně jako je tomu u Antarktidy, hlubokomořského dna nebo vnějšího vesmíru. Přijetím práva na protiútok by v tomto prostoru mohl každý potírat kybernetické piráty stejně jako dříve piráty mořské coby *hostes humani generis*. Státy by ovšem musely na takovouto volbu nejprve přistoupit, nehledě na skutečnost, že režimy mezinárodních prostor fungují také v některých ohledech problematicky.

ZÁVĚREM

Při vymezení zásad pro bezpečný kybernetický prostor odkazuje Harašta[63] na současná pravidla NATO: „*teritorialitu, odpovědnost, spolupráci, sebeobranu, ochranu dat, řádnou péči, včasnou výstrahu, přístup k informacím, kriminalizaci a jasný mandát.*" Teritorialita přitom zaujímá první místo. Fungování těchto pravidel koncentruje Harašta v následujících větách: „*Pokud byl z informačních sítí státu veden útok na stát jiný, existuje nejenom odpovědnost, ale zároveň i povinnost asistovat poškozenému při napra-*

59 JENSEN, E. T. Computer Attacks on National Infrastructure, s. 240.

60 HARAŠTA, J. Právní aspekty kybernetické bezpečnosti ČR – Hrozby a nástroje, s. 81.

61 Otázkou zůstává, nakolik by toto opatření bylo žádoucí a zůstalo bez nežádoucích důsledků. Mohlo by např. zahájit sérii uměle vyprovokovaných protiútoků apod.

62 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, s. 212–216.

63 HARAŠTA, J. Právní aspekty kybernetické bezpečnosti ČR – Hrozby a nástroje, s. 81.

vování a odhalování škod.“[64] Jeho závěry, především důraz na teritorialitu, poté ilustrují trend rozdělit kybernetický prostor podle státního území a takto na něj také aplikovat právo.

Tento příspěvek svou analýzou dokládá, že DDoS a obdobné útoky lze ve většině případů kvalifikovat jako porušení suverenity, která je definovatelná právě na teritoriální bázi. Přímou odpovědnost cizího státu za kybernetický útok podmiňuje přičitatelnost tohoto útoku státu na základě testu efektivní kontroly. Prokázat efektivní kontrolu státu nad kybernetickým útokem může být přitom technicky velmi komplikované. Stát, z jehož území útok pochází, však může být vinen za nečinnost. Judikatura a doktrína popisují povinnost státu varovat ostatní státy před nebezpečím z jeho území, nedopustit, aby jeho území bylo zneužito k protiprávním aktivitám a případně nahradit škodu, která vzniká činností na jeho území ostatním státům i jednáním nezakázaným mezinárodním právem. Těchto norem se může poškozený stát dovolávat vůči státu, z jehož území útok pochází. Z těchto norem je pak také možné dovodit citovanou odpovědnost a povinnost asistovat poškozenému státu při odhalování a napravování škod. V případě, že útok či útoky neustanou, může poškozený stát následně uplatnit proporcionální protiopatření.

Otázkou – a to skutkovou, nikoli právní – ovšem je, zdali tento postup představuje efektivní řešení i za situace, kdy např. DDoS útok prochází územím desítek států a nelze odhalit jeho původce. Pro takovéto situace se může zdát lepším řešením vytvoření zvláštních pravidel pro kybernetický prostor, například práva na okamžitý kybernetický protiútok,[65] případně mezinárodněprávního režimu pro kybernetický prostor.

Na obecné úrovni probíhá v současné době debata mezi „exceptionalisty“ a „neexceptionalisty“.[66] Podle prvých si výjimečný charakter kybernetického prostoru vytváří svá vlastní pravidla. Ti druzí tvrdí opak – současná pravidla reálného světa jsou plně aplikovatelná na kybernetický prostor. Na straně jedné tak Mezinárodní strategie USA pro kybernetický prostor ubezpečuje, že tento prostor plně ovládají letité zásady mezinárodního práva, jejichž fungování může být jen drobně obměněno. Na straně druhé řada teoretiků takovýto názor napadá.[67] V jiné konkrétní verzi tohoto sporu americký soudce Frank Easterbrook 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.*“[68] Jeho odpůrce Lawrence Lessig[69] se poté přiklonil k opačnému názoru, že speciální charakter kybernetického prostoru, jeho architektura, mění možnosti aplikace práva.[70]

---

64 Ibidem.

65 Podobného efektu by bylo možné dosáhnout i změnou výkladu – např. rozšířením výkladu zákazu použití síly v kyberprostoru, čímž by častěji docházelo k založení práva na sebeobranu.

66 HOROWITZ, Steven J. *As Boundaries Fade: The Social Contract In Cyberspace*. Temple University Libraries, 2006. Dostupné z: <http://digital.library.temple.edu/cdm/ref/collection/p15037coll12/id/1617>, [2014-03-22].

67 SCHMITT, Michael N. International Law in Cyberspace: The Koch Speech and Tallinn Manual Juxtaposed. *Harward International Law Journal*. 2012, roč. 54. Dostupný z: <http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf>, [2014-03-22].

68 MATEJKA, Ján. *Internet jako objekt práva*. Praha: CZ.NIC, 2013, s. 26–27.

69 LESSIG, Lawrence. The Law of the Horse: What Cyberlaw Might Teach. *Harvard Law Review*. 1999. Dostupné z: <http://cyber.law.harvard.edu/works/lessig/LNC_Q_D2.PDF>, [2014-03-22].

70 Zjednodušeně řečeno – právo reguluje Internet, ale Internet také reguluje právo (jeho aplikovatelnost).

Výsledkem „neexceptionalistického“ přístupu je zaprvé klasifikace DDoS útoku jako porušení suverenity, zadruhé stanovení pravidel přičitatelnosti, a zatřetí určení možnosti poškozeného státu požadovat řešení po státu, z jehož území útok pochází. Jak výše naznačuje Harašta, zásada teritoriality v kyberprostoru hraje v „neexceptionalistickém“ přístupu klíčovou roli. Díky ní může stát využívat ochrany mezinárodního práva i před DDoS útoky.

Musíme však vzít v úvahu také argument „exceptionalistů“. Samotnou zásadu teritoriality může narušit další rozvoj technologie a rostoucí globalizace kybernetického prostoru smazávající hranice území. DDoS útok může být směrován prostřednictvím počítačů na území desítek států, přičemž nebude zjistitelné, odkud skutečně pochází. Efektivita uplatňování mezinárodního práva vůči všem státům, z jejichž území by takovýto útok pocházel, bude pravděpodobně poměrně nízká. Charakter kyberprostoru tedy může podstatným způsobem ovlivnit působení práva, jak tvrdí Lessig. Právě na frekvenci takovýchto případů závisí „exceptionalistická“ potřeba přijetí nových norem mezinárodního práva pro kybernetický prostor.

Původní verze tohoto příspěvku vznikla v rámci studentské vědecké odborné činnosti na Právnické fakultě.

Mgr. Tomáš Bruner
Právnická fakulta Univerzity Karlovy v Praze
Fakulta sociálních věd Univerzity Karlovy v Praze

Tomáš Bruner

On the Possibility of Legal Protection Against Cyber Attacks from abroad under Public International Law

Abstract: *The article poses a research question how a state can use public international law when countering cyber-attacks from abroad. It uses, as a model example, DDoS attacks carried out in the past on targets in the Czech Republic. Firstly, it qualifies cyber-attack as internationally wrongful conduct. It explores possible objective element (infringement) of such conduct. It attempts to identify the conditions under which cyber-attack breaches national sovereignty or constitutes the unlawful use of force and as such violates the Charter of the United Nations. Then, the article focuses on the subjective element of unlawful conduct, i.e. the attribution of cyber-attack to a country. The third part deals with frequent situations when the subjective element (attribution, imputability) is not demonstrably present. In this context, the article considers the liability of states and other possible alternatives.*

Key words: *public international law, cyber attack, internationally unlawful conduct, use of force, violation of sovereignty, imputability, DDoS*