Univerzita Palackého v Olomouci

Právnická fakulta

David Polách

Přičitatelnost kybernetických útoků v rámci mezinárodního práva veřejného

Diplomová práce

Olomouc 2018

Prohlašuji, že jsem diplomovou práci na téma přičitatelnost kybernetických útoků v rámci mezinárodního práva veřejného vypracoval samostatně a citoval jsem všechny použité zdroje.

V Olomouci dne 19. 4. 2018 David Polách

Poděkování

Velice rád bych tímto poděkoval JUDr. Ondřeji Svačkovi, LL.M. Ph.D. za jeho odborné vedení při psaní této práce. Jeho rady, vedení a trpělivost mají lví podíl na finální podobě této práce a já si jich velmi cením.

Obsah

Úvod

Aktivně se zajímám o moderní technologie. V dnešní době je normální, že máme převážnou část pošty v elektronické podobě, sociální sítě jsou fenomén, který v Česku oslovil téměř polovinu populace,[1] pomocí nich jsme ve spojení s přáteli, rodinou, kolegy z práce a také pomocí nich hledáme partnery. Část nebo veškerou práci máme uloženou na discích vlastních počítačů nebo na cloudových úložištích Googlu či Microsoftu. Informační technologie jsou v dnešním životě jednotlivce prakticky všude. I lidé, které se těmto technologiím vyhýbají, se s nimi potkávají, aniž by to tušily. Subjekty mezinárodního práva veřejného[2] - státy jsou na tom se závislostí na informačních technologiích obdobně. Jak ukazuje vývoj z poslední doby tak se pomocí sociálních sítí vyhrávají volby,[3] o umělé inteligenci zase jeden z největších podnikatelů a mozků Sillicon Valley varuje jako před možným spouštěčem 3. světové války[4] a světové špičky v Davosu poslouchají přednášky od sociálního antropologa, který tvrdí, že lidé jsou ve skutečnosti pouze velice sofistikované seskupení nespočtu algoritmů – sofistikovaných nástrojů obdobných těm, které pohání informační technologie.[5] Výpočetní technologie se používají na úřadech při státní správě, v armádě pro obranné účely, při správě energetické či dopravní infrastruktury, v továrnách či elektrárnách.

Teoreticky je možné se skrz výpočetní technologie a internetovou síť dostat přes zabezpečení jednotlivých systémů a pracovat s nimi jako s vlastními. Je možné prohlížet a krást data, provádět různé úkony nebo data mazat. S ohledem na širokou funkčnost informačních zařízení je možné udělat mnoho užitku stejně tak jako napáchat mnoho škod. Subjekty MPV tyto nové prostředky jistě neopomíjejí – užívají jich ke špionáži, k sabotáži nebo ovlivňování veřejného mínění.

Cílem této práce je odpovědět na tyto otázky: je možné kybernetické útoky přičíst jako mezinárodně protiprávní chování subjektům MPV? Na tuto otázku logicky navazují další. Jak MPV chápe nový fenomén kybernetických útoků? Je kybernetický útok definován obdobně jako například užití síly? Jaké chování lze za kybernetický útok označit a kdy je chápáno jako

---

[1] *Forecast of Facebook user numbers in the Czech Republic from 2015 to 2022* [online]. Statista.com, [cit. 14. 4. 2018] Dostupné na <https://www.statista.com/statistics/568761/forecast-of-facebook-user-numbers-in-the-czech-republic/>

[2] Dále jen MPV

[3] VESELOVSKÝ, Martin. *Volby se pomocí dat z Facebooku ovlivňují, Cambridge Analytica je jen špička ledovce, tvrdí Řežáb* [online]. Dvtv.cz, 24. 3. 2018 [cit. 14. 4. 2018]. Dostupné na <https://video.aktualne.cz/dvtv/volby-se-pomoci-dat-z-facebooku-ovlivnuji-cambridge-analytic/r~1243a9c42eab11e88560ac1f6b220ee8/>

[4] HERN, Alex. *Elon Musk says AI could lead to third world war* [online]. 4. 9. 2018 [cit. 14. 4. 2018]. Dostupné na <https://www.theguardian.com/technology/2017/sep/04/elon-musk-ai-third-world-war-vladimir-putin>

[5] http://www.ynharari.com/wef2018/

mezinárodně protiprávní? K odpovědi na hlavní výzkumnou otázku je třeba dále vymezit jak v MPV probíhá přičtení odpovědnosti za mezinárodně protiprávní chování. Na závěr se budu zabývat otázkou – jaké důkazní prostředky bude možné užít v případě sporu o kybernetický útok před Mezinárodním soudním dvorem?[6] Jaká je možnost užití digitálních důkazů?

Problematika diplomové práce není nová, jasná úprava však chybí. Dodnes například nebyl před mezinárodními tribunály řešen jediný spor, jehož předmětem by byl kybernetický útok. V úvodní části první kapitoly, kde se snažím vydefinovat kybernetický útok, jsem prošel řadu publikací a dokumentů organizací s mezinárodním přesahem. Dále vycházím z Budapešťské smlouvy, mezinárodní smlouvy, která se problematice kybernetických útoků věnuje, úpravy evropského (a tím pádem i českého) práva a názoru akademiků. Nejvíce relevantním zdrojem na dané téma se však ukázal Tallinnský manuál. Z toho vycházím také v následující části, kdy se věnuji teorii přičitatelnosti kybernetických útoků. Zde je inspirací také Návrhu článků o odpovědnosti států od Komise pro mezinárodní právo a judikatura MSD a jeho předchůdce, která se odpovědnosti států věnuje. V poslední kapitole, která se věnuje dokazování kybernetických operací, vycházím z procesních předpisů MSD, judikatury a názorů akademiků. Snažím se o aplikaci jednotlivých závěrů na problematiku kybernetických operací a doplňuji ji o praktické příklady aplikace.

[6] Dále jen MSD

1. Vymezení pojmu kybernetický útok

Téma, kterému se ve své diplomové práci věnuji, je do značné míry specifické. Jde o prolnutí odvětví právního, konkrétně mezinárodního práva veřejného, a odvětví informačních technologií. Tato odvětví zpravidla fungují bez vzájemné závislosti. A každé z nich si vytvořilo své vlastní pojmy a názvosloví. Tím, že technologický vývoj neustále pokračuje a právo se jej snaží následně regulovat, je tato problematika stále aktuální, živá. V propojení těchto dvou odvětví se dosud nestihla vytvořit ustálená terminologie. Tedy to, co jeden pojem znamená z technického hlediska, nemusí odpovídat obsahu pojmu právního.

Kybernetický útok je ústředním pojmem mé diplomové práce. V objektivní realitě jde o pojem široký. Je obecný a zahrnuje pod sebe řadu různých variant. Může se jednat o „odposlouchávání" komunikace sítí, u kterých bylo prolomeno šifrování, může jít o DOS či sofistikovanější DDOS útoky[7], o phinshing útok[8] či o útoky, které vyžadují fyzický přístup k cílovému zařízení. Tyto útoky se liší způsobem spáchání, záměrem, motivací, závažností, představou pachatele o oběti a dalšími okolnostmi útoku. Podřadit všechny tyto eventuality významné jak z hlediska práva, tak z hlediska ICT pod jeden pojem tedy není jednoduché.

Situace je komplikovaná, protože ani Česká ani evropská právní úprava se tématům nevěnuje podrobně. Přestože již v roce 2001 byla v Budapešti přijata Úmluva Rady Evropy o kybernetickém zločinu,[9] mnohé pojmy ještě vydefinovány nejsou. V mezinárodním právu vzniklo dílo, které se přímo soustředí na kybernetické útoky a otázky s nimi se pojící. Je jím Tallinnský manuál, který je však pouhým názorem expertní skupiny[10] sestavené z odborníků na IT a právo. Práce byly organizovány pod hlavičkou NATO CCD COE,[11] ale finální produkt je třeba chápat pouze jako názor skupiny expertů, nikoliv NATO, výše zmíněné NGO, mezinárodní komise Červeného kříže ani států, jichž jsou experti státními příslušníky.[12]

---

[7] DOS útok (Denial of Service) spočívají v zahlcení cílového serveru požadavky tak, aby ten traffic nezvládl a stal se pro ostatní uživatele nedostupný. Pokročilejší variantou je DDOS útok (Distributed Denial of Service), který je na rozdíl od kalsického DOS útoku vykonán z rozsáhlé sítě počítačů (botnetu). To má za cíl těžší zabránění útoku. U DOS útoku stačí zablokovat přístup zařízení z jedné IP adresy. U DDOS útoků může jít o stovky a tisíce zařízení. Obrana a zprovoznění cílového serveru je daleko složitější.

[8] Phisihing je typ kybernetického útoku, který má za cíl falešnou zprávu z oběti vylákat citlivé údaje, ať se jedná o informace o platební kartě nebo o přihlašovací údaje do informačního systému. Klasicky probíhá pomocí emailů. Pokročilejší variantou je tzv. spear phishing kdy je dopředu konkrétně vytyčen cíl útoku, klasicky jednotlivec nebo společnost. Spear phishing v sobě zahrnuje také kromě IT znalostí i prvky sociálního inženýrství.

[9] Dostupná on-line na http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[10] SCHMITT N. Michael, VIHUL Liis. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017. s. 9

[11] North Atlantic Treaty Organisation – Cooperative Cyber Defence, Center of Excellence (https://ccdcoe.org/)

[12] SCHMITT: *Tallinn Manual 2.0*... s. 11

1.1 Příklady definic kybernetického útoku

Ústředním pojmem diplomové práce je kybernetický útok. Součástí práce je tedy i snaha kybernetický útok definovat. V mezinárodním právu veřejném definován není. Definici nenalezneme ani v obyčejovém právu, nedá se zde hovořit o dlouhodobém užívání některého z níže uvedených pojmů.[13] Definic od různých institucí je však spousta. Většina z nich je nepřesných, bez podložení autoritami relevantními pro MPV, neužívaných nebo prostě příliš vágních na to, abych z nich mohl ve své diplomové práci vycházet.

Obecně je možno kybernetický útok chápat jako škodlivý počítačový kód, nebo úkon na počítači, který je záměrně použit ke změně, narušení, odepření přístupu nebo ke smazání informace uložené v počítači nebo v počítačové síti nebo počítačů či počítačových sítí samotných.

Americké ministerstvo obrany vydalo roku 1991 interní publikaci, Memorandum pro armádní velitele,[14] která měla za cíl sjednocovat terminologii v oblasti kybernetických operací. Definice zní: „Kybernetický útok je kategorie výpadů užitých pro útočné účely, které jsou uskutečněny skrz počítačovou síť za účelem narušit, odepřít přístup, změnit či smazat informaci, která je uložena v cílovém informačním systému nebo počítačové síti, nebo s cílem zničit informační systém či počítačovou síť samotnou. Výsledný zamýšlený efektem nemusí být způsoben v samotném napadeném informačním systému či počítačové síti, ale může sloužit jako prostředek ke zpravodajským či anti-teroristickým operacím, jako např. pozměňování či odposlouchávání komunikace nebo získání či odepření přístupu ke komunikačním a logistickým kanálům protivníka.“[15]

Nejnovější definice z roku 2017, která pochází od amerického ministerstva obrany, konkrétně od jeho *Vědecké rady pro obranu*, uvádí[16] tuto definici: „Pro účely této zprávy je

[13] SCHMITT, N. Michael. Computer Network attack and the use of force in international law: Thoughts on a normavitve framework. *Columbia Journal of Transnational Law*. Vol. 37, 1998-99. s. 22

[14] CARTWRIGHT, E. James. *Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directories*. [online]. nsci-va.org, 21. 3. 2018 [cit. 21. 3. 2018]. Dostupné na <http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf>

[15] A category of fires employed for offensive purposes in which actions are taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems networks themselves. The ultimate intended effect is not necessarily on the targeted system itself, but may support a larger effort, such as information operations or counter-terrorism, e.g., altering or spoofing specific communications or gaining or denying access to adversary communications or logistics channels.

[16] FIELDS, Craig. *Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence* [online]. acq.osd.mil/dsb, 21.3.2018 [cit. 21.3.2018]. Dostupné na <https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf>

kybernetickým útokem chápán jakýkoliv úmyslný čin, který ovlivňuje zamýšlenou dostupnost a/nebo integritu dat nebo informačních systémů, které jsou důležité pro fungování napadených organizací. Ne všechny kybernetické průniky však lze považovat za útoky; u velké většiny je tomu opačně. Kybernetické útoky mohou mít dočasný či trvalý efekt; mohou mít za následek zničení elektronických zařízení či přerušení služeb, která zařízení poskytují; mohou být vykonány pomocí vzdáleného přístupu, anebo na místě (včetně útoků provedených členy organizace samotné). Dále, přestože je značná pozornost směřována na kybernetické útoky zaměřené na data a software, zranitelnost zásobovacích kanálů nabývá na důležitosti s tím, kde kritické infrastruktury jsou vystavěny a udržovány pomocí globálních zásobovacích kanálů, které mohou být v jakékoliv své části napadeny."[17]

Program výzkumu humanitární politiky a konfliktů při Harvardské univerzitě udává ve svém Manuálu mezinárodního práva v leteckém válečnictví následující definici kybernetického útoku: „Útok počítačovou sítí je operace manipulující, narušující, odmítající, měnící či mazající informaci uloženou v počítačích a počítačových systémech, nebo počítačovou síť samotnou, nebo operace mající za cíl získat kontrolu nad počítačem či počítačovou sítí."[18][19]

Americká *Národní Akademie vědců* definuje ve své publikaci[20] kybernetický útok následovně: „Kybernetickým útokem se rozumí úmyslné jednání po delší časový úsek, které má za účel, změnu, narušení, uvedení v omyl, poškození, či smazání nepřátelských počítačových systémů či sítí, nebo informací a programů, které jsou v těchto systémech či sítích uloženy, či na nich běží. Zmíněné následky na nepřátelské systémy či sítě mohou mít také nepřímý efekt na osoby spojené či spoléhající na dané systémy či sítě. Kybernetický útok má za cíl vyřadit služby mimo provoz nebo je znevěrohodnit a tím je v důsledku učinit méně užitečnými. Protože existuje mnoho možností, jak lze daného cíle dosáhnout, pojem „kybernetický útok" by měl být chápán

[17] Tamtéž. s. 10; Cyber Attack. For the purposes of this report, a cyber attack is any deliberate action that affects the desired availability and/or integrity of data or information systems integral to operational outcomes of a given organization. Not all cyber intrusions constitute attacks; indeed the vast majority do not. Cyber attacks may have temporary or permanent effects; they may be destructive of equipment or only disruptive of services; and they may be conducted remotely or by close access (including by insiders). In addition, while there is considerable attention given to cyber attacks focused on data and software-in-operation, supply chain vulnerabilities are of growing concern in a world where critical infrastructure is built and sustained through a global supply chain subject to malicious alteration across various phases of system life cycles.

[18] "Computer network attack" means operations to manipulate, disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computer network itself, or to gain control over the computer or computer network.

[19] BRUDERLEIN, Claude. *HPCR Manual on International Law Applicable to Air and Missile Warfare*. [online]. reliefweb.int, 21. 3. 2018 [cit. 21. 3. 2018]. Dostupné na <https://reliefweb.int/sites/reliefweb.int/files/resources/8B2E79FC145BFB3D492576E00021ED34-HPCR-may2009.pdf>

[20] OWENS A. William a kol. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC 20055: The National Academies Press, 2009. s. 11

jako způsob provedení akce, nikoliv jako pojem, ze kterého je možné odvodit následky daného jednání."[21]

Banka pro mezinárodní vypořádání ve své publikaci Pokyny ke kybernetické odolnosti informačních infrastruktur finančního trhu z června 2016 definuje kybernetické útoky jako: „Využití softwarové chyby s úmyslem ji zneužít a způsobit negativní následky v kybernetickém prostředí."[22]

Dle NBÚ je kybernetický útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.[23]

Výčet výše uvedených definic není konečný, pro ilustraci však postačí. Uvedené definice nejsou pro mezinárodní právo veřejné závazné. Jejich závaznost zpravidla končí tam, kde končí pole působnosti organizace, která ji pro své potřeby vytvořila. Definice se shodují v tom, že kybernetický útok je veden přes počítač či počítačovou síť. Neméně důležité otázky jako motivace, cíl, následek, identita útočníka či rozsah způsobených škod však jsou řešeny pouze v některých případech. Přitom pro stanovení jasných hranic pojmu kybernetický útok jsou stěžejní.

1.2 Mezinárodní právo veřejné

Primárním zdrojem mé diplomové práce je mezinárodní právo. Jako relevantní zdroje Statut Mezinárodního soudního dvora uvádí mezinárodní úmluvy, mezinárodní obyčeje a obecné zásady právní uznávané civilizovanými národy. Jako podpůrný prostředek jsou chápány soudní rozhodnutí a učení nejkvalifikovanějších znalců mezinárodního práva veřejného. [24]

V oblasti mezinárodního práva existují smlouvy, které se problematice kyberprostoru věnují. Žádná z nich však nedefinuje přímo pojem kybernetický útok. Budapešťská úmluva o počítačové

[21] Cyberattack refers to the use of deliberate actions—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks. Such effects on adversary systems and networks may also have indirect effects on entities coupled to or reliant on them. A cyberattack seeks to cause adversary computer systems and networks to be unavailable or untrustworthy and therefore less useful to the adversary. Furthermore, because so many different kinds of cyberattack are possible, the term "cyberattack" should be understood as a statement about a methodology for action—and that alone—rather than as a statement about the scale of the action's effect.

[22] Banka pro mezinárodní vyrovnání. *Guidance on cyber resilience for financial market infrastructure*. Červen 2016. s. 23. Dostupné na <https://www.bis.org/cpmi/publ/d146.pdf >; The use of an exploit by an adversary to take advantage of a weakness(es) with the intent of achieving an adverse effect on the ICT environment.

[23] JIRÁSEK, Petr. NOVÁK, Luděk. POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. Policejní akademie ČR & Česká pobočka AFCEA, 2013. s. 59

[24] Mezinárodní soudní dvůr, *Statut mezinárodního soudního dvora*, čl. 38, dostupné na <http://www.icj-cij.org/en/statute>

kriminalitě, upravuje kybernetické operace se zaměřením na vnitrostátní právo. Pokrývá základní objekty důležité pro bezpečnost dat[25] tak, jak jej chápe obor kybernetické bezpečnosti. Jsou jimi důvěrnost, integrita a dostupnost dat.[26] Porušením těchto objektů dojde ke spáchání trestné činnosti. Přístupem k úmluvě se její strany zavazují, že takové trestné činy zavedou do svých právních řádů. Úmluva dále obsahuje část věnující se mezinárodní spolupráci. Je stanoveno, že státy budou při vyšetřování kybernetických zločinů spolupracovat a budou si vzájemně nápomocny. Jsou stanoveny podmínky vydávání osob[27], povinnosti o sběru dat a umožnění přístupu k nim ostatním státům.[28] Přestože byla Úmluva sepsána pod hlavičkou Rady Evropy, přistoupila k ní i řada zemí z celého světa jako Spojené státy americké, Kanada a řada afrických zemí. Celkem je Úmluva ratifikována v 57 státech světa.[29] Autorita tohoto dokumentu je tedy, ve srovnání s další úpravou kybernetického práva, poměrně značná.

Z hlediska mezinárodního obyčeje nebo obecné právní zásady je také těžké vycházet. Kybernetické útoky a kyberprostor obecně jsou fenoménem posledního čtvrt století, tedy od 90. let 20. století, kdy došlo k prvnímu masivnímu rozšíření internetu. Podmínky pro vytvoření mezinárodního obyčejového práva – dlouhodobé používání a přesvědčení o závaznosti tedy v případě kybernetického útoku zatím neměly příliš šanci zakořenit. V mezinárodním společenství zatím nepanuje shoda v takovém rozsahu, aby se o ní dalo mluvit jako o mezinárodním obyčeji. Je faktem, že pro vytvoření některých zvyklostí postačí čas krátký v řádech jednotek let. Prvek přesvědčení o závaznosti je však nezbytný. A ani ten nebyl naplněn. Žádná definice nebyla natolik respektována, aby si dané postavení v rámci mezinárodního společenství vydobyla.[30]

1.3 Tallinnský manuál

Publikací, která danou oblast reguluje nejpodrobněji je Tallinnský manuál. V době psaní mé práce vyšlo již druhé rozšířené vydání. Tallinnský manuál je však pouhým názorem expertní skupiny[31] sestavené z odborníků na IT a právo. Práce byly organizovány pod hlavičkou NATO CCD COE,[32] ale finální produkt je třeba chápat pouze jako názor skupiny expertů, nikoliv

[25] Sbírka mezinárodních smluv č. 104/2013, částka 56, rozesláno dne 23. prosince 2013. *Úmluva o počítačové kriminalitě*. s. 4
[26] „confidentiality, integrity a availability“
[27] SbMS. *Úmluva o počítačové*... Čl. 24
[28] SbMS. *Úmluva o počítačové*... Čl. 29 – 33 Úmluvy.
[29] Rada Evropy. Přehled podpisů a ratifikací smlouvy. Dostupné na: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=I7b2z8Y2>
[30] SCHMITT: *Computer Network Attack*...s. 22
[31] SCHMITT: *Tallinn Manual 2.0*.... s. 2
[32] North Atlantic Treaty Organisation – Cooperative Cyber Defence, Center of Excellence (https://ccdcoe.org/)

NATO, výše zmíněného think-tanku, Mezinárodního výboru Červeného kříže ani států, jichž jsou experti státními příslušníky.

V Tallinnském manuálu se pro kybernetický útok v technickém smyslu užívá několik označení.

Za obecný pojem lze označit „kybernetickou aktivitu" (*cyber acitvity*).[33] Jedná se o jakoukoliv aktivitu, k jejímuž vykonání je užita kybernetická infrastruktura[34] nebo kybernetické prostředky, které směřují k ovlivnění kybernetické infrastruktury. Tyto aktivity jsou širším pojmem než kybernetická operace (*cyber operations*)[35], která pod kybernetickou aktivitu spadá. Kybernetické operace jsou chápány jako užití kybernetických schopností k dosažení cílů v kyberprostoru nebo skrze kyberprostor. Pojem kybernetické operace nejblíže odpovídá obecnému pojmu kybernetický útok tak, jak byl popsán na začátku kapitoly.

Tallinnský manuál definuje i přímo pojem „*cyber attack*", který je do češtiny překládán jako kybernetický útok. Na tomto místě je třeba si uvědomit odlišnost terminologie právní a terminologie ICT. Výseč objektivní reality, kterou ICT označuje za kybernetický útok, je mnohem širší, než situace, kterou pod pojmem kybernetický útok chápe Manuál. Manuál kybernetický útok definuje jako kybernetickou operaci učiněnou ať v útoku či obraně, u které lze mít důvodně za to, že způsobí zranění či smrt osob nebo škodu či zničení věci.[36] Manuál kybernetický útok zařazuje do práva ozbrojených konfliktů, pravidel, které státy musí dodržovat v době, kdy mezi nimi probíhá ozbrojený konflikt.

Tallinnský manuál se zabývá otázkou, které normy mohou být kybernetickým útokem v materiálním slova smyslu porušeny. Od státní suverenity, přes povinnosti náležité opatrnosti, dále přes specializovaná odvětví práva jako diplomatické a konzulární právo, mořské právo, kosmické právo, pokračujíc právní úpravou k zajištění míru a bezpečnosti jako zákaz vměšování se do záležitostí cizích států a užití síly a konče právem kybernetických ozbrojených konfliktů.

Z těchto jsem vybral právní odvětví, která budou dle mého porušována nejčastěji, či k jejichž porušování již dnes dochází, a tudíž bude jejich význam největší. Zákaz nevměšování se do vnitřních záležitostí a porušení suverenity státu jsou povinnosti, které je možno podřadit pod

[33] SCHMITT: *Tallinn Manual 2.0*... s. 564
[34] „cyber infrastructure" je definována jako komunikační, úložná a výpočetní zařízení, která jsou užita k vystavění a užívání informačních systémů. Jde tedy o širokou paletu přístrojů od počítačů, přes tablety, laptopy a smartphoney až po televize a tiskárny.
[35] Tamtéž
[36] Tamtéž s. 415

obecné MPV. Oblast užití síly spadá do části MPV nazývané *ius ad bellum*.[37] Pojem ozbrojeného útoku do části *ius in bello*.[38] Užití síly a ozbrojený útok spáchané kybernetickými prostředky jsou z hlediska způsobených následků nejzávažnější.

Právě definování kybernetického útoku pomocí následků a norem, které poruší, mi přišlo po prostudování dostupných pramenů jako nejvhodnější. Vzhledem k rozsáhlosti pojmu kybernetický útok v technickém slova smyslu a všem jeho možným podobám není možné vymezit jednotnou definici, která by na jedné straně zahrnovala všechny způsoby provedení a na straně druhé všechny myslitelné následky. Užití pojmu kybernetická operace jak byl definován výše, bude sloužit jako výchozí bod vymezení, co vše může být kybernetickým útokem porušeno.

1.3.1. Kybernetický útok jako zásah do suverenity státu

Suverenitou státu rozumíme jeho nezávislost. Ve vztahu dovnitř se suverenita projevuje tím, že stát je vůči svému obyvatelstvu nejvyšším nositelem veřejné moci. Ve směru navenek stát není podroben žádné vyšší moci a suverénní státy jsou si vzájemně rovné. Základní omezení státní suverenity spočívá v tom, že stát, nemůže vykonávat vlastní moc na území cizího státu, ledaže existují normy povolující mu dané chování.[39]

Tallinnský manuál uvádí, že princip státní suverenity je aplikovatelný na kyberprostor.[40] Kybernetické operace jako nový fenomén, kterým je možné zasahovat do suverenity států, chápou i další akademikové.[41] Suverenitu, jako princip, který je i v kybernetickém prostředí třeba dodržovat, chápe i skupina vládních expertů zabývajících se otázkou kybernetického prostoru při Organizaci spojených národů.[42] Manuál tedy není jediný, kdo je názoru, že kybernetickou operací může být zasaženo do suverenity států. Tímto pravidlem jsou chráněny kybernetické infrastruktury a kybernetické aktivity, jak na území státu, tak ty, které se fyzicky nachází či odehrávají v zahraničí a státu patří či je vykonává. Princip státní suverenity je dle mezinárodního soudního dvora úzce propojen se zákazem užití síly a nevměšováním se do záležitostí státu.[43]

---

[37] *Ius ad bellum* – překládáno jako právo na válku. Shodně se užívá též pojem *ius contra bellum* – právo proti válce. Obsah těchto pojmů je shodný.
[38] *Ius in bello* – překládáno jako právo válečné. Jde o pravidla, která mají zavazovat válčící strany v průběhu konfliktu.
[39] Stálý dvůr mezinárodní spravedlnosti: Rozsudek ze dne 7. září 1927, *The case of the S.S. "Lotus"*, s. 18
[40] SCHMITT: *Tallinn Manual 2.0*.... Rule 1
[41] MARGULIES, Peter. Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. *Melbourne Journal of International Law*, 2013, roč. 14 č. 1, s. 1
[42] Skupina vládních odborníků při OSN. Vývoj v oblasti informačních technologií v kontextu mezinárodní bezpečnosti. Zpráva za rok 2015. s. 8. Dostupné na: <https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf>
[43] Mezinárodní soudní dvůr: Rozsudek ze dne 27. června 1986, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* odst. 212

Manuál rozděluje kybernetický prostor pro účely státní suverenity na tři složky. Složku fyzickou, jež zahrnuje fyzické části vybavení jako osobní počítače, routery, kabely nebo serverová úložiště. Logickou složku, která zahrnuje připojení těchto zařízení k síti. Ta zahrnuje aplikace, data a protokoly, které umožňují předávání informací skrz fyzickou složku. Poslední je sociální složka zahrnující jednotlivce a skupiny, které vykonávají kybernetické operace.[44] Suverenitou jsou kryty všechny tyto tři složky. Zásahem do suverenity je tedy zásah do jakékoliv ze tří výše uvedených složek ať už na území státu nebo mimo něj, jestliže nad ní stát vykonává moc. Zahrnuty budou kybernetické operace, které budou cíleny na kritické infrastruktury,[45] ve vlastnictví fyzických i právnických osob zahraničního původu, umístěné na území státu. Rozhodující je fakt, že stát nad infrastrukturou vykonává svrchovanou moc.

S ohledem na vnější projevy suverenity stát může provádět všechny kybernetické operace, které nevylučují normy mezinárodního práva, jimiž je stát vázán.[46] Limitace výkonu suverenity se obdobně uplatňují i v kyberprostoru. Nebude například zasaženo do suverenity hostitelského státu, v němž bude napadeno zařízení diplomatické mise vysílajícího státu.

V mezinárodním právu veřejném se s možností danou oblast regulovat zpravidla pojí také odpovědnost za ni.[47] Pokud tedy budeme takto chápat i suverenitu v kyberprostoru dojdeme k zajímavým závěrům. Nejen že z ní bude plynout povinnost respektovat suverenitu ostatních států, povinnost do záležitostí cizích států nezasahovat, ale také povinnost kontrolovat chování, které se odehrává na území, kde suverénní moc stát vykonává.[48] S tím by se pojila povinnost států vykonávat svou státní moc takovým způsobem, aby na jeho území nedocházelo k chování, které by porušovalo mezinárodní právo.[49] Stát by byl povinen monitorovat své území tak, aby ke kybernetickým operacím porušujícím mezinárodní právo nedošlo. V případě, že by k porušení došlo, byl by stát povinen poskytnout součinnost za účelem odhalení osoby či skupiny, která operaci vykonala.[50]

Koncept suverenity je aplikovatelný také v případech, kdy probíhají ozbrojené konflikty a mezi válčícími státy je uplatňované válečné právo. V těchto případech pro neutrální stát, plyne

---

[44] SCHMITT: *Tallinn Manual 2.0*... Pravidlo 1, odst. 4
[45] Kritická infrastruktura je definována jako fyzický nebo virtuální systém a aktiva státu, které jsou tak zásadní, že jejich vyřazení mimo provoz nebo zničení mohou ohrozit bezpečnost státu, ekonomiku, veřejné zdraví nebo životní prostředí. SCHMITT: *Tallinn Manual 2.0*... s. 564
[46] SCHMITT*: Tallinn Manual 2.0*... pravidlo 3
[47] Mezinárodní soudní dvůr: Samostatný názor soudce Alvareze ze dne 9. dubna 1949, *Případ kanálu Korfu*, odst. 43
[48] Evropský soud pro lidská práva: Rozsudek ze dne 8. července 2004, *Ilascu a ostatní proti Moldávii a Rusku*, (Application no. 48787/99). odst. 312
[49] JENSEN, T. Eric. Cyber Sovereignty the Way Ahead *Texas International Law Journal.* 2015, roč. 50, č. 1, s. 296
[50] Tamtéž s. 297

povinnost zabránit užití svého teritoria pro válečné účely nepřátelských stran.[51] Toto pravidlo zahrnuje povinnost neutrálního státu mít přehled o aktivitách na svém území, pokud mu to jeho prostředky dovolují. Cílem je zabránit znepřáteleným státům porušení neutrality tohoto státu. Aktivity válčícího státu v reakci na neschopnost nebo neochotu neutrálního státu udržet neutralitu by jistě představovaly porušení suverenity neutrálního státu.[52] Pokud by například mezi dvěma státy probíhal ozbrojený konflikt a na území třetího státu by se nacházela skupina, která by jeden ze států, účastnících se ozbrojeného konfliktu, chápala jako svého nepřítele a bez návaznosti na druhý stát účastnící se konfliktu, proti němu zahájila kybernetickou operaci, nemohl by proti této skupině napadený stát zakročit, aniž by porušil suverenitu neutrálního státu.

V případě, kdy kybernetická operace skončí neúspěchem a je zablokována firewallem či jiným obraným prostředkem a nenastane očekávaný účinek, nedojde v tomto případě k zásahu do suverenity. Manuál konstatuje, že k porušení suverenity se musí projevit následky kybernetické operace.[53]

Je také možné, aby stát, proti němuž je kybernetická operace vedena, s ní předem vyslovil souhlas, a tím vyloučil její nezákonnost. Příkladem může být okamžik, kdy je stát napaden kybernetickou operací a sám nemá CERT[54] či jiné prostředky, jak se proti těmto útokům bránit. Požádá tedy stát, s nímž má uzavřenou smlouvu, který mu pomůže se zastavením a analýzou kybernetické operace.

Manuál se staví proti zařazení kybernetického prostoru jako „páté domény", která postrádá fyzickou složku a je ze své podstaty nehmotná. Dle názoru autorů by tím byla pominuta fyzická složka, která stojí za kyberprostorem a kybernetickými operacemi. Tímto pominutím by docházelo k omezení aplikovatelnosti zásady suverenity. Přestože mohou kybernetické útoky během několika vteřin překročit nespočet státních hranic a způsobit rozsáhlé škody, ve finále je zde vždy osoba, která útok vykoná. Tato je pak subjektem práva státu, jehož je občanem či na jehož území se nachází a který by měl její chování regulovat.[55]

---

[51] Haagská úmluva V, Práva a povinnosti neutrálních mocností a osob v případě války pozemní ze dne 18. října 1907. čl. 5. Dostupné na: <http://avalon.law.yale.edu/20th_century/hague05.asp>

[52] JENSEN, T. Eric. Sovereignty and neutrality in cyber conflict. *Fordham Inernational Law Journal*, 2012, roč. 35, č. 3, s. 834

[53] SCHMITT: *Tallinn Manual 2.0*... Pravidlo 4, odst. 24

[54] CERT – Zkratka pojmu Cyber Emergency Reaction Team – jedná se o entity zpravidla vládního charakteru, které mají za úkol předcházení rizikům plynoucích z kybernetických útoků, reakci na kybernetické útoky, jejich analýzu a pátrání po jejich původcích

[55] SCHMITT: *Tallinn Manual 2.0*... Pravidlo 1, odst. 5

1.3.2. Kybernetický útok jako zasahování do vnitřních záležitostí států

Manuál stanoví: „Stát má zakázáno zasahovat do vnitřních či vnějších záležitostí států kybernetickými prostředky.“[56] Obdobně kybernetické operace jako zasahování do vnitřních záležitostí státu chápou i akademicikové.[57] Toto pravidlo je založeno na základním principu suverenity států. Zákaz zasahování do vnitřních záležitostí státu byl mnohokrát Mezinárodním soudním dvorem potvrzen jako obyčejové právo.[58] Mezinárodní soudní dvůr konstatoval srozumění s faktem, že k zasahování do vnitřních záležitostí státu jinými státy dochází a neočekává, že by k porušování tohoto pravidla nedocházelo.[59] Přestože v mezinárodním společenství dochází k porušování pravidla nevměšování se do vnitřních záležitostí státu, neuvažuje se o něm jako o zastaralém či přestávajícím existovat, protože přesvědčení o jeho závaznosti je naplněno dostatečně.[60] Fakt, že v praxi často dochází k porušování zákazu nevměšování se ze strany států právě na základě kybernetických operací, není důvodem pro povolení těchto chování.[61] Tento názor sdílí také řada akademiků, kteří o zákazu zasahování do vnitřních záležitostí státu běžně uvažují a aplikují v modelových i skutečných případech.[62]

Pravidlo zahrnuje situace, kdy je zasaženo do vnitřních či vnějších záležitostí státu kybernetickými prostředky nebo je klasickými prostředky zasaženo do kybernetických aktivit napadeného státu. Zákaz nevměšování se obsahuje dva prvky. Prvním je zasažení do vnitřních či vnějších záležitostí státu, druhým je donucení, které ze zásahu vyplývá.[63]

Vnitřní záležitosti státu jsou typicky ty, které si dle principu suverenity může každý stát určit sám. Vnitřní záležitosti státu nepřímo zakotvuje Deklarace zásad mezinárodního práva týkajících se přátelských vztahů a spolupráce mezi státy. Tato stanovuje povinnost států vystříhat se užití síly jak proti územní celistvosti, tak proti politické nezávislosti, Dále zakotvuje povinnost se nevměšovat do záležitostí, které patří do vnitřních pravomocí kteréhokoli státu, kam je možné

[56] Tamtéž; pravidlo 66
[57] SCHMIT. N. Michael, 'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International law,* 2014, roč. 54, č. 1, s. 705
[58] MSD: *Nikaragua*... odst. 202. MSD. *Korfu*... s. 35
[59] MSD: *Nikaragua*... odst. 186
[60] Tamtéž odst. 202
[61] SCHMITT: *Computer Network Attack*..pravidlo 66, odst. 5
[62] WATTS, Sean. Low-Intensity Computer Network Attack and Self-Defense. *International Law Studies*, 2011, roč. 87; KASTENBERG, E. Joshua. Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law. *Air Force Law Review*, 2009, roč. 64, č. 1
[63] MSD: *Nikaragua*... odst. 205

zařadit politické uspořádání, ekonomický systém státu nebo hospodářské a kulturní základy státu.[64] Tyto jsou typickým příkladem vnitřních záležitostí státu.

Druhým prvkem zasahování do vnitřních záležitostí je úmysl zasahujícího státu donutit k určitému chování v jeho záležitostech cílový stát. Standardně by se stát rozhodnul volně, stát zasahující do vnitřních záležitostí jiného státu ale tuto volbu manipuluje svým zasahováním. Typickým případem, kdy dochází k zasahování do vnitřních záležitostí státu je užití síly. Ať už přímo jako v případech vojenských akcí, nebo nepřímo v případě podpory podvratných či teroristických akcí proti cílovému státu.[65]

Účelem kybernetické operace, kterou lze kvalifikovat jako porušení zákazu nevměšování se, má být ovlivnění jednání státu. Například kybernetická operace, při níž je cílem určitá etnická skupina sídlící v sousedním státě, nemusí naplnit podmínky vměšování se do vnitřních záležitostí státu. Příkladem může být umístění obrázků kočiček na oficiální stránky organizace sdružující toto etnikum. Dojde k narušení suverenity státu, jehož občany budou členové etnické skupiny, ale nedojde-li k donucování státu ohledně interních záležitostí, do vnitřních záležitostí státu nebude zasaženo.

Ta samá operace může být za vměšování se do vnitřních záležitostí v jiných podmínkách považována. Představme si situaci, kdy by například v cílovém státě mělo proběhnout jednání vlády o zrušení jazyka této menšiny jako jednoho z oficiálních jazyků státu. V případě, že by cizí stát provedl kybernetické operace na server, který by měl za cíl sdružovat příslušníky dané etnické skupiny a na oficiální vládní web s tím, že umístil na obě stránky „*hate speech*" namířené proti sobě, dojde k upozornění na dané téma. Na skandál vzniklý díky kybernetické operaci může zareagovat mezinárodní společenství či početná skupina stejného etnika ve státě, který kybernetickou operaci vykonal nebo ve třetím státě. Na cílový stát začne být vyvíjen nátlak. Ze strany příslušníků etnické skupiny může dojít až k aktům násilím. Všechny akce budou činěny za účelem zachování jazyka etnika jako oficiálního jazyka daného státu. V tomto případě byla kybernetická operace vykonána za účelem ovlivnit rozhodnutí vlády o vyloučení jazyka jako oficiálního jazyka daného státu a bylo jí zasaženo do vnitřních záležitostí tohoto státu. Došlo by tedy k porušení pravidla o zákazu nevměšování se do vnitřních záležitostí státu.

Suverenita a zákaz zasahování do vnitřních záležitostí státu se uplatňují i v době probíhajícího ozbrojeného konfliktu, který nemá mezinárodní charakter. Lze uvažovat o situaci, kdy skupina

[64] FAIX, Martin, BUREŠ, Pavel, SVAČEK, Ondřej. *Rukověť ke studiu mezinárodního práva 1: Dokumenty*. Praha: Leges. 2015, s. 27 – 28
[65] MSD: Nikaragua... odst. 205

hackerů působící především na území jednoho státu provede, ať už k tomu má jakýkoliv důvod, kybernetickou operaci proti cílovému státu. Pokud v tomto případě napadený stát proti skupině, která útok vykonala, spustí odvetnou operaci, která by byla užitím síly (například vyšle skupinu agentů s cílem vyřadit servery, ze kterých byla operace vykonána), půjde o zasažení do suverenity a do vnitřních záležitostí státu, na jehož území se skupina vyskytuje.[66] Pokud by například Estonsko v roce 2007, kdy bylo pod DDoS útokem vykonala odvetnou operaci proti Rusku, které vnímalo jako zemi, která za útokem stojí, došlo by k porušení suverenity a zasažení do vnitřních záležitostí Ruské federace.

Výsledek kybernetické operace se nemusí vůbec projevit ve fyzické sféře, aby k zasahování do vnitřních záležitostí došlo. Není třeba, aby došlo k poškození počítače nebo fyzickému zničení sítě. Může se jednat čistě o kybernetické následky. Může jít o DDoS útok, kdy budou znepřístupněny servery tohoto etnika či o operaci, při které bude změněn obsah webových stránek.

Aplikujeme-li závěry MSD ve věci Nicaragua na kybernetické prostředí, dojdeme k závěru, že vměšováním se do vnitřních záležitostí státu je také podpora osvobozeneckých hnutí, které provádějí kybernetické operace. Může jít o instruktáže, vzdělávání, podporu finanční, technickou o poskytnutí zázemí nebo vybavení.[67]

1.3.3. Kybernetický útok jako užití síly

Několik odborníků na mezinárodní právo se zabývá spojitostí mezi kybernetickými útoky a mezinárodním právem v oblasti zákazu užití síly. Akademikem, který je v tomto ohledu nejvíce respektován, je Michael Schmitt, který se problematice věnuje již od 90. let[68] a je vedoucím autorem Tallinnského manuálu. Mnohost forem kybernetického útoku v technickém slova smyslu a jeho rozdílné následky vedly odborníky k řešení otázky, jaké normy mohou být tímto porušeny. Byla řešena otázka, zda může být kybernetická operace kvalifikována jako hrozba silou či užití síly dle článku 2 odst. 4 Charty OSN či dokonce ozbrojeným útokem.[69] Vztah těchto dvou institutů je takový, že ozbrojený útok je vždy užitím síly a zakládá, za splnění dalších podmínek, právo státu na sebeobranu. U užití síly, nedosahující intenzity ozbrojeného útoku, nárok na sebeobranu státu nevzniká. Je-li tedy jako odplata užita síla napadeným státem, dopustí se tento

[66] JENSEN. *Sovereignty...*
[67] MSD: *Nikaragua...* odst. 242
[68] SCHMITT: *Computer Network Attack...*
[69] Organizace spojených národů, . čl. 2 odst. 4, Charta OSN ze dne 26. června 1945. *„Všichni členové se vystříhají ve svých mezinárodních stycích hrozby silou nebo použití síly jak proti územní celistvosti nebo politické nezávislosti kteréhokoli státu, tak jakýmkoli jiným způsobem neslučitelným s cíli Organizace spojených národů."*

reagující stát svým jednáním porušení norem mezinárodního práva. Zaměřím se nejprve na pojem užití síly a hrozbu silou.

Zákaz užití síly je postaven tak, aby chránil klíčové zájmy mezinárodního společenství. Zájmy, kterých si lidské společenství cení nejvíce, jsou vyjmenovány v preambuli Charty OSN a její první kapitole. Za účelem ochrany těchto zájmů OSN v Chartě zakazuje jednání, která by chráněné zájmy porušila. Mezi takové zákazy se řadí i zákaz hrozby silou a zákaz užití síly. Mezinárodní společenství se nevyhrazuje proti užití síly jako takovému, ale proti jeho následkům. Bylo by však mimořádně obtížné kvantifikovat nebo kvalifikovat důsledky normativně praktickým způsobem. Zákaz síly jako takové, jak činí článek 2 odst. 4 Charty OSN, je tedy jasnější a praktičtější.[70]

Mezinárodní soudní dvůr konstatoval, že články Charty OSN zakazující užití síly a ozbrojený útok, jsou aplikovatelné na každé užití síly bez ohledu na to, jaký druh zbraně byl použit.[71] Skutečnost, že je užití síly spácháno kybernetickou operací, tedy v tomto ohledu není překážkou. Situace, kdy kybernetická operace nedosáhne na hranici užití síly, neznamená, že se jedná o legální jednání. Mohou jím být porušeny jiné normy MPV zejména zákaz nevměšování se do záležitostí cizích států a porušení suverenity státu.

Charta OSN nestanovuje žádná kritéria pro určení, kdy se jedná o užití síly. V rozhodnutí MSD ve věci *Nikaragua* Soud tvrdí, že pro určení, kdy se jedná o užití síly, se vychází z kritérií „rozsahu a následku".[72] Manuál toto pravidla přebírá a používá jej též při kvalifikaci kybernetických operací. Experti došli k závěru, že není důvod vyloučit z užití síly následek způsobený kybernetickou operací tehdy, pokud je srovnatelný s následky způsobenými konvenčním jednáním, které by jako užití síly kvalifikováno bylo. [73]

Navazující otázkou je, co vše pod pojem užití síly spadá a kdy pod něj lze zařadit kybernetickou operaci. Vídeňská úmluva o smluvním právu říká, že k interpretaci smluv je možno užít přípravné dokumenty, které předcházely schválení smlouvy samotné.[74] Z těchto lze vyčíst, že při přijímání Charty OSN diskutovaným tématem byla otázka, jestli lze pod pojem užití síly podřadit politický a ekonomický nátlak. Brazilská komise navrhla zařazení ekonomického nátlaku pod pojem užití síly, ten byl však odmítnut.[75] Na druhou stranu v rozsudku v případu *Nikaragua* Mezinárodní soudní dvůr judikoval, že výcvik a vyzbrojení může být považována za

[70] SCHMITT: *Computer Network Attack*... s. 16
[71] Mezinárodní soudní dvůr: Rozsudek ze dne 8. července 1996. *Legalita hrozby nebo užití jaderných zbraní.* odst. 39
[72] MSD: *Nikaragua*... odst. 195, 212
[73] SCHMITT: *Tallinn Manual 2.0*.. s. 331
[74] Vídeňská úmluva o smluvním právu, . čl. 31. Sjednána dne 23. května 1969
[75] EDITOŘI. The Use of Nonviolent Coercion: A Study in Legality under Article 2(4) of the Charter of the United Nations. *University of Pennsylvania Law Review*, 1974, roč. 122, č. 4, s. 994

hrozbu silou či užití síly.[76] Tyto dva případy ukazují, co ještě spadá pod pojem užití síly a co už ne. Ve finále však posouzení, zda se bude jednat o užití síly či nikoliv bude záviset na individuálních okolnostech daného případu. Čím více invazivní kybernetická operace bude a čím větší škody způsobí, tím pravděpodobnější bude její kvalifikace jako užití síly.[77]

Aplikací závěrů z rozsudku ve věci *Nikaragua* vyplývá, že financování hacktivistů,[78] kteří bojují proti své vládě, nebude užitím síly. Na druhou stranu poskytnutí výcviku takovéto skupině a poskytnutí malware[79] k provedení útoku již užitím síly bude.

Manuál poukázal na nejasnost klasifikace kybernetických útoků v okamžiku, kdy již nedosahují hranice ozbrojeného útoku, ale bylo by možné je kvalifikovat jako užití síly. Vyjmenovává osm kritérií, ale i sami autoři označují výčet za demonstrativní.[80] Mezi kritérii je závažnost, která stanovuje, že v případě fyzického poškození věci nebo způsobení zranění osobě se vždy jedná o užití síly. Dále je stanoveno, že čím důležitější zájmy státu jsou kybernetickým útokem zasaženy, tím více je pravděpodobné, že je mezinárodní společenství bude vnímat jako užití síly. Rozsah, délka trvání a intenzita jsou tímto kritériem zahrnuty a všechny mají vliv na posouzení kybernetické operace jako užití síly. Dalšími kritérii jsou bezprostřednost, která zohledňuje čas mezi vykonanou kybernetickou operací a okamžikem, kdy nastanou její následky, přímost, sledující kauzalitu mezi operací a způsobenými následky. Dále je zohledňováno, jak moc operace zasahuje do záležitostí států, měřitelné následky kybernetické operace, vojenský charakter kybernetické operace, účast státu na kybernetické operaci a její předpokládaná legalita.

1.3.4. Kybernetický útok jako ozbrojený útok

Již dříve bylo uvedeno, že MSD ve svém rozhodnutí *ve věci jaderných zbraní* vymezil, že ozbrojený útok lze spáchat bez ohledu na to, jaké prostředky jsou ke spáchání útoku užity.[81] Z toho vyplývá, že i kybernetická operace může být ozbrojeným útokem ve smyslu Charty OSN a

[76] MSD: *Nikaragua*... odst. 119, 212, 228
[77] ROSCINI, Marco. *Cyber Operations and the Use of Force in International Law*. 1. vydání. Oxford University Press, 2014. s. 54
[78] Označení pro osobu, která chce pomocí kybernetické operace dosáhnout změny systému nebo sociálního řádu – více na https://en.wikipedia.org/wiki/Hacktivism
[79] Malware je pojem vzniklý spojení dvou slov – malicious a software. Je užíván jako zastřešující pojem pro počítačové viry, Trojské koně, ransomware, adware a další škodlivé kódy. Více na https://en.wikipedia.org/wiki/Malware
[80] SCHMITT: *Computer Network Attack*.. s. 334 – 337
[81] MSD: *Legalita hrozby*... odst. 39

Ženevských úmluv. K tomuto závěru se kloní též například NATO[82] nebo Nizozemí,[83] ale také další členové mezinárodní komunity.

Manuál chápe kybernetický útok jako kybernetickou operaci učiněnou ať v útoku či obraně, u které lze mít důvodně za to, že způsobí zranění či smrt osob nebo škodu či zničení věci.[84] Definice kybernetického útoku je založena na definici útoku dle čl. 49 odst. 1 Dodatkového protokolu 1 k Ženevským úmluvám. Ten je vymezen užitím násilí proti nepříteli.[85] U obou těchto prvků je třeba posuzovat jejich rozsah a následek. Užití násilí je chápáno ve smyslu způsobených následků nikoliv jen v násilných jednáních jako takových. Příkladem může být poškození ovládacích prvků hasičské ochrany, v jehož důsledku dojde k požáru. Definiční znak „proti nepříteli" nepovažuje Manuál za přesný. Je toho názoru, že o ozbrojený útok se bude jednat také tehdy, pokud bude kybernetická operace s násilnými následky vykonána též proti civilistům. Rozhodující jsou tedy následky způsobené chráněným subjektům.[86] Nezáleží na tom, jaké prostředky jsou užity, jaké je jejich původní určení, ale úmysl s jakým jsou užity a způsobený následek. Užití jakéhokoliv nástroje, které vyústí ve ztráty na životech nebo rozsáhlé škody tedy mohou naplnit kritérium ozbrojeného útoku.[87] Pod toto tvrzení lze jistě stáhnout i malware a kybernetické operace.

Problematika kybernetických útoků se stále vyvíjí a ne vždy státy a odborníci na mezinárodní právo dojdou ke stejnému závěru. Například případ malware Stuxnet, který poničil centrifugy užívané v íránském jaderném programu, část expertů hodnotí jako ozbrojený útok, část měla za to, že této intenzity nebylo dosaženo. Všichni se však shodli na tom, že šlo o užití síly ve smyslu čl. 2 odst. 4 Charty.

1.4 České a evropské právo

V Českém právu je problematika kybernetických útoků upravena zákonem č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon"), vyhláškou č. 316/2014 o kybernetické bezpečnosti (dále jen „vyhláška"), která zákon o kybernetické bezpečnosti provádí a

---

[82] NATO, Deklarace z Waleského summitu. [online]. odst. 72, 5. září 2014 [cit. 7. 4. 2018]. Dostupné na: <https://www.nato.int/cps/ic/natohq/official_texts_112964.htm>

[83] Poradní rada pro mezinárodní záležitosti a poradní komise v oboru mezinárodního práva – společné stanovisko ke kybernetickému válečnictví. *AIV, CAVV Cyber warfare No 77, AIV/No 22, CAVV*. Prosinec 2011 [cit. 7. 4. 2018]. Dostupné na: <https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf> s. 23

[84] SCHMITT: *Tallinn Manual 2.0*... pravidlo 92

[85] Dodatkový protokol k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí mezinárodních ozbrojených konfliktů (Protokol 1), čl. 49

[86] SCHMITT: Tallinn Manual 2.0... s. 417

[87] ZEMANEK, Karl. *Armed Attack*. *Encyklopedie* mezinárodního práva Maxe Plancka. [online]. Mezinárodní encyklopedie Maxe Plancka, říjen 2013 [cit. 8. 4. 2018]. Dostupné na <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241>

dalšími předpisy, které se problematiky nepřímo týkají.[88] Zákon a vyhláška pracují s pojmy kybernetická bezpečnostní událost a kybernetický bezpečnostní incident.[89] Jako kybernetická bezpečnostní událost [90]je chápána událost, která může narušit bezpečnost informací v bezpečnostních systémech nebo bezpečnost služeb anebo bezpečnost a integritu sítí elektronických komunikací. Kybernetický bezpečnostní incident [91]je kybernetická bezpečnostní událost, která způsobila narušení chráněných objektů. S KBU se pojí povinnost detekovat,[92] zato KBI je nutno hlásit CERTu.[93] Vyhláška třídí kybernetické incidenty z hlediska jejich technického provedení. Jsou uvedeny průniky do systému, užití škodlivých kódů či překonání technických opatření.

Domnívám se, že vymezení pojmu KBI, byl zvolen proto, že dané objekty je možno narušit širokou paletou různých aktivit. Například je možné se do určitého počítačového systému dostat vzdáleně pomocí internetu. Typicky za předpokladu získání přihlašovacích údajů jednotlivých uživatelů. Tento způsob je materiálně chápán jako kybernetický útok.[94] Do počítačového systému je však možné se dostat i tak, že pachatel jako zaměstnanec získá fyzický přístup k serveru, kde jsou dané informace uloženy a zkopíruje je z/na flash disk. Tím může poškodit cílový systém nebo z něj naopak vynést cenná data.[95]

Fiktivním případem může být napadení ovládacích systémů přehrady a otevření jejich stavidel za účelem zaplavení datového centra v městě pod ní. Toho je možno dosáhnout mnoha způsoby včetně dvou výše uvedených. Pojem KBI na tomto místě kryje veškeré eventuality. Tím, že je KBI definována pomocí způsobených následků a nikoliv pouze prostředků užití tak kromě jednání třetích osob kryje i *vis maior* v podobě živelních pohrom.

Evropská úprava v podobě směrnic, které nejčastěji řeší problematiku kybernetických útoků, je transponována do českého právního řádu ve výše uvedených zákonech a vyhláškách. Některé instituty uvedené v evropské úpravě nejsou transponovány doslovně, a proto zmíním ty, které mohou mít vliv na lepší pochopení obsahu pojmu kybernetický útok tak, jak jej vnímá EU.

---

[88] Zákon č. 240/2000 Sb., krizový zákon, ve znění pozdějších předpisů, který definuje pojem kritické infrastruktury, Nařízení vlády č. 432/2010 Sb., Nařízení vlády o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů, které stanovuje kritéria pro určení kritické infrastruktury. Dále vyhláška č. 317/2014 sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů, která v návaznosti na předchozí zákon a vyhlášku stanoví, co jsou významné informační systémy a jaká jsou jejich určující kritéria.
[89] Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti, ve znění pozdějších předpisů, § 7
[90] Dále jen „KBÚ".
[91] Dále jen „KBI".
[92] Zákon č. 181/2014 Sb. § 7 odst. 3
[93] Zákon č. 181/2014 Sb. § 8
[94] Tzv. spear phishing
[95] V IT komunitě se tyto činy označují jako insider attack.

Směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii[96], která byla do zákona o kybernetické bezpečnosti transponována s účinností od 1. 1. 2018, vymezuje jako chráněné subjekty provozovatele základních služeb a poskytovatele digitálních služeb. Provozovatelem základních služeb směrnice chápe veřejnoprávní i soukromoprávní subjekty, které poskytují služby považované za základní z hlediska zachování kritických společenských nebo ekonomických činností s tím, že poskytování dané služby je závislé na sítích a informačních systémech.[97] Směrnice subjekty chrání před významným narušením poskytování služeb. Pro určení, zda se jedná o významné narušení, je nezbytné brát v potaz počet uživatelů služby, závislost dalších odvětví na této službě, možný dopad incidentů na ekonomické a společenské činnosti či veřejnou bezpečnost, podíl daného subjektu na trhu a důležitost subjektu s přihlédnutím k alternativám.[98] Druhy digitálních služeb je dle přílohy III ke směrnici on-line tržiště, internetový vyhledávač a služba cloud computingu. Směrnice tímto rozšiřuje počet chráněných subjektů. Nově jsou chráněny i subjekty, které jsou více relevantní z běžného uživatelského hlediska.

Přestože české a evropské právo není relevantním zdrojem z hlediska mezinárodního práva, považuji za vhodné je do své diplomové práce zařadit. Zmíněné české a o to více evropské předpisy, kterou jsou uváděny, jsou totiž produktem mezinárodní organizace svého druhu – Evropské unie. Česká právní úprava transponuje různé vyhlášky, které jsou následně promítány do znění zákona o kybernetické bezpečnosti a dalších předpisů, které se kyberprostoru věnují. Nejedná se tedy o čistě partikulární úpravu vytvořenou jedním státem, ale o úpravu, která reprezentuju názor širší skupiny států – Evropské unie. Mezinárodní právo veřejné problematiku kybernetických útoků dostatečně neřeší. V této situaci mi přijde vhodné, využít unifikující snahy jako možnou inspiraci pro mezinárodní právo. V budoucnu může dojít k inspiraci ohledně jednotlivých aspektů problematiky kyberprostoru, do takové míry, že dojde k dohodě, se kterou bude souhlasit celé či určitá část mezinárodního společenství.

1.5 Shrnutí kapitoly

V této kapitole jsem se zabýval otázkou, jak mezinárodní právo chápe technický pojem kybernetický útok. Vzhledem k tomu, že samo MPV problematiku kybernetického prostoru neupravuje a termín kybernetického útoku není definován ve smlouvách ani v mezinárodních obyčejích bylo třeba vycházet z jiných zdrojů. Bylo naznačeno, jak definují kybernetický útok

[96] Směrnice Evropského parlamentu a Rady (EU) 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii
[97] Vyhláška č. 316/2014 Sb. čl. 5
[98] Vyhláška č. 316/2014 Sb. Čl. 6

světově renomované instituce, jejichž názor však pro MPV není autoritou, jak problematiku kybernetického útoku řeší publikace, kterou lze v této oblasti považovat za nejautoritativnější – Tallinnský manuál a na závěr jak se k problematice staví evropská a česká právní úprava.

Kvůli mnohosti způsobů spáchání, forem jednání a možných následků se mi pro účely MPV jeví jako nejrozumnější způsob regulace, který zvolil Tallinnský manuál. Kybernetický útok, tak jak jej chápeme v technickém smyslu, nedefinuje, ale dle výše zmíněných kritérií jej podřazuje pod porušení různých norem mezinárodního práva. Kybernetickým útokem tedy může být jak zasaženo do státní suverenity či jeho vnitřních záležitostí tak jím může být spáchán ozbrojený útok. Úprava evropského a českého práva oproti Manuálu konkrétně vymezuje chráněné objekty a poměrně široce způsoby, jak je do nich možno zasáhnout. Mezi tyto způsoby řadí i kybernetický incident, který lze pojmově zařadit pod kybernetický útok v technickém smyslu.

2. Odpovědnost států v mezinárodním právu

2.1 Úvod a odpovědnost v mezinárodním právu

Odpovědnost v právu je chápána jako nutnost nést důsledky za nějaké konání či opomenutí. Jedním z druhů odpovědnosti státu v mezinárodním právu veřejném je odpovědnost vzniklá protiprávním jednáním a zaviněním. Jde o postih za jednání či opomenutí, kterým je porušena norma či zvyklost. Odpovědnost, jako následek porušení právní normy, existuje v mezinárodním právu již velice dlouho.

V tradičním mezinárodním právu se za odpovědnost považovala vlastnost státu spočívající ve způsobilosti plnit, co je mu uloženo mezinárodněprávními normami.[99] Do těchto vztahů spolu mohly vstupovat pouze státy, které se navzájem uznávaly jako subjekty mezinárodního práva. Respektive vůči státu neuznanému nevznikaly právní závazky, ve vzájemném vztahu působila faktická volnost.

Problematiku lze demonstrovat na případu ozbrojeného konfliktu mezi dvěma státy. Po ukončení konfliktu chtěly státy narovnat vzájemné závazkové vztahy. Dosáhnout obnovení právního vztahu vyžadovalo odčinit újmu způsobenou deliktem – ozbrojeným konfliktem. Projevem tedy mohla být situace, kdy došlo k ukončení válečného konfliktu mezi státy a následnému uzavření smluv o reparaci. Typicky byla poražená strana nucena k reparacím vůči vítězi. Mohlo však dojít i k situaci, kdy jeden ze států nebyl jako stát, tedy subjekt mezinárodního práva, uznán. V důsledku to znamenalo nemožnost s ním smlouvu o reparaci uzavřít. V případě, že byly oba státy považovány za subjekty mezinárodního práva, stále záleželo na vůli obou států, zda k reparaci dojde. Pokud došlo k uzavření smlouvy o reparaci, vznikl mezi státy nový závazek a došlo k narovnání vzájemných vztahů. Pokud však ani tento nový závazek nebyl splněn, mohl stát, vůči němuž nebyl závazek splněn, znovu zvážit postup proti povinnému. Například mohl opětovně rozpoutat válečný konflikt.

V době tradičního mezinárodního práva převládala faktická volnost v chování vůči neuznanému státu i vůči státu uznanému v případě, že se škůdce rozhodl, že smlouvu o narovnání dodržovat či uzavírat nebude.[100]

Postupem času se do institutu mezinárodní odpovědnosti začala promítat rozhodnutí z arbitrážní praxe v Evropě během období míru na konci 19. a počátku 20. století. Šlo o

[99] FAIX, Martin, BUREŠ, Pavel, SVAČEK, Ondřej. *Rukověť ke studiu mezinárodního práva 1: Dokumenty*. Praha: Leges. 2015, s. 325
[100] Tamtéž

rozhodnutí, která směřovala k ochraně investic v jednotlivých zemích. Ačkoliv se nejednalo o spory, kde byl předmětem sporu vztah mezi státy, docházelo zde k zakotvení zvyklostí, které byly následně přebírány do mezinárodního práva veřejného. První rozsudek, který se věnoval odpovědnosti států v mezinárodním právu, byl rozsudek ve věci *Továrny Chorzow*.[101] V něm bylo řečeno, že porušení práva s sebou nese povinnost reparace v příslušné formě. Dle soudu jde o princip vlastní mezinárodnímu právu.[102]

Došlo tedy k posunu od tradičního mezinárodního práva v tom smyslu, že reparační povinnost vznikla škůdci *ex lege*. Nemuselo již docházet k uzavírání smluv o reparaci a ponechávat možnost smlouvu uzavřít na vůli států.

I přes tento a navazující rozsudky je však odpovědnost a náhrada škody v mezinárodním právu problematická. Horizontální a decentralizovaný systém, kde jsou jeho účastníci zároveň tvůrci a adresáti norem, neposkytuje vhodné podmínky k vytvoření jednotných a jasných pravidel systému sankcí za porušení norem mezinárodního práva. Společenství suverénů – států, které nemá nadřazenou autoritu, není možné trestat obdobně jako osoby v právu národním. Státy neuzavřely společenskou smlouvu a nemají mezi sebou někoho, kdo má monopol na násilí. Státy jsou si rovny.

2.2 Návrh článků o odpovědnosti států

Problematikou mezinárodněprávní odpovědnosti se dlouhodobě zabývá Komise OSN pro mezinárodní právo. Od ní pochází Návrh článku o odpovědnosti států,[103] dokument, který zachycuje obyčejové právo v oblasti odpovědnosti států za mezinárodní protiprávní chování. Ačkoliv původně zamýšlen jako mezinárodní smlouva, komise z obavy, že by nebyl přijat dostatečným počtem států a tím by byl zpochybněn jeho obyčejový základ, doporučila Valnému shromáždění OSN, aby jej vzalo na vědomí, které tak učinilo.[104] Na tomto místě je nutno zdůraznit, že se Návrh zabývá toliko odpovědností států. Odpovědnost dalších subjektů mezinárodního práva zachycena v tomto dokumentu není a je možno o ní uvažovat v obyčejové rovině.[105] Příkladem je Návrh článků o mezinárodní odpovědnosti mezinárodních organizací za

[101] Stálý dvůr mezinárodní spravedlnosti: Rozsudek ze dne 26. července 1927, *Případ továrny v Chorzowě*
[102] SDMS. *Továrna v Chorzowě*, s. 21
[103] Komise pro mezinárodní právo. *Návrh článků o odpovědnosti státu za mezinárodně protiprávní chování*. 2001. Dostupné na: <http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf>
[104] Rezoluce Valného shromáždění OSN. *A/Res/56/83 o odpovědnosti států za mezinárodně protiprávní chování.*
[105] KMP. *Návrh článků*... čl. 57, čl. 58

mezinárodně protiprávní chování. Zároveň je v kapitole čerpáno z Manuálu. Ten sám uvádí, že čerpá z Návrhu a jeho ustanovení aplikuje na kybernetické prostředí. [106]

Návrh se v první části zabývá zakotvením základních principů mezinárodněprávní odpovědnosti, konstituováním toho, co je chápáno pod pojmem mezinárodně protiprávní akt, přičitatelností protiprávních aktů a okolnostmi vylučujícími protiprávnost. V části druhé pak Návrh rozebírá následky porušení normy jako sekundární povinnost. Třetí část se zabývá procesními aspekty uplatňování náhrady škody a čtvrtá obsahuje obecná ustanovení.

2.2.1. Obecné zásady

První tři články Návrhu zakotvují obecné zásady, na kterých je přičitatelnost vystavěna. Zásady jsou následující: Každé mezinárodně protiprávní chování státu má za následek mezinárodně právní odpovědnost tohoto státu.[107] O mezinárodně protiprávní chování státu se jedná, jestliže chování spočívající v jednání nebo opomenutí je státu podle mezinárodního práva přičitatelné a představuje porušení mezinárodního závazku státu.[108] Označení chování za mezinárodně protiprávní se řídí mezinárodním právem. Tato charakteristika není dotčena charakteristikou stejného chování jako legálního podle vnitrostátního práva.[109]

Z úvodních článků vyplývají dva prvky mezinárodně protiprávního chování. Objektivní prvek v podobě porušení mezinárodně právní povinnosti a subjektivní prvek, kterým je přičitatelnost jednání státu. K porušení mezinárodně protiprávní povinnosti musí být naplněny oba prvky.[110] Není tedy možné konstatovat, že došlo k porušení, aniž dojde k přičtení.

Na těchto základních zásadách je vystavěn zbytek Návrhu článků. Je stanoven objektivní prvek v podobě porušení mezinárodního závazku a subjektivní prvek v podobě přičitatelnosti chování státu. Bez naplnění těchto dvou prvků nedojde k mezinárodně protiprávnímu chování. Z ustanovení vyplývá nemožnost státu hájit chování státu argumentem, že dle jeho národního práva je chování dovoleno. Národní právo v této otázce není relevantní. Kdyby tomu tak nebylo, mohlo by to vést k absurdním situacím. Dle národního práva státu by bylo legální obsazovat území a zasahovat do suverenity cizích států a mezinárodní společenství by tento fakt muselo respektovat. Nešlo by totiž o porušení norem. Něco, co tvoří základ mezinárodního práva veřejného, by tedy bylo možno porušit na základě usnesení národního zákonodárce.

---

[106] SCHMITT: *Tallinn Manual 2.0*... s. 79
[107] FAIX. *Rukověť*... s. 298
[108] KMP. Návrh článků... čl. 2
[109] KMP. Návrh článků.... čl. 3
[110] Situaci, kdy nedojde k naplnění objektivního prvku, teorie mezinárodního práva označuje, jako málo přátelský akt. Případy nedostatku subjektivního prvku teorie mezinárodního práva ze své podstaty neřeší.

Manuál tato úvodní ustanovení odráží tak, že stát nese odpovědnost za chování související s kybernetickými operacemi, které jsou přičitatelné státu a které představuje porušení mezinárodního závazku státu.[111] Pojem chování související s kybernetickými útoky má zahrnovat jak kybernetické operace, tak i jiná chování. Například situace, kdy stát poskytne svou kybernetickou infrastrukturu skupině hackerů a ta ji využije ke spáchání kybernetické operace.

2.2.2. Porušení mezinárodního závazku – objektivní prvek

Porušení mezinárodního závazku je objektivním prvkem mezinárodní odpovědnosti. Jde o volní chování státu jako subjektu mezinárodního práva, které je v rozporu s jeho mezinárodními závazky a tím vyvolává právní následky. Není důležitý původ nebo charakter porušovaného závazku.[112] Chování státu nezakládá porušení mezinárodního závazku, pokud stát není vázán tímto závazkem v době, kdy k danému chování došlo.[113] Porušení mezinárodněprávního závazku státem, které nemá pokračující charakter, se časově vztahuje k okamžiku uskutečnění jednání. V případech pokračujícího charakteru chování, se za dobu spáchání považuje celá doba, po kterou není chování státu v souladu se závazkem. Je-li povinností státu zabránit protiprávní události, je za dobu spáchání považována doba, počínající okamžikem zahájení události a trvající až do okamžiku, kdy událost přestane být v rozporu s mezinárodním právem veřejným.[114] V takovém případě se za počátek protiprávního jednání považuje první ze série jednání či opomenutí a trvá tak dlouho, dokud se jednání opakují a nejsou v souladu s mezinárodními závazky státu.[115]

Z hlediska doby spáchání je zajímavý údajný případ kybernetické operace, kterou Ruská federace měla ovlivnit volby amerického prezidenta v roce 2016, cílící na Demokratický národní výbor. Samotné volby se odehrávaly 8. listopadu 2016. Zpravodajské agentury však již v září 2015 upozornily výbor, že nejméně jeden z jejich počítačů byl ruskými hackery napaden. Ke zveřejnění téměř 20.000 emailů došlo 22. července 2016, několik dní před shromážděním demokratické strany. Emaily byly zveřejněny na stránce wikileaks[116] a jejich obsah vyznívá negativně pro kandidátku na prezidenta za Demokratickou stranu Hillary Clinton. Pro určení období porušení mezinárodního práva je nezbytné určit, porušení jaké normy je v daném chování spatřováno. Pokud budeme uvažovat o zasahování do vnitřních záležitostí státu pomocí kybernetické operace, tak uvažujeme

[111] SCHMITT: *Tallinn Manual 2.0*... pravidlo 14
[112] KMP. *Návrh článků*... Čl. 11
[113] KMP. *Návrh článků*... Čl. 13
[114] KMP. *Návrh článků*... Čl. 14
[115] KMP. *Návrh článků*... Čl. 15
[116] *Wikileaks email database*. [online] Wikileaks.org, [cit. 14. 4. 2018] Dostupné na <https://wikileaks.org/dnc-emails/>

o časovém úseku od září 2015 či ještě dříve, kdy došlo k průniku do systému až do doby, než se podařilo v přístupu do systému zabránit. Datum není veřejně známo, ale bude následovat po 22. červenci 2016, dni, kdy byly emaily zveřejněny.

Manuál k objektivnímu prvku přičitatelnosti poznamenává, že je třeba jej vykládat restriktivně. Stát nebude odpovědný za chování přímo dovolené nebo mezinárodním právem neregulované.[117] Špionáž pomocí kybernetických prostředků, kterou Manuál chápe jako institut neporušující obyčejové právo, tedy nebude možno postihnout. Mezinárodní soudní dvůr poznamenal, že "je zcela možné, aby určitý čin ... nebyl porušením mezinárodního práva, aniž by nezbytně představoval výkon práva, které mu bylo svěřeno".[118] Manuál však zároveň uvádí, že špionáží může dojít k porušení jiných norem mezinárodního práva, především zásahu do státní suverenity a vměšování se do vnitřních záležitostí státu.[119]

2.2.3. Subjekt a přičitatelnost mezinárodně protiprávního chování – subjektivní prvek

Subjektivním prvkem mezinárodně protiprávního chování je přičtení tohoto chování státu. Druhá kapitola první části Návrhu článků upravuje podmínky, za kterých je možné státu jednání přičíst. Jsou zde především vyjmenovány subjekty, za jejichž jednání je stát odpovědný a podmínky, za nichž je přičtení možné.

Chování jakéhokoliv státního orgánu se považuje za chování tohoto státu podle mezinárodního práva, ať již tento orgán vykonává legislativní, výkonné, soudní nebo jiné funkce, má jakýkoliv charakter, jde o orgán centrální vlády nebo územní jednotky státu. Orgán zahrnuje jakoukoliv osobu nebo entitu, která má tento status v souladu s vnitrostátním právem.[120] Pojem orgán je v tomto případě nutno chápat v širokém slova smyslu. Nezáleží na druhu orgánu, zařazení, funkci či hierarchii orgánu.[121] Chování osoby nebo entity, které Návrh článku za orgány státu nepovažuje, ale jsou zmocněny právem tohoto státu k výkonu prvků státní moci, se považuje za chování státu podle mezinárodního práva, za předpokladu, že osoba nebo entita jednají v daném případě jako orgány státu.[122] Dle Návrhu článků jde o polostátní orgány, které vykonávají prvky vládní moci a bývalé státní podniky, které byly zprivatizovány, ale zůstala jim

[117] SCHMITT: *Tallinn Manual 2.0*... s. 85
[118] Mezinárodní soudní dvůr: Poradní posudek ze dne 22. července 2010, *Soulad prohlášení Kosovské nezávislosti s mezinárodním právem.*
[119] SCHMITT: Tallinn Manual 2.0... s. 170
[120] *KMP. Návrh článků*... Čl. 4
[121] Zpráva Komise pro mezinárodní právo, dokument A/56/10 ze dne 23. dubna - 1. června a 2. července - 10. srpna 2001; s. 40
[122] KMP. Návrh článků... Čl. 5

určitá část veřejných funkcí.[123] V kontextu kybernetických útoků může jít například o CERT týmy, které jsou pověřeny k reakcím na kybernetické útoky.

Manuál uvádí, že není možné se vyhýbat mezinárodní odpovědnosti upíráním entitě statusu státního orgánu.[124] Obdobný názor zastal také MSD, kdy v případě *Genocidy* vyslovil, že pro odpovědnostní účely mohou být osoby nebo skupiny osob považovány za státní orgány, pokud jsou plně závislé na státu a fungují jako jeho nástroj. V takových případech je vhodné se zaměřit nad rámec práva na skutečný vztah státu a osob, které jednání vykonaly.[125]

Chování orgánu státu nebo osoby či entity zmocněné k výkonu prvků státní moci se považuje za chování státu podle mezinárodního práva, pokud orgán, osoba nebo entita jednají jako státní orgány, dokonce i kdyby překročily své pravomoci nebo jednaly v rozporu se služebními příkazy.[126] Jde o případy jednání *ultra vires*, za které je stát odpovědný tehdy, pokud se jednající dopustil protiprávního činu v souvislosti se svým postavením garantovaným mu státem. Není možné, aby stát mezinárodně protiprávní chování hájil argumentem, že dle ustanovení národního práva nebo udělených instrukcí k tomuto chování nemělo dojít anebo k němu mělo dojít jiným způsobem.[127] Klíčové při užití této normy pro přičtení chování státu je určení, jestli osoba jednala ještě v rámci svěřených pravomocí nebo už mimo ně. Ve druhém případě se chování považuje za tak vzdálené od obsahu jejich funkce, že není možné je státu přičíst. Otázkou tedy zjednodušeně je, jestli bylo chování vykonáno osobami chráněnými vládní autoritou. Rozlišení, jestli je jednáno ve státních záležitostech či ne vychází z toho, jak působí jednání dané osoby či orgánu navenek. Chová-li se osoba, jakoby užívala své postavení svěřené jí státem, bude její jednání státu přičitatelné.[128] Test pro posouzení, zda se jedná o chování osoby přičitatelné státu či nikoliv byl ustaven v případu *Mallén*, kdy zástupce šerifa dvakrát napadl mexického konzula. Poprvé jako soukromá osoba, podruhé jako státní orgán. Jedním z důvodů pro posouzení druhého útoku jako přičitatelného státu bylo mimo jiné to, že osoba, jejíž jednání bylo státu přičteno, zavřela oběť do cely, která sloužila k zadržování zločinců. Protože státy mají

[123] Zpráva Komise pro mezinárodní právo, dokument A/56/10 ze dne 23. dubna - 1. června a 2. července - 10. srpna 2001; s. 42
[124] SCHMITT: *Tallinn Manual 2.0*... s. 88
[125] Mezinárodní soudní dvůr: Rozsudek ze dne 26. února 2007, *Případ zabývající se aplikací Úmluvy o prevenci a trestání zločinu genocidy*. Odst. 392
[126] *KMP. Návrh článků*.... čl. 7
[127] Komise A/56/10... s. 45
[128] Komise A/56/10... s. 42

na svém území svrchovanou moc a monopol na násilí došlo tímto k jednání, které je za běžných okolností předmětem výkonu státní moci.[129]

V případě, že bude stát napaden kybernetickou operací, bude jeho prvotní reakcí uvést do pohotovosti CERT, který bude na kybernetickou operaci reagovat. Proběhne analýza typu útoku, zasažených systémů a shromáždění informací o původci operace. Předběžné výsledky technické analýzy budou nasvědčovat tomu, že původcem operace je sousední stát. Tyto závěry budou navíc podpořeny zprávami bezpečnostních složek, které budou upozorňovat na zvýšené riziko kybernetických operací ze strany sousedního státu. Vedoucí CERTu přesto přikáže pokračovat v analýze. V okamžiku, kdy jeden z pracovníků CERTu bude jednat v rozporu s příkazy a na vlastní pěst se sám pokusí získat přístup do systému sousedního státu, aby zjistil, jestli ten stojí za kybernetickou operací, dojde k porušení mezinárodních závazků, které bude přičitatelné původně napadenému státu.

Jedním z dříve užívaných způsobů, jak chování přičíst státu bylo zjistit, užitím jakých prostředků k porušení mezinárodního závazku došlo. Typicky armádní vybavení, jako jsou tankové divize či letadlové lodě, můžeme považovat za prostředky, kterými jiné entity než státy nedisponují. V případě užití těchto prostředků se dá předpokládat, že to byly orgány státu, které svým chování porušily mezinárodní právo. Obdobná analogie u kybernetických operací není tak jednoduchá. Je možné, aby kybernetické operace byly vedeny přes kybernetické infrastruktury jiných států a cíleně v nich zanechávaly stopy například v podobě zpět odesílaných logů. Obdobné skutečnosti nejsou dostatečným důkazem k tomu, aby bylo na jejich základě jednání státu přičteno, nicméně je to indikací, že stát může být s kybernetickou operací spojen. Situace, kdy stopy ukazují ke kybernetickým infrastrukturám vlastněným soukromými osobami, jsou v tomto ohledu ještě méně vypovídající.[130] Navíc cena, za kterou je možno realizovat kybernetický útok, je neporovnatelně nižší s cenou pořízení letadlové lodě. Na *deep web*[131] je možné DDoS útoky pořídit od pár desítek dolarů.[132]

Přičitatelnost dále komplikují technické možnosti kyberprostoru v podobě tzv. *spoofingu*. Jeho cílem je zastření vlastní identity při vykonání kybernetických operací a jejich přesměrování

[129] Stálý soud mezinárodní spravedlnosti: Rozsudek ze dne 27. dubna 1927, *Francisco Mallén proti Spojeným státům Americkým*. s. 174 - 177
[130] SCHMITT: Tallinn Manual 2.0... s 91
[131] Deep web je termín označující neindexované internetové stránky. To znamená, že „nejsou viditelné" pro internetové vyhledávače. K těmto stránkám se typicky přistupuje zadáním URL nebo IP adresy, kterou uživatel předem zná.
[132] MARKUSHIN, Denis. *Cena DDoS útoku* [online]. Securelist.com, 23. března 2017. [cit. 27. 3. 2018]. Dostupné na <https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/>

skrz jiné uživatele s cílem přimět oběť aby uvěřila, že proti ní kybernetickou operaci vede jiná osoba, či jí odradila od náročného postupu při zjišťování, kdo útok původně vykonal. To je případ, který nastal mezi NATO CCD COE[133] a Ukrajinou. Ukrajinské vládní weby byly zasaženy kybernetickou operací, která měla vyvolat dojem, že jsou od tohoto think-tanku. Jeho web spolu s weby Estonských bezpečnostních sil a některých zemí NATO byly zase zasaženy kybernetickou operací, která měla vyvolat dojem, že autorem je Ukrajina.[134] Pomocí těchto technik je možné manipulovat názory a vztahy v mezinárodním prostředí tak, jako dříve ne. Každá takováto operace musí být hodnocena v kontextu. K přičtení mohou sloužit informace získané od zpravodajských služeb nebo vzájemné vztahy států, které jsou domnělými stranami útoku.[135] Samotná identifikace zařízení, ze kterého přišel útok, napadající cílový počítač tedy nemusí mít ani z technického hlediska žádnou váhu, pokud nám není umožněn přístup k tomuto zařízení a analýza jeho logů. Pomocí *spoofingu* může dojít k několikerému přesměrování a námi identifikované zařízení může být pouze poslední v řadě. V případě, kdy je nad kybernetickou infrastrukturou státu, před tím, než je z ní vykonána kybernetická operace, převzata kontrola nevládní skupinou, je třeba být s přičtením jednání státu obezřetný ještě více.

Chování orgánu daného k dispozici státu jiným státem se považuje za chování prvého státu podle mezinárodního práva, pokud tento orgán jedná při výkonu prvků státní moci toho státu, jemuž byl dán k dispozici.[136] Návrh článků upřesňuje, že k přičtení je v tomto případě třeba kontroly orgánu výhradně přijímajícím státem a chování je vykonáno jménem a pouze v zájmu přijímajícího státu. Typickým příkladem je poskytnutí záchranných či pořádkových jednotek při přírodních katastrofách. Vysílající stát v takových případech svěří své jednotky do pravomoci státu přijímajícího a ten je následně odpovědný za jejich chování. Přijímajícímu státu jsou přičitatelná i jednání *ultra vires*. Z hlediska kybernetických operací lze uvažovat o situaci, kdy je provedena kybernetická operace proti více státům. Tato skupina států nebude technicky vyspělá a budou mít uzavřenou smlouvu s třetím státem, který jim poskytne služby svého CERT. Tento bude pod kontrolou pouze jednoho ze skupiny napadených států. V případě, že na kybernetickou operaci bude tento CERT reagovat a v průběhu poruší mezinárodní právo vlastní kybernetickou operací, bude tato přičitatelná pouze státu, kterého daný CERT ovládá.

Chování osoby nebo skupiny se považuje za chování státu podle mezinárodního práva, pokud osoba nebo skupina osob ve skutečnosti jednají podle pokynů státu, nebo je jejich chování

[133] Think-tank jež organizoval práce na Tallinnském manuálu
[134] SCHMITT: Tallinn Manual 2.0... s. 92
[135] Tamtéž
[136] *KMP. Návrh článků...* Čl. 7

tímto státem řízeno nebo kontrolováno.[137] Pro přičtení je vyžadována existence faktického spojení mezi osobami vykonávajícími chování a státem. Osoby soukromého práva jednají buď podle pokynů státu, nebo je jejich chování řízeno či kontrolováno státem. Pro přičtení je vyžadováno skutečné pouto mezi osobami a státem. Pokud je prokázána existence tohoto pouta, není důležité, že osoba není součástí vládní struktury, ani jestli je její chování považováno za výkon vládní aktivity.[138] Od těchto případů jsou v Návrhu článků odlišeny situace zakotvené v článku 17, kdy jednání vykoná stát pod nátlakem jiného státu. V tomto případě je za porušení mezinárodního práva po prokázání řízení a kontroly odpovědný stát donucující. Návrh v komentáři k tomuto článku upřesňuje, že o jednání dle pokynů nejčastěji půjde v případech, kdy stát neužije k dosažení svých cílů vlastních kapacit, ale pomůže si najmutím či podněcováním osob soukromého práva jako pomocného personálu které zůstávají mimo vládní struktury. Tyto osoby, které nejsou oficiálně součástí státu, jsou najatými prostředníky a vykonají své úkoly jako "dobrovolníci". Jsem toho názoru, že toto bude častý případ u kybernetických operací.

V IT komunitě vešlo ve známost několik skupin hackerů, které jsou spojovány s konkrétními státy, které jim dle dostupných zdrojů poskytují podporu a využívají jejich služeb. Americká technologická společnost *Crowdstrike* například zmiňuje skupiny *Cozy bear* a *Fancy bear*, které spolupracují s Ruskou federací.[139] Ke stejným závěrům došla i Nizozemská tajná služba AIVD.[140]

V případech řízení a kontroly bude státu přičitatelné pouze takové chování, které je součástí větší operace řízené či kontrolované státem. Za chování státu se nebude považovat chování, které bylo spojeno s operací náhodou či omylem.[141] Tato norma zaštituje například chování armádních struktur, které se na kybernetické operace specializují. Je známo, že například Čína či Spojené státy americké takovými jednotkami disponují.[142] Dle mého názoru budou dnes

---

[137] *KMP. Návrh článků...* Čl. 8
[138] Komise A/56/10... s. 47
[139] ALPEROVITCH, Dimitri. *Medvědi vprostřed: Průnik do Demokratického národního* výboru [online]. Crowdstrike.com, 15. června 2016 [cit. 27. 3. 2018]. Dostupné na <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>
[140] MODDERKOLK, Huib. *Holandské zpravodajské agentury poskytly důležité zprávy o ruském vměšování se do amerických* voleb [online]. Volkskrant.nl, 25. ledna 2018 [cit. 27. 3. 2018]. Dostupné na <https://www.volkskrant.nl/tech/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~a4561913/>
[141] Komise A/56/10... s. 48
[142] *Cyber force* [online]. Wikipedia.org, [cit. 27. 3. 2018] Dostupné na <https://en.wikipedia.org/wiki/Cyber_force>

státy, které jednotky zaměřené na kybernetickou doménu boje mít nebudou, spíše výjimkou. Do roku 2025 plánuje mít tuto jednotku také AČR[143]

Problematikou přičtení jednání skupiny osob státu se věnoval MSD v případě *Nikaragua*. MSD shledal, že Spojené státy financovaly, organizovaly, vycvičily, zásobovaly a vybavily jednotky *contras*.[144] Mezinárodní soudní dvůr shledal, že Spojené státy tímto jednáním nedosáhly efektivní kontroly. Pouze v několika málo případech bylo shledáno, že by Spojené státy přímo "kontrolovaly" *contras* a jejich chování. Mezinárodní soud tedy konstatoval, že nebyla prokázána existence skutečného pouta – tzv. efektivní kontroly a tudíž nedošlo k přičtení jednání *contras* Spojeným státům.[145] Soud v případu *Tadić* konstatoval, že si je vědom, že pro přičtení chování se vyžaduje efektivní kontrola chování subjektu. Zároveň ale uvedl, že nevidí důvod, aby nebyl použit jiný než nejpřísnější přístup k přičitatelnosti.[146] Soud se odchýlil od ustálené praxe a shledal, že v tomto případě postačí celková kontrola, přesahující financování a poskytování zásob zahrnující též účast při plánování a dohled nad vojenskými operacemi.[147] Je ale nutno poznamenat dvě věci. Pravomoc soudu v tomto případě směřovala k vyslovení trestní odpovědnosti jednotlivce, nikoliv odpovědnosti státu a vůči žalovanému subjektu bylo konstatováno nikoliv přičtení protiprávního chování, ale možnost užití norem humanitárního práva.[148] Mezinárodní komise uzavírá, že každý případ je nutno posuzovat individuálně. Především je nutné se zaměřit na vztah mezi udělenými pokyny nebo řízením a kontrolou a předmětným chováním.[149] Pod čl. 8 je zahnuto jednání jak fyzických a právnických osob tak skupin osob, které nemají *de iure* právní osobnost ale jednají na *de facto* bázi.[150]

Manuál za efektivní kontrolu považuje situaci, kdy stát určuje, kdy dojde k vykonání kybernetické operace, která je součástí většího celku aktivit.[151] Pod efektivní kontrolu spadá možnost nařídit jak začátek operace, tak ukončení operace probíhající. Příkladem může být situace, kdy stát ovlivní technologickou společnost dodávající software cílovému státu, aby do následujícího softwarového update vložila takovou část kódu, která umožní prvnímu státu přístup do těchto systémů. Naopak do efektivní kontroly nespadá pouhá podpora skupin. Poskytnutí

[143] Ministerstvo, obrany. Koncepce výstavby armády České republiky 2025. Str. 11;] Dostupné na: <http://www.mocr.army.cz/images/id_40001_50000/46088/KVA__R_ve__ejn___verze.pdf>
[144] Contras bylo seskupení odporu proti Sandinovské frontě národního osvobození. Tyto strany se spolu střetly o moc po Sandinistické revoluci v roce 1979.
[145] MSD: *Nikaragua*... odst. 86, 109, 115, 212
[146] Mezinárodní trestní tribunál pro bývalou Jugoslávii: Rozsudek ze dne 15. července 1999, *Žalobce proti Duško Tadićovi*. odst. 117
[147] MTTJ. *Tadić*... odst. 145
[148] Komise A/56/10... s. 48
[149] Komise A/56/10... s. 48
[150] Komise A/56/10.... s. 49
[151] SCHMITT: Tallinn Manual 2.0... s. 96

malware k páchání libovolných útoků tedy nezakládá možnost útoky přičíst státu. Z rozsudku MSD vyplývá, že takto není přičitatelné ani financování, organizace, trénink, zásobování a poskytování vybavení jednotlivci či skupině.[152]

Státu je též přičitatelné chování osob, které *de facto* vykonávají prvky státní moci v době, kdy stát nemá oficiální vládu či je nepřítomna.[153] Jedná se o ojedinělé případy revolucí, ozbrojených konfliktů či zahraničních okupací. Jednání povstaleckých hnutí, která se stanou novou vládou, jsou přičitatelné státu, v němž se staly vládou. V případě že se povstaleckému hnutí podaří rozdělit teritorium a založit svůj stát, či obnovit stát předchozí, přičítá se toto jednání tomuto vzniklému státu. Tímto článkem nejsou dotčena pravidla přičitatelnosti chování státu původního státu, která spadají pod čl. 4 a 9.[154]

Chování, která nelze přičíst státu podle předchozích článků, se nicméně považuje za chování tohoto státu podle mezinárodního práva, a to v rozsahu, v jakém tento stát uzná a přijme chování za své vlastní.[155] Předchozí články počítají s tím, že je to stát, kdo dal k chování prvotní impulz, bylo jednáno z jeho vůle. Nezáleží na tom, jestli bylo protiprávní chování vykonáno jeho orgány nebo orgány mimo státní strukturu. Touto normou je umožněno státu přijmout za své takové chování, které bylo vykonáno entitou odlišnou, a stát se k němu přihlásil až následně.

V případě *diplomatického a konzulárního personálu spojených států amerických v Teheránu* bylo uplatněno přičtení chování na základě čl. 11 Návrhu článků. Rabující dav, který vtrhnul na americkou ambasádu, nebyl vládou řízen a nebyly mu dávány instrukce. Duchovní vůdce ajatolláh Chomejní a další představitelé íránské vlády však následně svými výroky přijali chování davu jako chování státu.[156] Analogií pro kybernetické operace může být situace, kdy skupina hackerů naruší kybernetickou infrastrukturu cizího státu. Ten v rámci reakce provádí analýzu logů, které mají jednajícího odhalit. Pokud třetí stát, který se útoku neúčastnil, užije svých kybernetických schopností k zakrytí stop po hackerské skupině, bude možné mu její jednání přičíst na základě přijetí tohoto jednání za vlastní.

2.3 Shrnutí kapitoly

V této kapitole jsem se zabýval otázkou přičitatelnosti kybernetických útoků, tak jak ji chápe Manuál a Návrh článků. Bylo vymezeno, co je chápáno objektivní a subjektivním prvkem,

---

[152] MSD: *Nikaragua*... odst. 115, 212
[153] *KMP. Návrh článků*... Čl. 9
[154] *KMP. Návrh článků*... Čl. 10
[155] *KMP. Návrh článků*... Čl. 11
[156] Mezinárodní soudní dvůr: Rozsudek ze dne 24. května 1980, *Případ diplomatického a konzulárního personálu spojených států amerických v Teheránu*. Odst. 74

které jsou k přičtení jednání potřebné. Kybernetická operace jako objektivní prvek porušující normy MPV, kterými je stát vázán, byla podrobně rozebrána v předchozí kapitole. Nyní byla zahrnuta teorie pro přičtení nezbytná. U subjektivního prvku byly vymezeny jednotlivé orgány a entity, jejichž chování je státu přičitatelné, podmínky pro přičtení a ilustrační příklady, které se k těmto u kybernetických operací vážou. Za nejdůležitější považuji úpravu přičtení chování orgánu státu a chování prostředníků, kteří budou jednat za stát. Z dosavadní historie kybernetických útoků se totiž jeví jako pravděpodobné, že právě tyto entity budou kybernetické operace vykonávat za stát nejčastěji a právě jejich chování bude třeba přičítat.

3. Dokazování v případech kybernetických operací před MSD

3.1 Obecně k dokazování před MSD

V této kapitole se zaměřím na otázku jaké důkazní prostředky je možno k přičtení kybernetické operace užít, jak je dokazování upraveno ve vnitřních předpisech MSD a jak se k dokazování obecně staví MSD s ohledem na dosavadní judikaturu.

Na úvod kapitoly je dobré si uvědomit, že přičtení chování určitému státu příliš problematické není. Daleko větším problémem je předložení dostatku důkazů pro unesení důkazního břemene v samotném sporu.[157] Situace je o to komplikovanější, že v mém případě mají být přičteny kybernetické operace, které jsou z velké části vykonávány po internetu. Technické možnosti pro zastření původce, které tento prostředek umožňuje, jsou vnímány mezinárodním společenstvím jako velká výzva.[158]

Účastníky řízení před MSD jsou státy. Je logické, že stát jako suverén má být v řízení aktivní a odpovědný za předložení důkazů ve prospěch svých tvrzení. Funkcí MSD je především dohlížet na získání důkazů, rozhodování o jejich přípustnosti, relevanci a síle. Na rozdíl od vnitrostátního soudu, který má jako podklad ke svému rozhodnutí zákony nebo precedenty a ví, z čeho vycházet, musí MSD v každém sporu nalézat jak právo, dle kterého rozhodovat, tak fakta ze kterých při rozhodování vycházet.[159]

Nakládání s důkazy před MSD je upraveno ve statutu MSD a v jeho Jednacím řádu. Soud určuje formu a lhůty pro předložení důkazů,[160] může před počátkem řízení vyzvat strany k předložení dokladů a vysvětlení a o nepředložení učinit poznámku.[161] Pokud uběhla lhůta k předložení důkazů a ty byly předloženy, MSD další písemné a ústní důkazy odmítne, ledaže druhá strana s předložením souhlasí.[162] MSD může využít svých prostředků ke shromáždění důkazů jako pověření jednotlivců, orgánů, úřadů, komisí či jiných organizací k provedení šetření či vypracování znaleckého posudku.[163] V případě, kdy se jedna ze stran nedostaví nebo svůj

[157] MSD: *Nikaragua*... odst. 57
[158] Zpráva generálního tajemníka, dokument, A/66/152 ze dne 15. července 2011
[159] VALENCIA-OSPINA, Eduard. Evidence before the International Court of Justice. *International Law Forum du Droit International*, 1999, roč. 1, č. 4, s. 203
[160] MSD. *Statut*...
[161] MSD. *Statut*... Čl. 49
[162] MSD. *Statut*... Čl. 52
[163] MSD. *Statut*... Čl. 50

postoj nehájí, může druhá strana žádat, aby dvůr, po zjištění příslušnosti a skutkové odůvodněnosti návrhu, rozhodl ve prospěch jejich nároků.[164]

Jednací řád stanoví, že každé tvrzení, které strana činí, má být podpořeno ověřenou kopií důkazního materiálu, ze kterého vyplývá.[165] Jednací řád omezuje možnost předkládat písemné důkazy po zahájení ústních slyšení. Ty budou odmítnuty, ledaže je přijme druhá strana, nebo jestli je následně povolí soud. [166] Soud má právo požadovat informace, které považuje za důležité pro dané řízení, také po jednotlivých státech.[167] Stát jako suverén k tomu však nemůže být donucen. Soudní dvůr se může kdykoli rozhodnout, buď na základě vlastního podnětu, nebo na žádost účastníka řízení, aby vykonával své funkce týkající se získání důkazů v místě, na které se případ vztahuje, s ohledem na názory stran.[168] Soud může také využít zpráv od mezinárodních organizací, které pověří vyšetřováním daného případu.[169]

V souvislosti s dokazováním rozlišujeme tři základní pojmy. Důkazní břemeno, důkazní standard a pravidla přičtení. Důkazní břemeno identifikuje stranu, která má k prokázání svého tvrzení předložit důkazy a je dále rozvedeno pomocí zásady *actori incumbit onus probandi*. Důkazní standard označuje kvantum důkazů, které musí strana předložit, aby přesvědčila soud o svém tvrzení. Pravidla přičtení zahrnují úroveň propojení osoby nebo skupiny osob a státu, která musí existovat, aby mohlo dojít k přičtení chování státu.[170] Přičtení chování státu jsou chápány jako obyčejové právo a zachyceny v Návrhu článků o mezinárodní odpovědnosti států. Tato problematika byla podrobněji rozebrána v předchozí kapitole. Strany řízení musí předložit takové důkazy, aby naplnily test pro přičtení stanovený v Návrhu článků, pokud chtějí dokázat, že dané chování způsobil cizí stát.

U MSD se neužívá legální teorie důkazní, není stanovena žádná hierarchie důkazů. Předpisy Mezinárodního soudního dvora neurčují vyšší kvalitu důkazů pro důkazy písemné než důkazy získané ústně nebo pro zprávy od mezinárodních organizací či vyšetřovacích komisí než pro oficiální stanoviska států. Soud se k tomuto přihlásil ve své judikatuře.[171] Častěji se vychází

---

[164] MSD. *Statut*... Čl. 53
[165] Mezinárodní soudní dvůr, *Jednací řád Mezinárodního soudního dvora* ze dne 14. dubna 1978, čl. 50. dostupné na <http://www.icj-cij.org/en/rules> čl. 50
[166] MSD. *Řád*... čl. 56
[167] MSD. *Řád*... čl. 62
[168] MSD. *Řád*... čl. 67
[169] MSD. *Řád*... čl. 69
[170] ROSCINI, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas inernational law journal*, 2015, roč. 50, s. 240
[171] MSD: *Nikaragua*.. odst. 212, 60

z písemných důkazů, ale Jednací řád MSD upravuje i svědecké výpovědi a znalecké posudky.[172] Je také možno předkládat různorodé prameny důkazů. Soud ve své praxi připouští užití fotografií, modelů, filmů apod.[173]

Z toho lze dovodit, že v případě dokazování kybernetických útoků by soud povolil i důkazy technického rázu. V praxi se primárně vychází z analýzy logů systému, které zaznamenávají všechny akce na zařízení. Jako kritéria pro identifikaci hackera se používají profesionalita provedení kybernetické operace, informace z hackerských fór, jazyk, kterým je škodlivý kód opoznámkován a způsob postupu. Z hlediska profesionality se vžilo několik pojmů pro různé skupiny hackerů. Od teenagerů, kteří z nudy „prochází internet" až po profesionály, kteří se kybernetickými operacemi živí. Ať už je jejich chování legální či nelegální.[174] Na hacekrských fórech je možno narazit na příběhy a vychloubání různých hackerů, kteří se chtějí předvést před komunitou. I tyto informace mohou přispět k identifikaci. Programy, které slouží ke kybernetickým útokům, jsou psány programovacími jazyky. Jednotlivé prvky lze však různě pojmenovat. Tyto programy bývají při pokročilejších funkcích opatřeny poznámkami, které popisují jednotlivé funkce kódu. Pokud se při analýze dat po útoku podaří získat část programu je možné, že budou objeveny tyto poznámky nebo například přezdívka hackera. Obojí může být užito k jeho identifikaci. Kybernetické útoky procházejí několika fázemi, než jsou dokončeny. Celkově trvají dny, týdny až měsíce. Jednotlivé fáze se provádějí s časovým odstupem, aby se zmenšily šance odhalení útoku. Pokud je útočník nucen provést všechny fáze v krátkém časovém úseku je šance na odhalení vyšší, protože v počítačových systémech a síti bude více neobvyklé aktivity.

3.2 Důkazní břemeno

V procesu samotném je pro dokazování užita zásada *actori incumbit onus probandi*.[175] Soudní dvůr toto potvrdil také ve své judikatuře, z níž plyne, že v případě, kdy si strany nárokují suverenitu nad územím, musí svůj tvrzený titul dokázat předložením faktů, ze kterých vycházejí. Prohlášení stran v kompromisu, že před soud předstupují společně a v jejich sporu není žalobce a žalovaný na tom nic nezměnilo.[176]

---

[172] MSD. Řád... Sekce B, podsekce 3
[173] VALENCIA-OSPINA. *Evidence before the IC*J. s. 204
[174] GrayHat4Life. *7 Types of Hacker You Should Know*. [online]. Cybrary.it, 9. září 2015 [cit. 31. 3. 2018]. Dostupné na <https://www.cybrary.it/0p3n/types-of-hackers/>
[175] Ten kdo něco tvrdí, musí to dokázat.
[176] Mezinárodní soudní dvůr: Rozsudek ze dne 17. listopadu 1953, *Případ Minquiers and Ecrehos (Francie proti Spojenému království)*. s. 52

Tato zásada je omezena ve třech směrech. Fakta, která nejsou rozporována, nemusí být prokazována. Dále není třeba dokazovat věci notoricky známé. Toto omezení vyplývá například z rozsudku ve věci *Nikaragua*, kde se soud věnoval užití zpráv z médií jako důkazního prostředku.[177] Třetím omezením zásady *onus probandi incumbit actori* je, že soud zná právo (zásada *iura novit curia*). MSD však v tomto ohledu rozlišuje mezi mezinárodními smlouvami a obyčejovým právem. Obyčejové právo někdy dokazováno být musí. Zvláště v případech, kdy jde o obyčejové právo místního charakteru.[178]

V akademické rovině se v souvislosti s kybernetickými operacemi uvažovalo i o možnosti obrácení důkazního břemene. Důkazní břemeno by tedy neleželo na straně, která tvrdí, že byla operace vykonána, ale na straně, které je dávána za vinu.[179] Některé názory tvrdí, že pokud je kybernetická operace spáchána z kybernetické infrastruktury státu, jde *prima facie* o důkaz, že stát o chování věděl a je za něj odpovědný.[180] K obrácení důkazního břemene by bylo třeba naplnit určitou výši důkazního standardu, po kterém by k obrácení mohlo dojít.

Takovéto převrácení důkazního břemene je však v rozporu s judikaturou MSD. V případě *Korfského průlivu* Soud vyslovil, že přestože stát vykonával nad územím výlučnou kontrolu, není to důvod k *prima facie* odpovědnosti za chování, které se na tomto území odehrálo, ani k převrácení důkazního břemene.[181] Pokud tyto názory aplikujeme na případy kybernetických operací, dojdeme k závěru, že není založena odpovědnost státu za kybernetickou operaci, byť pochází z kybernetické infrastruktury státu či z kybernetické infrastruktury, která se na území státu nalézá. Může dojít maximálně k porušení povinnosti náležité péče. Nedojde tedy k obrácení důkazního břemene a obě skutečnosti, vykonání kybernetické operace a přičtení chování státu, budou muset být dokázány tím, kdo je tvrdí. MSD je názoru, že i v případě, kdy jsou důkazy převážně v rukou jednoho státu, nedochází k obrácení důkazního břemene.[182] Nelze ani přijmout argument, že stát, který má komplikace s přístupem k důkazům, a v jejich důsledku není schopen je předložit, by při odstranění komplikací a předložení důkazů své důkazní břemeno unesl.[183]

---

[177] MSD: *Nikaragua*... odst. 92
[178] Mezinárodní soudní dvůr: Rozsudek ze dne 20. listopadu 1950, *Případ Asylum (Kolumbie proti Peru)*. s. 276 – 277
[179] CLARKE, Richard, A. KNAKE, Robert. ; *The Next Threat to National Security and What to Do About it*. Ecco, 2011 s. 249
[180] RYAN, J. Daniel. a kol. International Cyberlaw: A Normative Approach. *Georgetown Journal of International Law*, 2017, č. 48
[181] MSD. *Korfu*... s. 18
[182] MSD. *Avena*.... s. 57
[183] Mezinárodní soudní dvůr: Rozsudek ze dne 11. září 1992 *Případ hraničních sporů (El Salvador, Honduras, Nikaragua)*. Odst. 63

Lze tedy říci, že obracení důkazního břemene by bylo u kybernetických operací nešťastným řešením. Vzhledem k faktu, že je lze snadno vést několika státy, vydávat se za stát jiný nebo jednat zcela skrytě, mohlo by obrácení důkazního břemene vést k poškození těch, kdo se na kybernetické operaci vůbec neúčastnili pouze proto, že nebudou schopni dokázat, kdo kybernetickou operaci vykonal. Vzhledem ke složitosti dokazování v těchto případech však může MSD uvolnit pravidla pro dokazování obdobně, jako učinil v případě Korfského průlivu. Mohlo by tedy dojít k předložení nepřímých důkazů a jejich volnějšímu hodnocení.[184]

3.3 Důkazní standard

V angloamerickém typu řízení fungují různé důkazní standardy. Jsou různě silné pro trestní právo (*beyond a reasonable doubt*) a pro právo civilní (*clear and convincing evidence* a *preponderance of the evidence*).[185] Neexistuje shoda na tom, jaké standardy může MSD pro dokázání konkrétních věcí požadovat.[186] Některá fakta však musí být prokázána *prima facie* – například příslušnost soudu.[187] Pokud je předmět sporu v konkrétním případě shodný s jiným, který byl již dříve před MSD předmětem řízení, je logické, aby byl vyžadován standard stejný. Dá se předpokládat, že čím závažnější je předmět řízení, tím přesvědčivější musí důkazy být. Pro přičtení kybernetické operace, která zasáhla do suverenity státu, by tedy postačovaly méně přesvědčivé důkazy než pro kybernetickou operaci kvalifikovanou jako užití síly.

V případu *Ropných plošin* bylo například shledáno, že miny, které způsobily škodu, mají stejné značkování jako jiné miny a poukazují na vlastnictví Iránu. Ten byl z položení min obviněn. Soud důkaz označil za velmi sugestivní, ale nikoliv dostatečný průkazný.[188] Takový důkaz byl pro prokázání tvrzeného shledán nedostatečným.[189] V případu *Ozbrojených aktivit na území Konga* MSD dále používá standardy jako přesvědčivé důkazy,[190] fakta přesvědčivě prokázaná důkazy[191] a důkazy závažné a přesvědčivé.[192] Předpokládá se, že pro prokázání užití síly jsou

[184] MSD. *Korfu*... s. 18
[185] *Standard of proof* [online]. Lectlaw.com, [cit. 30. března 2018]. Dostupné na <https://www.lectlaw.com/def2/s217.htm>
[186] Šestá komise Valného shromáždění OSN, proslov soudkyně Rosalyn Higgins prezidentky Mezinárodního soudního dvora ze dne 2. listopadu, 2007. s. 4
[187] VALENCIA-OSPINA. *Evidence before the ICJ*. s. 203
[188] Mezinárodní soudní dvůr: Rozsudek ze dne 6. listopadu 2003, *Případ ropných plošin*. Odst. 71
[189] Mezinárodní soudní dvůr: Rozsudek ze dne 6. listopadu 2003, *Případ ropných plošin*. odst. 61
[190] Mezinárodní soudní dvůr: Rozsudek ze dne 19. prosince 2005, *Případ zahrnující ozbrojené aktivity na území Konga*. odst. 91
[191] MSD. *Ozbrojené aktivity*... odst. 72
[192] MSD. *Ozbrojené aktivity*... odst. 136

vyžadovány jasné a přesvědčivé důkazy.[193] Jasné a přesvědčivé důkazy pro přičtení kybernetické operace navrhuje také M. Schmitt.[194]

3.4 Důkazní prostředky

Přestože MSD přijímá všechny nosiče důkazů a důkazy hodnotí volně, jsou některé druhy důkazních prostředků častější a průkaznější než jiné. Jako základ sporu před MSD typicky slouží kompromis – rozsáhlé písemné podání, které je dále doplněno listinnými důkazy, které doplňují tvrzená fakta. Důkazy lze teoreticky dělit na několik typů popsaných v následujících podkapitolách.

3.4.1. Písemné důkazy

Tyto důkazy zahrnují veškeré písemnosti, které jsou soudu předloženy. Jedná se o publikované mezinárodní smlouvy, oficiální dokumenty mezinárodních organizací a orgánů států, diplomatickou korespondenci, knihy, plány, mapy a další. Například v případu *Nikaragua* bylo pro přičtení operací *contras* Spojeným státům užito manuálu pro psychologický boj, jehož autorem byla CIA. Tento byl jednotkám *contras* distribuován a tím bylo potvrzeno, že se Spojené státy zprostředkovaně dopustily porušení humanitárního práva.[195] V případě kybernetických operací mohou o jejich vykonání vypovídat například návody jak při operacích postupovat nebo jakým způsobem organizovat osoby na operaci se účastnící. Informace jak vytvořit botnet a jak anonymně vykonat kybernetickou operaci u sebe mohou mít hackerské skupiny stejně tak, jako u sebe měly *contras* manuál pro psychologický boj.

Dá se předpokládat, že většina dokumentů, které státy mají a které se problematice kybernetických operací věnují, bude v různém režimu utajení. Problematika nepředložení dokumentů byla řešena v případu *Korfu*. Velká Británie byla vyzvána k předložení dokumentů, což však neučinila. Argumentovala námořním tajemstvím. Předvolaní svědkové odmítli vypovídat o jejich obsahu z téhož důvodu. Soud konstatoval, že z nepředložení důkazů není možno vyvozovat další závěry nad rámec těch, které z případu již vyplývají.[196] V případu *Genocidy* Bosna vyzvala soud, aby na základě čl. 49 Statutu a čl. 62 Jednacího řádu vyžádal od Srbska dokumenty, které byly předloženy redigované na důležitých místech. Jednalo se o dokumenty Nejvyšší obranné rady, které byly v režimu utajení, protože obsahovaly vojenská tajemství a byly hodnoceny jako důležité pro národní bezpečnost. Soud poznamenal, že Bosna má přístup

[193]ROSCINI. *Evidentiary issues*... s. 250
[194] SCHMITT: *Tallinn Manual 2.0*... s. 595
[195] MSD: *Nikaragua*... odst. 113
[196] MSD. *Korfu*... s. 32

k dokumentům z předchozích sporů, které dokazují to, co si přeje prokázat redigovanými dokumenty. Originály redigovaných dokumentů si nevyžádal, ponechal si však možnost tak dle svého uvážení učinit v budoucnu. [197] Soud pouze konstatoval, že má možnost udělat si o věci vlastní závěry.[198]

V kybernetickém prostředí lze uvažovat kybernetickou operaci, která je následně řešena před MSD. Stát, kterému je kybernetická operace kladena za vinu její vykonání odmítá a vyzve poškozený stát, aby předložil analýzu od CERT. Tvrdí, že CERT jako autorita sledující kybernetické prostředí bude mít objektivní informace a bude možné je podrobit přezkoumání odborníků na kybernetickou bezpečnost. V rámci předkládání důkazů tato analýza však chybí. Aplikujeme-li dosavadní závěry judikatury MSD, bude záležet na tom, jaké důkazy napadený stát bude pro své tvrzení schopen předložit. Nepředložení analýzy CERTu může ve svém důsledku vést k neunesení důkazního břemena a tím k neúspěchu státu ve sporu. Je však na napadeném státu, zda se k předložení daných důkazů rozhodne či nikoliv.

Jako důkazy mohou být užity i dokumenty mezinárodních organizací. Spojené národy se problematikou kyberprostoru zabývají již od roku 1998.[199] Pravidelně bývají vydávány zprávy, které se zabývají nejčastějšími hrozbami v oblasti, způsoby jak posilovat důvěru mezi státy a odolnost sítí a také navrhovány normy, pravidla a principy odpovědnosti států. Předloženy také mohou být zprávy nezávislých vyšetřovacích komisí. V kybernetickém kontextu existuje pouze jeden vzdálený příklad týkající se kybernetických operací v Gruzii roku 2008.[200]

Předloženy mohou být i dokumenty pocházející od nevládních organizací a think-tanků. Do této kategorie spadá Tallinnský manuál, který je hlavní inspirací mé diplomové práce.

V poslední řadě mohou být použity jako důkaz články z médií. MSD je s jejich užitím jako důkazního prostředku opatrný. V případě *Nikaragua* konstatoval, že s tímto druhem důkazů je nutno zacházet opatrně. I když zprávy působí jako objektivní, nepokládá je za vhodné zdroje faktů ale pouze jako ilustrační, doplňkové matriály na dokreslení faktů. Dále soud konstatoval, že novinové články mohou sloužit k rozšíření všeobecné známosti faktu a tím jej dostat pod výjimku ze zásady *actori incumbit onus probandi*. Ten, kdo takový fakt tvrdí, bude zbaven důkazního břemene, pokud půjde díky rozšíření zprávy o informaci notoricky známou. Soud také

[197] MSD. *Případ genocidy*... odst. 44
[198] MSD. *Případ genocidy*... odst.. 206
[199] Výstupy dostupné zde: https://www.un.org/disarmament/topics/informationsecurity/
[200] Nezávislá mezinárodní vyšetřovací komise konfliktu v Gruzii, Zpráva, 2. svazek, 2009. Dostupné na <http://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf>

konstatoval, že je důležité hledat zdroje zpráv. Bez ohledu na to, jak moc byla zpráva rozšířena, nebude její hodnota větší než její původní zdroj, jestli pouze z jednoho zdroje pochází.[201]

I některé kybernetické operace byly světově medializovány.[202] Do kategorie notoricky známých informací lze zařadit i zprávy společností, které se specializují na kybernetickou bezpečnost.[203] Pokud půjde o důkaz předložený pouze ve formě zprávy uveřejněné na internetu, je třeba s ním takto zacházet, bez ohledu na to, jak moc je technicky pokročilá a co z ní vyplývá.[204]

3.4.2. Oficiální stanoviska

Oficiální stanoviska osob představující orgány státu mohou být také použity jako důkazní prostředek. Síla důkazů bude záležet na tom, osoba jaké funkce jej pronesla, u jaké to bylo příležitosti a do jaké míry je možné její stanovisko chápat jako stanovisko státu. Rozdíl bude mezi důkazní sílou stanoviska osoby, která je členem volené samosprávy hlavního města pro regionální noviny a mezi projevem premiéra před orgánem mezinárodní organizace. Takováto stanoviska mohou být chápána jako souhlas s tvrzenými fakty.[205]

Institut uznání jednání za vlastní se v mezinárodním právu objevuje ojediněle. Došlo k němu v případě *diplomatického a konzulárního personálu spojených států amerických v Teheránu*. V kybernetickém prostředí dochází spíše k popírání vykonání kybernetické operace,[206] případně k mlčení ohledně tvrzených obvinění.[207] V současné situaci, kdy je prokázání vykonání kybernetické operace problematické, se jedná o logické jednání států. Ať už se chování dopustily či nikoliv, dokazovat kdo je za kybernetické operace odpovědný je složité.

---

[201] MSD: *Nikaragua*... odst. 62, 63

[202] Sony hack: <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.4204d753ba57>, <https://www.vox.com/cards/sony-hack-north-korea/why-are-the-attacks-on-sony-a-big-deal>nebo Stuxnet: <https://www.theguardian.com/technology/stuxnet>, <http://large.stanford.edu/courses/2015/ph241/holloway1/>, <https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>

[203] Jde například o americký Symantec, Fireeye, McAfee či slovenský ESET. Obdobné zprávy však na svých blozích publikují téměř všechny společnosti, které se kybernetickou bezpečností zabývají jako určitou formu propagace.

[204] ROSCINI. *Evidentiary issues*... s. 244

[205] MSD: *Nikaragua*... odst. 64, 65

[206] ENGLAND, *Rachel. Russia denies UK claim it was behind NotPetya cyberattack* [online]. engadget.com, 15. února 2018 [cit. 15. 4 2018]. Dostupné na <https://www.engadget.com/2018/02/15/russia-denies-uk-claim-it-was-behind-notpetya-cyberattack/>, OLIPHANT, James. GOLUBKOVA, Katya. *Putin rejects accusations of meddling in U.S. election* [online]. Reuters.com, 12. října 2016 [cit. 15. 4 2018]. Dostupné na <https://www.reuters.com/article/us-usa-election/putin-rejects-accusations-of-meddling-in-u-s-election-idUSKCN12C27H>

[207] WILLIAMS, Christopher. *Stuxnet virus: US refuses to deny involvment* [online]. Telegraph.co.uk, 27. května 2011 [cit. 15. 4 2018]. Dostupné na <https://www.telegraph.co.uk/technology/news/8541587/Stuxnet-virus-US-refuses-to-deny-involvement.html>

3.4.3. Svědecké výpovědi, šetření a znalecké posudky

Jednací řád mezinárodního soudního dvora upravuje možnost stran navrhnout výslech svědka jako důkazní prostředek. Svědek může být povolán, jestliže s tím druhá strana souhlasí, nebo jestli je soud přesvědčen o relevantnosti svědecké výpovědi.[208] V historii rozhodování soudu nejsou výpovědi užity často.[209]

Dvůr může kdykoliv pověřit kteréhokoliv jednotlivce, orgán, úřad, komisi nebo jinou organizaci, kterou si vybere, aby provedli šetření nebo podali znalecký posudek.[210] Užití šetření jsem v praxi MSD nezaznamenal, znalecké posudky byly užity například v případu *Korfu*.[211] Expertní názory byly užity k objasnění rozporovaných faktů, které vyžadovaly odborné znalosti chybějící soudcům MSD.

Dá se předpokládat, že v případech kybernetických operací bude tento důkazní prostředek užíván často. Znalosti nutné pro pochopení především subjektivního prvku kybernetických operací budou vyžadovat podrobnou technickou analýzu a následné tlumočení technických závěrů soudcům.

3.4.4. Digitální důkazy

Věda známá jako digitální forenzika se zabývá sběrem informací z hardware a software za účelem rekonstrukce událostí ve vnějším světě. Jak bylo řečeno výše, MSD připouští veškeré nosiče důkazů. Je tedy předpoklad, že i tyto důkazy mohou být v řízení užity. Jak často ale budou užity a jaká bude jejich relevance, je otázkou k diskuzi. S digitálními důkazy se totiž pojí několik problémů.

K získání velké části relevantních informací je třeba součinnost poskytovatelů internetu.[212] ISP mají informace o tom, odkud a kam putují data skrz jejich sítě. Zjednodušeně by se dalo říci, že mají tedy informace o tom, odkud a kam byla kybernetická operace směřována. ISP však nemusí nicméně svolit ke spolupráci s danou zemí a informace jednoduše nepředložit. Co může dělat jihoasijská země, která by chtěla přesvědčit ISP z jižní Ameriky, aby s ní spolupracoval? Tento samotný krok komplikovaný národními právními řády obou států, jazykovou bariérou, zdlouhavostí procesu a dalšími se samotný jeví velmi náročný. V okamžiku, kdy si uvědomíme, že kybernetická operace může být vedena přes desítky či stovky různých zařízení v různých zemích světa s různými ISP je pouze teoretickou otázkou jak dlouho může obstarání relevantních

[208] MSD. *Řád...* čl. 63
[209] MSD: *Nikaragua...* s. 7-8
[210] MSD. *Statut...* čl. 50
[211] MSD. *Korfu...* s. 9
[212] Z angličtiny *Internet service provider* Dále jen „ISP"

informací, tedy informací o původci operace, trvat. ISP nemají z důvodu ochrany osobních údajů navíc možnost archivovat tato data věčně. Je možné hovořit o časovém horizontu několika měsíců. Zvládnout analýzu všech bodů, přes které byla operace vedena, je tedy komplikováno i tímto faktorem.

Cílová informace, ke které je možné se dostat, nám navíc osvětlí, ze kterého zařízení byla operace vykonána a teoreticky pod jakým uživatelským profilem byla vykonána. Získáme však pouze informaci o uživateli, nikoliv konkrétní identitu této osoby. Může se stát, že byl účet či zařízení tohoto uživatele zneužit ke kybernetické operaci. A těžko můžeme prokazovat spojení osoby, kterou neznáme se státem, kterému chceme jednání přičíst. Odpověď na použitelnost digitálních důkazů nám snad poskytnou odborníci na IT, které soud k řešení budoucích sporů předvolá a státy, které svou praxí ukážou, jak moc přesvědčivé pro ně tyto důkazy jsou.

3.5 Nepřímé důkazy a odvozování

Nepřímé důkazy byly definovány jako fakta, která ač neposkytují přímý důkaz, činí závěry o tvrzeném pravděpodobné při dodatečném přemýšlení.[213] Problematikou nepřímých důkazů se MSD zabýval především v případech *Korfu* a *Genocidy*.

V případě Korfu povolil MSD Velké Británii užití nepřímých důkazů, zatímco Albánii ne. Velká Británie tvrdila, že Albánie věděla o minách, které poničily její lodě. Velká Británie nemohla předložit přímé důkazy o vlastnictví min Albánií, protože ty se nacházely pod výlučnou kontrolou Albánie. Z tohoto důvodu povolil MSD Velké Británii užití nepřímých důkazů a možnost činit z nich závěry. Soud poznamenal, že závěry o odpovědnosti státu nesmí ponechávat místo pro rozumné pochybnosti.[214] Soud by tedy měl povolit nepřímé důkazy ve dvou případech – přímé důkazy jsou pod výlučnou kontrolou jednoho státu a nepřímé důkazy nejsou v rozporu s přímými důkazy či uznanými fakty.[215]

V případě zabývajícím se aplikací *Úmluvy o prevenci a trestání zločinu genocidy* tvrdila Bosna, že Srbsko porušilo mezinárodní právo tím, že spáchalo genocidu a tím, že jí nezabránilo. K páchání genocidy Bosna uvedla, že jednání Srbska poukazuje na konkrétní jednotný záměr jeho jednání.[216] Soud však tyto závěry odmítá a se závěrem nesouhlasí. Bosně se nepodařilo prokázat, že chování Srbska může vést k jedinému závěru o jeho úmyslech.[217] V případě povinnosti Srbska, vztahující

[213] MSD. *Korfu*... s. 59
[214] MSD. *Korfu*... s 18
[215] SCHARF, P. Michael. DAY, Margaux. The International Court of Justice's Treatment of Circumstantial Evidence and Adverse Inferences, *Chicago Journal of International Law*. 2012, roč 13, č. 1, s. 131
[216] MSD. *Případ genocidy*... odst. 371
[217] MSD. *Případ genocidy*... odst. 373

se k předejití spáchání genocidy, bylo dle soudu prokázáno, že Srbsko o možnosti, že ke genocidě může dojít, vědělo. Přesto nepodniklo žádné kroky, aby jí předešlo. K porušení povinnosti prevence není nutné, aby bylo prokázáno, že stát měl jistou možnost zvěrstvům zabránit, stačí, pokud je prokázáno, že měl k zabránění prostředky a že se zabránění soustavně vyhýbal. Bosna však toto neprokázala.[218] MSD tedy užil nepřímé důkazy a došel k závěru, že Srbsko o možnosti genocidy vědělo a přesto nepodniklo nic, aby jí zabránilo.[219]

Pro případy kybernetických operací je dobré si uvědomit, že z judikatury plyne, že soud může povolit užití nepřímých důkazů v případě, kdy veškeré přímé důkazy budou na území výlučně kontrolovaném jedním státem. Aby ale mohl MSD dojít k závěru, že kybernetickou operaci vykonal konkrétní stát, budou muset nepřímé důkazy poukazovat na jediný závěr, kde nebudou přípustné rozumné námitky. Zde je místo pro odvážná tvrzení států o celostátní kontrole čínského internetu, o státem finančně sponzorovaných skupinách či částech kódu, které vypovídají o skupinách jiných. Je na MSD nakolik shledá důkazy přesvědčivé.

3.6 Shrnutí kapitoly

V této kapitole jsem se zabýval otázkou dokazování v případech kybernetických operací, kdyby je rozhodoval MSD. Nejdříve byla vymezena pravidla, která pro dokazování plynou ze Statutu a Jednacího řádu MSD. Následovalo objasnění klíčových pojmů, které se pojí s dokazováním – důkazní břemeno a důkazní standard. V souvislosti s důkazním břemenem je poznamenáno, že uvažované možnosti obrácení důkazního břemene jsou v rozporu s dosavadní judikaturou MSD a v souvislosti s kybernetickými operacemi a prostředím, kde se odehrávají, by mohly vést k vytvoření nešťastných problémů. Na závěr byly probrány různé důkazní prostředky, které mohou být dle dočasné praxe soudu ve sporech užity. Bylo vymezeno, že soud připouští důkazy na všech nosičích. Rozebrány tedy byly důkazy, které se standardně předkládají a navíc specifikum kybernetických operací – důkazy digitální. K jednotlivým prostředkům byly navrženy případy, které ilustrovaly užití těchto důkazů ve sporech ohledně kybernetických operací. Nemyslím si, že dojde k posunu vnímání důkazních prostředků pro spory, jejichž předmětem je kybernetická operace. Není objektivní důvod, ze kterého by plynulo, že budou ve velké míře užívány oproti typickým písemným důkazům například výpovědi svědků. Důkazní prostředky budou odlišeny případ od případu. Je pravdou, že patrně dojde k častějšímu užití znaleckých posudků. To souvisí s předmětem řízení – kybernetickými útoky. Při prokazování subjektivního prvku budou patrně předkládány i logy, analýzy sítí a další důkazy technického rázu, k jejichž

[218] MSD. *Případ genocidy*... odst. 438
[219] SCHARF, DAY. *Circumstential evidence*.... s. 140

interpretaci bude znalecký posudek vhodný. S ohledem na povahu digitálních důkazů, možnosti informací, které z nich je možné zjistit a důkazní standard, stanovený pro jednotlivá chování porušující MPV jsem však názoru, že ačkoliv užívány budou, nebudou tvořit základ dokazování státu. Respektive, že státy nebudou vznášet k MSD spory, pokud nebudou mít jistotu, že unesou důkazní břemeno i bez digitálních důkazů.

Závěr

Kybernetické útoky jsou fenoménem, o kterém do budoucna bude patrně slyšet čím dál více. Tím, jak se svět pomocí sítí propojuje, vznikají možnosti k jejich zneužití. Ohledně právní úpravy v MPV lze s nadsázkou říci, že současnou dobu lze charakterizovat jako dobu, kdy se čeká na kybernetické „11. září", které státy přinutí k přijmutí úprav. Do dnešních dní byly totiž ve vytváření nového rámce převážně pasivní – neměly motivaci se na vzájemné úpravě dohodnout. Nové technologie, související s kybernetickými útoky, které daly možnost vzniku také hybridnímu konfliktu, obklopují dnešní svět. Projevují se v různých sporech. Mezi rivaly Ruskou federací a Spojenými státy, v údajných manipulacích voleb nejen v západní Evropě, odehrávají se ve východních zemích jako Čína, součástí jejíž armády je kybernetická jednotka či Severní Korea, která údajně kybernetickými útoky dotuje svůj rozpočet po uvalení ekonomických sankcí.

Ve své práci jsem došel k závěru, že v rámci MPV je kybernetické útoky možné subjektům MPV přičíst. V úvodní kapitole jsem se pokoušel vymezit kybernetický útok jako mezinárodně protiprávní chování. Zdroje, ze kterých jsem vycházel, poskytovaly mnoho různých přístupů k vymezení kybernetického útoku. Žádnou ze zmíněných však mezinárodní komunita nepřijala jako závaznou. Úprava nového fenoménu v podobě kybernetických útoků dosud není upravena tak, aby jí státy respektovaly, a proto se východiskem stalo užití dosavadního právního rámce. Pojem kybernetický útok v technickém slova smyslu jako konkrétního protiprávního jednání v rámci MPV se tedy vydefinovat nepodařilo. Tento byl nahrazen obecnějším termínem kybernetická operace, jak činí Tallinnský manuál. Kybernetická operace je následně chápána jako chování, kterým je možno porušit různé existující normy MPV. Zaměřil jsem se na kybernetické operace, které mohou být zásahem do státní suverenity, vměšování se do vnitřních záležitostí státu, užitím síly a ozbrojeným útokům. Tyto, jakožto i další normy, je možné kybernetickými operacemi porušit.

Otázka přičtení a dokazování kybernetických operací, řešená v druhé části práce, nastiňuje, chování kterých orgánů bude státům přičítáno a jaká budou možná řešení sporů, jejichž je kybernetická operace předmětem. Byly vymezeny možnosti přičtení mezinárodně protiprávního chování subjektům státu. Zaměřil jsem se na chování entit, které považuji za pravděpodobné vykonavatele kybernetických operací – CERTů jako orgánů státu a hackerských skupin, jako prostředníků užitých k vykonání kybernetických operací. V poslední části práce rozebírám problematiku dokazování ve sporech o kybernetických operacích. Objasňuji pravidla, která pro proces dokazování před MSD vyplývají z jednacích předpisů a dosavadní praxe. V otázce důkazního břemene jsem došel k závěru, že jeho obrácení, tedy povinnost státu,

kterému je kybernetická operace kladena za vinu, prokazovat, že ji nevykonal, je v rámci MPV v rozporu s dosavadní judikaturou MSD a je problematická i z technického hlediska. U důkazních prostředků patrně dojde k vývoji v oblasti užití digitálních důkazů a znaleckých posudků. Oba se pojí s technickou povahou kybernetických operací.

Jak bylo konstatováno výše jsem názoru, že kybernetický útok v technickém smyslu (tedy jednotlivé kybernetické operace), je možno již dnes pod právní normy MPV subsumovat a v případě, že se státu podaří shromáždit i dostatek důkazních prostředků od písemných důkazů, přes oficiální stanoviska až po digitální důkazy či důkazy nepřímé vykonávajícímu státu přičíst a tím dosáhnout úspěchu ve sporu. Na první takovéto rozsudky však budeme ještě muset počkat.

Bibliografie

Monografie

1. SCHMITT N. Michael, VIHUL Liis. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017. 638 s.

    a. SCHMITT: *Tallinn Manual 2.0*...

2. CARTWRIGHT, E. James. *Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directories*. [online]. nsci-va.org, 21. 3. 2018 [cit. 21. 3. 2018]. Dostupné na http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf

3. FIELDS, Craig. *Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence* [online]. acq.osd.mil/dsb, 21.3.2018 [cit. 21.3.2018]. Dostupné na https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf

4. BRUDERLEIN, Claude. *HPCR Manual on International Law Applicable to Air and Missile Warfare*. [online]. reliefweb.int, 21. 3. 2018 [cit. 21. 3. 2018]. Dostupné na https://reliefweb.int/sites/reliefweb.int/files/resources/8B2E79FC145BFB3D492576E00021ED34-HPCR-may2009.pdf

5. OWENS A. William a kol. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC 20055: The National Academies Press, 2009. 390 s.

6. JIRÁSEK, Petr. NOVÁK, Luděk. POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. Policejní akademie ČR & Česká pobočka AFCEA, 2013. 200 s.

7. FAIX, Martin, BUREŠ, Pavel, SVAČEK, Ondřej. *Rukověť ke studiu mezinárodního práva 1: Dokumenty*. Praha: Leges. 2015. 432 s.

    a. FAIX. *Rukověť*...

8. CLARKE, Richard, A. KNAKE, Robert. ; *The Next Threat to National Security and What to Do About it*. Ecco, 2011. 320 s.

Odborné články

1. SCHMITT, N. Michael. Computer Network Attack and the use of Force in International Law: Thoughts on a Normavitve Framework. *Columbia Journal of Transnational Law*

a. SCHMITT: *Computer Network Attack*...

2. MARGULIES, Peter. Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. *Melbourne Journal of International Law*, 2013, roč. 14 č. 1

3. JENSEN, T. Eric. Cyber Sovereignty the Way Ahead *Texas International Law Journal*. 2015, roč. 50, č. 1

4. JENSEN, T. Eric. Sovereignty and neutrality in cyber conflict. *Fordham Inernational Law Journal*, 2012, roč. 35, č. 3

   a. JENSEN. *Sovereignty*...

5. SCHMIT. N. Michael, 'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International law,* 2014, roč. 54, č. 1

6. WATTS, Sean. Low-Intensity Computer Network Attack and Self-Defense. *International Law Studies*, 2011, roč. 87

7. KASTENBERG, E. Joshua. Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law. *Air Force Law Review*, 2009, roč. 64, č. 1

8. ROSCINI, Marco. *Cyber Operations and the Use of Force in International Law*. 1. vydání. Oxford University Press, 2014

9. ZEMANEK, Karl. *Armed Attack*. *Encyklopedie* mezinárodního práva Maxe Plancka. [online]. Mezinárodní encyklopedie Maxe Plancka, říjen 2013 [cit. 8. 4. 2018]. Dostupné na <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241>

10. VALENCIA-OSPINA, Eduard. Evidence before the International Court of Justice. *International Law Forum du Droit International*, 1999, roč. 1, č. 4,

    a. VALENCIA-OSPINA. *Evidence before the ICJ*

11. ROSCINI, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas inernational law journal*, 2015, roč. 50, č. 1

    a. ROSCINI. *Evidentiary issues*...

12. RYAN, J. Daniel. a kol. International Cyberlaw: A Normative Approach. *Georgetown Journal of International Law*, 2017, č. 48

13. SCHARF, P. Michael. DAY, Margaux. The International Court of Justice's Treatment of Circumstantial Evidence and Adverse Inferences, *Chicago Journal of International Law*. 2012

    a. SCHARF, DAY. *Circumstential evidence...*

14. EDITOŘI. The Use of Nonviolent Coercion: A Study in Legality under Article 2(4) of the Charter of the United Nations. *University of Pennsylvania Law Review*, 1974, roč. 122, č. 4

Rozsudky soudních tribunálů

1. Mezinárodní soudní dvůr: Rozsudek ze dne 27. června 1986, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*

    a. MSD: *Nikaragua...*

2. Stálý dvůr mezinárodní spravedlnosti: Rozsudek ze dne 7. září 1927, *The case of the S.S. "Lotus"*

3. Mezinárodní soudní dvůr: Samostatný názor soudce Alvareze ze dne 9. dubna 1949, *Případ kanálu Korfu*

    a. MSD. *Korfu...*

4. Evropský soud pro lidská práva: Rozsudek ze dne 8. července 2004, *Ilascu a ostatní proti Moldávii a Rusku (Application no. 48787/99)*

5. Mezinárodní soudní dvůr. Rozsudek ze dne 8. července 1996. *Legalita hrozby nebo užití jaderných zbraní*

    a. MSD: *Legalita hrozby...*

6. Stálý dvůr mezinárodní spravedlnosti: Rozsudek ze dne 26. července 1927, *Případ továrny v Chorzowě*

    a. SDMS. *Továrna v Chorzowě*

7. Mezinárodní soudní dvůr: Poradní posudek ze dne 22. července 2010, *Soulad prohlášení Kosovské nezávislosti s mezinárodním právem*

8. Stálý soud mezinárodní spravedlnosti: Rozsudek ze dne 27. dubna 1927, *Francisco Mallén proti Spojeným státům Americkým*

9. Mezinárodní soudní dvůr: Rozsudek ze dne 26. února 2007, *Případ zabývající se aplikací Úmluvy o prevenci a trestání zločinu genocidy*

    a. MSD. *Případ genocidy...*

10. Mezinárodní trestní tribunál pro bývalou Jugoslávii: Rozsudek ze dne 15. července 1999, *Žalobce proti Duško Tadićovi*

    a. MTTJ. *Tadić...*

11. Mezinárodní soudní dvůr: Rozsudek ze dne 24. května 1980, *Případ diplomatického a konzulárního personálu spojených států amerických v Teheránu.*

12. Mezinárodní soudní dvůr: Rozsudek ze dne 17. listopadu 1953, *Případ Minquiers and Ecrehos (Francie proti Spojenému království)*

13. Mezinárodní soudní dvůr: Rozsudek ze dne 20. listopadu 1950, *Případ Asylum (Kolumbie proti Peru)*

14. Mezinárodní soudní dvůr: Rozsudek ze dne 31. března 2004, (*Případ Avena a dalších mexických občanů (Mexiko proti Spojeným státům americkým)*

    a. MSD. *Avena...*

15. Mezinárodní soudní dvůr: Rozsudek ze dne 11. září 1992 *Případ hraničních sporů (El Salvador, Honduras, Nikaragua)*

16. Mezinárodní soudní dvůr: Rozsudek ze dne 6. listopadu 2003, *Případ ropných plošin.*

17. Mezinárodní soudní dvůr: Rozsudek ze dne 19. prosince 2005, *Případ zahrnující ozbrojené aktivity na území Konga.*

    a. MSD. *Ozbrojené aktivity...*

Mezinárodní smlouvy

1. Sbírka mezinárodních smluv č. 104/2013, částka 56, rozesláno dne 23. prosince 2013. *Úmluva o počítačové kriminalitě.*

    a. SbMS. *Úmluva o počítačové...*

2. Dodatkový protokol k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí mezinárodních ozbrojených konfliktů (Protokol 1

3. Komise pro mezinárodní právo. *Návrh článků o odpovědnosti státu za mezinárodně protiprávní chování*. 2001. Dostupné na: <http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf>

    a. *KMP. Návrh článků...*

4. Rezoluce Valného shromáždění OSN. *A/Res/56/83 o odpovědnosti států za mezinárodně protiprávní chování.*

5. Organizace spojených národů, Charta OSN ze dne 26. června 1945.

6. Vídeňská úmluva o smluvním právu. Sjednána dne 23. května 1969.

7. Haagská úmluva V, Práva a povinnosti neutrálních mocností a osob v případě války pozemní ze dne 18. října 1907. Dostupní na: <http://avalon.law.yale.edu/20th_century/hague05.asp>

Další

1. Skupina vládních odborníků při OSN. Vývoj v oblasti informačních technologií v kontextu mezinárodní bezpečnosti. Zpráva za rok 2015. s. 8. Dostupné na: <https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf>

2. Banka pro mezinárodní vyrovnání. *Guidance on cyber resilience for financial market infrastructure*. Červen 2016. s. 23. Dostupné na https://www.bis.org/cpmi/publ/d146.pdf

3. Poradní rada pro mezinárodní záležitosti a poradní komise v oboru mezinárodního práva – společné stanovisko ke kybernetickému válečnictví. *AIV, CAVV Cyber warfare No 77, AIV/No 22, CAVV*. Prosinec 2011 [cit. 7. 4. 2018]. Dostupné na: <https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf>

4. Zákon č. 240/2000 Sb., krizový zákon, ve znění pozdějších předpisů

5. Nařízení vlády č. 432/2010 Sb., Nařízení vlády o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů

6. Vyhláška č. 317/2014 sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů

7. Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti, ve znění pozdějších předpisů

    a. Zákon č. 181/2014 Sb.

8. Vyhláška č. 316/2014 Sb., vyhláška o kybernetické bezpečnosti

a. Vyhláška č. 316/2014 Sb.

9. Směrnice Evropského parlamentu a Rady (EU) 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii

    a. Směrnice 2016/1148

10. Směrnice Evropského parlamentu a Rady 2013/40/EU o útocích na informační systémy

    a. Směrnice 2013/40

11. Zákon č. 40/2009 Sb., trestní zákoník

12. *Wikileaks email database*. [online] Wikileaks.org, [cit. 14. 4. 2018] Dostupné na <https://wikileaks.org/dnc-emails/>

13. Zpráva Komise pro mezinárodní právo, dokument A/56/10 ze dne 23. dubna - 1. června a 2. července - 10. srpna 2001

    a. Komise A/56/10...

14. MARKUSHIN, Denis. *Cena DDoS útoku* [online]. Securelist.com, 23. března 2017. [cit. 27. 3. 2018]. Dostupné na <https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/>

15. ALPEROVITCH, Dimitri. *Medvědi vprostřed: Průnik do Demokratického národního* výboru [online]. Crowdstrike.com, 15. června 2016 [cit. 27. 3. 2018]. Dostupné na <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>

16. MODDERKOLK, Huib. *Holandské zpravodajské agentury poskytly důležité zprávy o ruském vměšování se do amerických* voleb [online]. Volkskrant.nl, 25. ledna 2018 [cit. 27. 3. 2018]. Dostupné na <https://www.volkskrant.nl/tech/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~a4561913/>

17. Zpráva generálního tajemníka, dokument, A/66/152 ze dne 15. července 2011

    a. Gen.T. A/66/152...

18. Mezinárodní soudní dvůr, *Statut mezinárodního soudního dvora*, dostupné na <http://www.icj-cij.org/en/statute>

    a. MSD. *Statut*...

19. Mezinárodní soudní dvůr, *Jednací řád Mezinárodního soudního dvora* ze dne 14. dubna 1978, dostupné na <http://www.icj-cij.org/en/rules>

    a. MSD. *Řád*...

20. GrayHat4Life. *7 Types of Hacker You Should Know*. [online]. Cybrary.it, 9. září 2015 [cit. 31. 3. 2018]. Dostupné na <https://www.cybrary.it/0p3n/types-of-hackers/>

21. *Standard of proof* [online]. Lectlaw.com, [cit. 30. března 2018]. Dostupné na <https://www.lectlaw.com/def2/s217.htm>

22. Šestá komise Valného shromáždění OSN, proslov soudkyně Rosalyn Higgins prezidentky Mezinárodního soudního dvora ze dne 2. listopadu, 2007

23. Nezávislá mezinárodní vyšetřovací komise konfliktu v Gruzii, Zpráva, 2. svazek, 2009. Dostupné na http://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf

24. Sony hack: <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.4204d753ba57>, <https://www.vox.com/cards/sony-hack-north-korea/why-are-the-attacks-on-sony-a-big-deal>, <https://www.cnbc.com/2015/11/24/the-sony-hack-one-year-later.html>

25. Stuxnet: <https://www.theguardian.com/technology/stuxnet>, <http://large.stanford.edu/courses/2015/ph241/holloway1/>, <https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>

26. ENGLAND, *Rachel. Russia denies UK claim it was behind NotPetya cyberattack* [online]. engadget.com, 15. února 2018 [cit. 15. 4 2018]. Dostupné na <https://www.engadget.com/2018/02/15/russia-denies-uk-claim-it-was-behind-notpetya-cyberattack/>

27. OLIPHANT, James. GOLUBKOVA, Katya. *Putin rejects accusations of meddling in U.S. election* [online]. Reuters.com, 12. října 2016 [cit. 15. 4 2018]. Dostupné na <https://www.reuters.com/article/us-usa-election/putin-rejects-accusations-of-meddling-in-u-s-election-idUSKCN12C27H>

28. WILLIAMS, Christopher. *Stuxnet virus: US refuses to deny involvment* [online]. Telegraph.co.uk, 27. května 2011 [cit. 15. 4 2018]. Dostupné na https://www.telegraph.co.uk/technology/news/8541587/Stuxnet-virus-US-refuses-to-deny-involvement.html

29. NATO, Deklarace z Waleského summitu. [online]. 5. září 2014 [cit. 7. 4. 2018]. Dostupné na: https://www.nato.int/cps/ic/natohq/official_texts_112964.htm

Abstrakt

Cílem diplomové práce je zjistit jestli je možno v rámci mezinárodního práva veřejného přičíst státům chování, které materiálně chápeme jako kybernetický útok.

Za tím účelem bylo nejprve třeba zanalyzovat současný stav právní úpravy týkající se kybernetických útoků. Práce zmiňuje, že v současnosti neexistuje definice kybernetického útoku, nastiňuje však definice, které nejsou chápány jako závazné, pro ilustraci obsahu pojmu. Následně je vymezen pojem kybernetické operace, který je zástupným pojmem pro kybernetickou aktivitu, kterou mohou být porušeny normy mezinárodního práva. Práce dále rozebírá jednotlivé normy, které mohou být kybernetickou operací porušeny s praktickými příklady. Následně je zpracována teorie pojící se s přičítáním mezinárodně protiprávního chování státu dle Návrhu článků o odpovědnosti států. Na závěr je vymezeno, jak probíhá dokazování před mezinárodním soudním dvorem, pojmy důkazního břemene, důkazního standardu a možnost užití různých důkazních prostředků v řízení o kybernetické operaci.

Práce je rozdělena na tři hlavní kapitoly, kdy první se zabývá vydefinováním pojmu kybernetický útok, druhá obsahuje teoretické vymezení přičitatelnosti a třetí dokazování před mezinárodním soudním dvorem.

Práce byla vypracována v souladu se Směrnicí děkanky č. 2/2010, kterou se stanoví náležitosti kvalifikačních prací na Právnické fakultě Univerzity Palackého v Olomouci.

Abstract

The main aim of this thesis is to discover whether is it possible to attribute a cyber-attack in its material meaning to a state in the field of public international law.

For this purpose, the analysis of the current legislation considering cyber-attacks was made. The thesis mentions that there is no definition of the term cyber-attack in the current public international law. On the other hand, it provides, several non-binding definitions to illustrate the content of the term cyber-attack. The term is therefore replaced by more general one; cyber operation. This term is used as a prompt to describe ill conduct of states by which different kinds of obligations can be breached. This thesis focuses on state sovereignty, prohibition of non-intervention, use of force and armed attack. Further on the thesis goes through the theory of attribution of a conduct to a state as set by the Draft Articles on Responsibility of States for Internationally Wrongful Acts. In the final part the thesis focuses on the proofing before the International Court of Justice. Terms burden of proof, standard of proof are discussed as well as means of proof which can be used in the cyber operation case before the International Court of Justice.

The thesis is divided into three main chapters. The first chapter focuses on the term cyber-attack and its definition. The second chapter describes the theory of attribution and the third focuses on proofing before the International Court of Justice.

This master thesis was written in compliance with The Regulation of the Dean of the Faculty No. 2/2010, establishing the terms of diploma thesis at Law Faculty, Palacký University in Olomouc.

Klíčová slova, keywords

Kybernetický útok	Cyber attack
Kybernetická operace	Cyber operation
Suverenita	Sovereignty
Zasahování do vnitřních záležitostí státu	Intervention
Užití síly	Use of force
Ozbrojený útok	Armed attack
Mezinárodně-právní odpovědnost	International responsibility
Důkazní břemeno	Burden of proof
Důkazní standard	Evidentiary standard
Mezinárodní soudní dvůr	International court of justice
Dokazování před Mezinárodním soudním dvorem	Evidence before ICJ