UNIVERZITA KARLOVA

Právnická fakulta

Martina Jirsová

Odpovědnost státu za protiprávní jednání v kyberprostoru

Diplomová práce

Vedoucí diplomové práce: JUDr. Milan Lipovský, Ph.D.

Katedra mezinárodního práva

Datum vypracování práce (uzavření rukopisu) : 1. 12. 2019

Prohlašuji, že jsem předkládanou diplomovou práci vypracovala samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 132 152 znaků včetně mezer.

Martina Jirsová

V Praze dne 1. prosince 2019

Poděkování

Ráda bych poděkovala JUDr. Milanu Lipovskému, Ph.D., vedoucímu mé práce, za poskytnuté rady a doporučení, jakož i za projevenou ochotu, trpělivost a vstřícnost při konzultacích, a to zejména v závěru přípravy této práce.

Děkuji též Dominiku Dvořákovi za mnohaleté přátelství, podporu a recenzi textu, a Ivanu Šivákovi za lásku, skvělé nápady a „kybernetické“ rady, bez nichž by tato práce nikdy nespatřila světlo světa.

Největší poděkování ale patří mým nejdražším rodičům a prarodičům, kteří při mně stáli po celou dobu mých studií a věřili, že dojdu do zdárného konce.

Obsah

Úvod ... **1**

1. Kyberprostor ... **4**

1.1. Pojem kyberprostoru ... 4
1.2. Nežádoucí aktivita v kyberprostoru ... 6
1.3. Kyberprostor a právo ... 7

2. Obecně o mezinárodněprávní odpovědnosti ... **11**

2.1. Porušení mezinárodního závazku ... 12
2.2. Přičitatelnost jednání ... 13
2.2.1. Orgány státu *de iure* ... 13
2.2.2. Orgány státu *de facto* ... 15
2.2.3. Zvláštní případy přičitatelnosti jednání státu ... 17
2.3. Okolnosti vylučující protiprávnost ... 18
2.4. Právní následky mezinárodně protiprávního jednání ... 18

3. Mezinárodněprávní odpovědnost v kyberprostoru ... **19**

3.1. Suverenita, územní a osobní výsost v kyberprostoru ... 20
3.2. Porušení mezinárodního závazku ... 21
3.2.1. Zákaz hrozby a použití síly ... 22
3.2.2. Zákaz hrozby a použití síly v kyberprostoru? ... 24
3.2.3. Vměšování se do vnitřních nebo vnějších záležitostí států ... 27
3.2.4. Narušení suverenity ... 30
3.2.5. Due diligence ... 31
3.2.6. Dílčí shrnutí ... 34
3.3. Přičitatelnost jednání ... 34
3.3.1. Orgány státu *de iure* ... 35
3.3.2. Přičitatelnost jednání nestátních aktérů ... 36
3.3.3. Koncept kontroly v kyberprostoru ... 38
3.3.4. Dílčí shrnutí ... 41
3.4. Reakce na kybernetickou operaci ... 42

Závěr ... **44**

Seznam zkratek ... **i**

Seznam použitých zdrojů ... **ii**

Abstrakt ... **xvi**

Abstract ... **xvii**

Úvod

„*Psal se leden 2010, když si vyšetřovatelé IAEA při rutinní inspekci závodu na obohacování uranu v Natanz všimli, že v halách s tisíci kaskádových centrifug patrně není něco v pořádku. […] Za normálních okolností musel Írán nahradit zhruba deset procent centrifug ročně díky provoznímu opotřebení. Při zhruba 8700 centrifugách instalovaných v Natanz se tedy ročně odepisovalo přibližně 800 z nich. Když ale IAEA zkoumala záznamy z kamer před kaskádovými halami, byli šokováni, když zjistili, jakým tempem museli zaměstnanci vyměňovat poškozené centrifugy. Během pouhých několika měsíců jich bylo nahrazeno mezi jedním a dvěma tisíci. Otázkou bylo: proč?*“.[1]

Odpověď na otázku, kterou si vyšetřovatelé v lednu 2010 kladli, byla objevena až o několik měsíců později a dostala jméno Stuxnet. Jednalo se o vysoce sofistikovaný škodlivý počítačový program. Jedna z jeho výjimečností tkví v tom, že přestože se šířil v celé řadě různých kybernetických zařízení, aktivoval se pouze v průmyslových zařízeních pracujících se softwarem SCADA od společnosti Siemens. Sám tedy dokázal rozpoznat, zda se jedná o zařízení, k jejichž napadení a kontrole byl vytvořen. Další jeho nebývalou vlastností je funkce dálkového přístupu (*backdoor*), která umožňovala nejen čtení získaných informací, ale též nahrání jeho nových verzí, čímž vznikaly další možnosti infikace Stuxnetu do cílových systémů.[2]

Cílem Stuxnetu byly součásti íránské kritické infrastruktury - závod pro obohacování uranu v okolí města Natanz a jaderná elektrárna v Búšehr – a jeho účelem byla pravděpodobně sabotáž íránského jaderného programu. Jedná se o první kybernetickou operaci, která kromě přerušení jejich funkčnosti způsobila též fyzickou škodu. Přestože došlo „pouze“ k obrovským škodám na íránském jaderném programu, společnost může být ráda, že Stuxnet nezpůsobil jaderný výbuch, který prakticky hrozí vždy, když dojde k narušení řídících jednotek jaderných elektráren. Jeho sofistikovanost vede experty k domněnce, že za jeho vytvořením musel stát přinejmenším cizím státem sponzorovaný nestátní aktér. Přestože stopy vedou k Izraeli a USA, za původce Stuxnetu až doposud nikdo nebyl označen.[3] K autorství se rovněž nikdo nepřihlásil.

---

[1] ERBEN, L. *Příchod hackerů: příběh Stuxnetu* [online]. 29.04.2014 [cit. 2019-11-30]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/.

[2] ZETTER, K. An Unprecedented Look at Stuxnet, the World's First Digital Weapon. *Wired* [online]. 03.11.2014 [cit. 2019-12-01]. Dostupné z: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/#.

[3] NAKASHIMA, E. a J. WARRICK. Stuxnet was work of U.S. and Israeli experts, officials say. *The Washington Post* [online]. 2 June 2012 [cit. 2019-12-01]. Dostupné z: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

Íránu tak vznikly obrovské škody, jejichž náhradu nemá vůči kom u uplatnit.

Od případu Stuxnetu uběhne zanedlouho deset let. Od té doby šly technologie kupředu takovou rychlostí, že na ně právo jen stěží stíhá reagovat. Vzkaz pro mezinárodní právo je tedy jasný.

Přestože se většina protiprávních kybernetických operací odehrává mimo ozbrojený konflikt, až do roku 2017, kdy byl vydán Tallinnský Manuál 2.0, jsme neměli k dispozici žádný ucelený normativní pohled na otázku mezinárodní odpovědnosti za protiprávní kybernetické jednání učiněné v době míru. Nakolik se Tallinnský Manuál snaží vyčerpávajícím způsobem aplikovat pravidla obecného mezinárodního práva na kyberprostor, v řadě otázek ani jeho autoři nenašli shodu a předkládají tak několik možných, doposud spíše teoretických, variant řešení.

Jelikož už dnes není sporu o tom, že se mezinárodní právo na jednání v kyberprostoru aplikuje, hlavní výzkumnou otázkou je stanovení, jakým způsobem se tak děje a zda je stávající právní úprava dostačující. Pro případ, že by současné mezinárodní právo efektivní uplatnění v kyberprostoru neumožňovalo, je další výzkumnou otázkou určení, jakým způsobem by bylo vhodné na daný stav reagovat.

Odpovědnost státu za protiprávní jednání v kyberprostoru je velice komplexní institut, jehož podrobná analýza by mnohonásobně přesáhla rozsah této práce. Pozornost proto bude věnována jen některým jejím dílčím aspektům, jmenovitě porušení mezinárodního závazku v kyberprostoru a přičitatelnosti kybernetického jednání konkrétnímu státu.

První část práce se nejprve zaměřuje na to, co se vůbec rozumí pojmem kyberprostor a k jakým druhům nežádoucích aktivit v něm může docházet. Na tomto místě dochází též k terminologickému odlišení pojmů „kybernetická operace“ a „kybernetický útok“, a k podrobnějšímu popisu vztahu kyberprostoru a práva.

Druhá část práce shrnuje základní postuláty obecného mezinárodního práva v oblasti mezinárodní odpovědnosti. Zde je nejprve definován objektivní prvek, následně je blíže zkoumána otázka přičitatelnosti (subjektivní prvek), kde jsou představeny varianty jednání různých entit, jejich (ne)přičitatelnost konkrétnímu státu a výklad v judikatuře. Závěrem jsou stručně představeny i okolnosti vylučující protiprávnost a právní následky mezinárodně protiprávního jednání.

Těžiště práce představuje část třetí, která aplikuje poznatky shrnuté ve druhé části na jednání učiněné v kyberprostoru. Pozornost je nejdříve věnována pojmům suverenita, územní a osobní výsost v kyberprostoru, neboť na tento výklad je poté navázáno v kapitole 3.2, která popisuje různé stupně narušení suverenity jako porušení mezinárodního závazku. Navazuje

kapitola 3.3 o přičitatelnosti a analýzu uzavírá několik úvah *de lege ferenda* stran reakce na kybernetickou operaci ze strany států. Jednotlivá primární pravidla jsou nejprve popsána obecně a poté jsou aplikována na kybernetický prostor. K výkladu je využito několik ilustrativních příkladů, na kterých je demonstrována (ne)dostatečnost současné právní úpravy.

Závěr práce je věnován zodpovězení výzkumných otázek a uvedení dalších souvisejících témat, která by si zasloužila bližší prozkoumání.

Primárními zdroji této práce jsou Tallinnský Manuál 2.0, rezoluce Valného shromáždění OSN a výstupy z práce skupiny vládních expertů v oblasti informací a telekomunikací ve vztahu k mezinárodní bezpečnosti (*Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*) v rozsahu, ve kterém se týkají tématu této práce. S ohledem na nedostatek primárních zdrojů v podobě mezinárodních smluv[4] či judikatury v oblasti kyberprostoru, byla ke zpracování práce využita též celá řada sekundárních zdrojů v podobě knižní i elektronické literatury a odborných i novinových článků, přičemž v potaz byla brána i potenciální možnost ovlivnění a mylný výklad ze strany autorů. Překlady těch částí rozhodnutí mezinárodních soudních orgánů, které se objevují v Casebooku vydaném katedrou mezinárodního práva Právnické fakulty Univerzity Karlovy,[5] byly převzaty z této publikace. U ostatních překladů, kde není uveden jejich autor, platí, že je překlad dílem autorky této práce.

Tato práce je vypracována převážně metodou analytickou, která umožňuje podrobnější poznání jednotlivých prvků institutu mezinárodní odpovědnosti a jejich vztah k celku. V částech, kde dochází ke srovnání názorů jednotlivých učenců, byla využita metoda komparativní, přičemž aplikována byla též metoda deskriptivní. Závěry byly zpracovány metodou syntézy a dedukce.

[4] Úmluvy přijaté na půdě Rady Evropy se týkají kybernetické kriminality a nejsou relevantní pro výzkumné otázky této práce.
[5] ŠTURMA, P. a kol. *Casebook: výběr případů z mezinárodního práva veřejného*. 4. upravené vydání. Praha: Univerzita Karlova, Právnická fakulta, 2019. Scripta iuridica. ISBN 978-80-87975-91-6.

1. Kyberprostor

Chceme-li se zabývat otázkou odpovědnosti států za jejich protiprávní jednání v kyberprostoru, bude vhodné si tyto pojmy nejprve vymezit. Následující část se proto pokouší pojem kyberprostoru charakterizovat, popisuje jednotlivé nežádoucí aktivity, ke kterým v něm dochází, a představuje, proč by je právo mělo brát na zřetel.

V této souvislosti bych ještě ráda upozornila na některé terminologické nepřesnosti, ke kterým při publikování na kybernetická témata velice často dochází. Přestože mnozí autoři velice často používají pojem „kyberútok" (*cyber attack*), tento by měl být používán pouze ve vztahu ke kybernetickým operacím, které budou představovat útok ve smyslu mezinárodní humanitárního práva.[6] Naproti tomu pojmy „kybernetická operace" (*cyber operation*) nebo „kybernetické jednání" (*cyber act*) jsou širší a zahrnují v sobě, jak kybernetické útoky, tak kybernetické trestné činy (*cybercrime*), jakož i veškeré jiné chování, ke kterému v kyberprostoru dochází. Tato práce proto používá zastřešující pojem kybernetická operace.

1.1. Pojem kyberprostoru

Jednotná definice kyberprostoru v současné době neexistuje a jeho samotný koncept se neustále vyvíjí. Kyberprostor se jako pojem poprvé objevil už v 80. letech minulého století,[7] reálný rozměr dostal ovšem až v letech devadesátých, kdy došlo k obrovskému rozvoji internetu. V této době byl kyberprostor ještě stále chápán jako nehmotný, virtuální a těžko uchopitelný počítačový svět,[8] přičemž jako virtuální realita, která nemá konec ani začátek, je ze strany laické veřejnosti často vnímán i dnes. Dnes již není pochyb o tom, že jeho existence je zcela závislá na hmotné podstatě - tedy na technologiích, které se ve světě fyzicky nacházejí, a jejichž poškození nebo narušení může v kyberprostoru způsobit rozsáhlé škody nebo i jeho zánik.[9]

---

[6] BRUNER, T. K podmínkám a způsobu aplikace mezinárodního humanitárního práva na kybernetické operace. In: BÍLKOVÁ, V. (ed.) *Mezinárodní humanitární právo: vznik, vývoj a nové výzvy*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2015, s. 159. ISBN 978-80-87975-35-0.

[7] Tento termín ve své povídce poprvé použil William Gibson na počátku osmdesátých let. Později ho své knize Neuromancer popsal jako „*konsenzuální datovou halucinaci, vizualizovanou v podobě imaginárního prostoru, tvořeného počítačově zpracovanými daty a přístupného pouze vědomí (a nikoli fyzické tělesnosti) uživatelů*". Do povědomí veřejnosti se tento pojem vryl ještě později, a sice po vydání tzv. Deklarace nezávislosti internetu. Srov. BARLOW, J. P. A Declaration of the Independence of Cyberspace. In: *EFF* [online]. 1996 [cit. 2019-10-05]. Dostupné z https://www. eff. org/cyberspace-independence.

[8] BASTL, M. a Z. GRUBEROVÁ. Kyberprostor jako „pátá doména"?. *Vojenské rozhledy* [online]. 2013 (4), s. 10-21 [cit. 2019-10-05]. Dostupné z: http://vojenskerozhledy. cz/kategorie-clanku/bezpecnostni-prostredi/kyberprostor-jako-pata-domena.

[9] KOLOUCH, J. Kyberprostor. In: *Teorie informační bezpečnosti* [online]. 2016 [cit. 2019-10-05]. Dostupné z http://www. teorieib. cz/pbi/files/281-Kyberprostor-Kolouch. pdf.

Kyberprostor bývá nejčastěji popisován pomocí tří vrstev – fyzické, logické a lidské (personální), které jsou od sebe sice zřetelně odlišeny, avšak zůstávají vzájemně propojené.[10] Fyzická vrstva sestává z hmotných zařízení a infrastruktur (hardware a elektromagnetické spektrum), sloužících k přenosu, zpracování a uchování dat. Jelikož se jedná o zařízení, která jsou fyzicky dosažitelná, je zapotřebí je chránit proti mechanickému poškození a neoprávněnému fyzickému přístupu k nim, neboť tento může posléze umožnit přístup i ke složce logické. Fyzická vrstva má nezastupitelnou funkci i pro svět právní, protože slouží jako jakýsi záchytný bod při stanovení zeměpisné polohy a tedy i odpovídajícího aplikovatelného právního rámce. Na fyzické vrstvě je potom „položena" vrstva logická, která je již abstraktnější a sestává z firmwarů vázaných přímo k hardwarovým prvkům celé sítě (tedy vlastně k fyzické vrstvě). Dále se zde nachází dnes již zcela zásadní skupina virtuálních zařízení a infastruktur s nimi spojených, či složka aplikační. Tyto kategorie prvků uvádí jednotlivé části sítě do provozu. Personální, nebo také „kyberpersonální" vrstva, je složena ze sítí a uživatelských účtů, ať už skutečných nebo robotických osob, a jejich vzájemných vztahů. Konkrétně se jedná o IP adresy, webové stránky, e-mailové schránky, uživatelská jména, uživatelská hesla a uživatele kyberprostoru, kteří představují hlavní a zároveň nezbytný prvek této vrstvy. Vzhledem k tomu, že „kyber-osoba", na rozdíl od skutečného člověka, může mít několik identit nebo její identita může být zcela skrytá, přičitatelnost jednání učiněného v kyberprostoru činí velké potíže, a proto (kyber)personální složka nemůže sloužit jako jediné kritérium pro stanovení aplikovatelného právního rámce.

Pojem kyberprostoru dnes slouží zejména jako souhrnné označení pro informační a komunikační technologie, které obvykle odkazují na „*počítače, počítačové sítě a systémy, a různé technologie sloužící k šíření a dodávce informací, jako pevninské a podmořské kabely, satelity, telefony i televize*"[11] a v žádném případě tedy nemůže být ztotožňován s pojmem internet, jak se dříve často stávalo, neboť internet představuje pouze jednu vrstvu z jeho technologického substrátu.

[10] Joint Chiefs of States. JP 3-12, Cyber Operations. In: *Federation of American Scientists* [online]. 2018, s. I-2 – I-5 [cit. 2019-10-05]. Dostupné z https://fas. org/irp/doddir/dod/jp3_12. pdf.

[11] UNIDIR. *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century* [online]. 2017, s. 7 [cit. 2019-10-06]. Dostupné z https://www. unidir. org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691. pdf.

1.2. Nežádoucí aktivita v kyberprostoru

Stejně tak, jako je možné kyberprostor členit na určité vrstvy (kategorie), lze takto rozčlenit i jednání v něm učiněné. Uznávané publikace je nejčastěji dělí do čtyř skupin, přičemž každá z nich se vyznačuje určitými vlastnostmi, které zásadně ovlivňují, jakým způsobem se dané chování v síti projevuje a jak s ním lze pracovat či se mu bránit.[12]

Prvním typem nežádoucí aktivity jsou takzvané DoS útoky (*denial of service attacks*), které mají jediný cíl, a to zastavit službu (webové stránky, servery, virtuální zařízení) bez jakéhokoli ničivého dopadu na kybernetickou infrastrukturu jako celek. Tento typ aktivity patří mezi ty nejméně sofistikované a autoři těchto kybernetických operací zpravidla nemají ambice výrazně a dlouhodobě poškodit cíl jejich operace.[13]

Další kategorii nežádoucích aktivit tvoří známý a v široké veřejnosti rozšířený anglický výraz *malware*. Za malware lze považovat jakýkoliv škodlivý program, který má za účel poškodit uživatele počítače, přičemž k danému počínání nebyl škodlivý program uživatelem oprávněn. Existuje několik druhů malwarů, mezi ty nejznámější typy škodlivých programů patří bezpochyby trojský kůň, počítačový virus červ a mnoho dalších. Každý z těchto druhů má mírně rozdílné zaměření - mohou se lišit ve způsobu chování, v práci, kterou pro útočníka vytvářejí, nebo způsobem, jak se do prostředí své oběti infikovali. Určité klíčové vlastnosti mají ale všechny typy škodlivého programu společné, a to zejména schopnost šířit se v dostupné síti a poškodit infikované zařízení.

Mezi další významnou kategorií nežádoucí aktivity v kyberprostoru je nepovolený pohyb v počítačové síti, nebo také neautorizované vniknutí do počítačové sítě (*network intrusion*). Nepovolené vniknutí se většinou neobejde bez krádeže citlivých dat oběti kybernetické operace, ale také zneužití různých zdrojů dané sítě. Útočník využívá slabin síťových prvků ve vlastní prospěch, které mu pak pomáhají v další škodlivé činnosti nebo nepozorovanému pohybu v síti. V tomto okamžiku se dostáváme k otázce, jak se před tímto typem nežádoucí aktivity v kyberprostoru bránit. Na tuto otázku často neznají odpověď ani profesionálové ve svém oboru. Bodem číslo jedna v tomto kontextu je vždy neustálá analýza aktuálního stavu dané sítě. Pokud se útočník v síti pohybuje neoprávněně je velmi důležité tento pohyb včas zaznamenat a podrobit ho zkoumání. Často se stává, že se útočníci v dané síti

[12] Srov. například GATTIKER, U. E. *The Information Security Dictionary: Defining the Terms that Define Security for E-Business, Internet, Information and Wireless Technology*. Springer US, 2004. ISBN 978-1-4020-7927-6.

[13] Ze základního DoS útoku vychází složitější forma, a to DDoS útok (*distributed denial of service attack*). Zatímco standardní DoS útok pochází zpravidla z jednoho zařízení, které využívá právě jedno připojení k síti, DDoS útok využívá k akci hned několik zařízení spolu s několika připojeními k síti. To přináší útočníkům větší sílu a možnost vyřadit z provozu i velmi dobře zabezpečené služby.

pohybují delší dobu, ale správa dané sítě o jejich neoprávněném pohybu netuší, což dává útočníkům drahocenný čas si v síti najít jednak data, pro která přišli, jednak možnost najít další slabá místa sítě pro případný opětovný návrat.

V neposlední řadě je nutné zmínit ještě jeden významný druh nežádoucí aktivity v kyberprostoru, a to narušování infrastruktury (*infrastructure-interference operation*). V tomto kontextu se jedná zejména o narušování kritických infrastruktur, které mají přímý dopad na zdraví a bezpečnost občanů.

V této kapitole byly představeny jednotlivé typy a oblasti nežádoucí aktivity v kyberprostoru. Kategorie byly srovnány chronologicky dle závažnosti daného nežádoucího chování. Z uvedeného vyplývá, že narušování kritické infrastruktury[14] patří mezi zdaleka ty nejzávažnější typy nežádoucího chování v kyberprostoru, které, jak bude popsáno níže v této práci, mohou za splnění určitých okolností představovat též zakázané použití síly, neboť již z účelové podstaty těchto sítí je naprosto zřejmé, že tyto jsou extrémně zranitelným bodem pro každý stát, a jejich narušení, ovládnutí nebo zničení může mít katastrofické následky. To ovšem neznamená, že by prvně uvedené kybernetické operace byly bezvýznamné. I ty mohou za určitých okolností představovat porušení mezinárodního závazku[15] a zavdat tak příčinu k odpovědnosti státu za ně.

1.3. Kyberprostor a právo

Vzhledem k tomu, že hranice kyberprostoru nelze určit, objevovaly se v minulosti názory, že se na něj právo vůbec neaplikuje,[16] protože se jedná o doménu, která leží mimo politickou kontrolu jakéhokoli státu a která je univerzálně přístupná odkudkoli,[17] anebo že by se na něj právo aplikovat nemělo, protože kyberprostor by měl zůstat svobodný a otevřený.[18]

---

[14] Názory států na otázku, co přesně bude kritickou infrastrukturu představovat, se liší. Obecně ale lze konstatovat, že infrastruktura vysokého elektrického napětí, železniční infrastruktura, infrastruktura řízení letového provozu, či řídící infrastruktura jaderné elektrárny do této kategorie spadne vždy. V českém právním řádu s pojmem kritická infrastruktura pracuje § 2 písm. g) – i) zákona č. 240/2000 Sb., o krizovém řízení (Krizový zákon). Pro pojem kritické *kybernetické* infrastruktury srov. § 2 písm. b) zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

[15] Srov. kapitolu 3.2 níže.

[16] JOHNSON, D. R. a D. POST. Law and boarders: The rise of law in cyberspace. *Stanford Law Review* [online]. 1996, 48 (5), s. 1367 - 1402 [cit. 2019-10-07]. Dostupné z https://heinonline. org/HOL/P?h=hein. journals/stflr48&i=1385.

[17] WATTS, S. a T. RICHARD. Baseline Territorial Sovereignty and Cyberspace. *Lewis & Clark Law Review*. 2018, 22 (3), s. 779-780.

[18] Po svobodě a otevřenosti kyberprostoru volal již John Perry Barlow ve svém díle „A Declaration of the Independence of Cyberspace“. Jako další zastánce této myšlenky lze jmenovat například Davida Johnsona a Davida Posta - viz WU, T. S. Cyberspace sovereignty? – The Internet and the International System. *Harvard Journal of Law & Technology* [online]. 1997, 10 (3), s. 648 – 649 [cit. 2019-10-07]. Dostupné z http://jolt. law. harvard. edu/articles/pdf/v10/10HarvJLTech647. pdf.

Se stále zvyšujícím se množstvím zneužití těchto technologií[19] už dnes ovšem není sporu o tom, že regulace kybernetického prostoru právní cestou je nejen možná, ale i nutná, a proto se o ni státy pokouší, ať už na vnitrostátní nebo mezinárodní úrovni.[20]

S ohledem na to, že současné kybernetické právo se soustředí zejména na otázku kybernetické bezpečnosti, přesněji na počítačovou kriminalitu, tedy oblast, která je spíše předmětem zájmu práva trestního, lze regulaci jednání v kyberprostoru na vnitrostátní úrovni nalézt nejčastěji v trestních zákonících,[21] které ovšem definici pojmu kyberprostor zcela pomíjí. Český právní řád v tomto směru poněkud vybočuje, když kromě kybernetických trestných činů, které vypočítává trestní zákoník,[22] přichází též s definicí kyberprostoru („*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací*"), kterou nalezneme v zákoně o kybernetické bezpečnosti.[23] Ještě o něco přesnější definici pak obsahuje zákon slovenský,[24] který pod pojem kyberprostor zahrnuje i kyberpersonální vrstvu, která byla popsána výše v kapitole 1.1.

O důležitosti regulace kyberprostoru svědčí i zájem ze strany Evropské unie, na jejíž půdě vzniklo nařízení o kybernetické bezpečnosti, jehož cílem je posílení kybernetické bezpečnosti uvnitř Unie, přičemž jedním z hlavních důvodů pro jeho vydání byl právě nárůst kybernetických bezpečnostních hrozeb a jejich přeshraniční povaha.[25]

---

[19] Srov. Phishing, Ransomware and Co. – An increasing threat. *OneClick Blog* [online]. 30 October 2017 [cit. 2019-10-18]. Dostupné z: https://oneclick-cloud. com/en/blog/trends-en/increasing-threat-of-cyber-crime/; Master Table. *Hackmaggedon* [online]. [cit. 2019-10-18]. Dostupné z: https://www. hackmageddon. com/2018-master-table/.

[20] GOLD, J. Two Incompatible Approaches to Governing Cyberspace Hinder Global Consensus. In: *Leiden Security and Global Affairs Blog* [online]. 2019 [cit. 2019-10-12]. Dostupné z: https://leidensecurityandglobalaffairs. nl/articles/two-incompatible-approaches-to-governing-cyberspace-hinder-global-consensus.

[21] Srov. například art. 615-ter, 615-quater, 615-quinquies, Codice Penale, R. D. 19 ottobre 1930, n. 1938 (Trestní zákoník Italské republiky); art. 197 bis, 197 ter, 197 quater, 197 quinquies y ss. y 270 y ss., Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (Trestní zákoník Španělského království); art. 138ab, 139c, 139d, 161 sexies, 161 septies, 350a, 350b, Wet van 3 maart 1881, Wetboek van Strafrecht (Trestní zákoník Nizozemského království).

[22] Viz §§ 230 (neoprávněný přístup k počítačovému systému a nosiči informací), 231 (opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat) a 232 (poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti) zákona č. 40/2009 Sb., trestní zákoník.

[23] § 2 písm. a) zákona o kybernetické bezpečnosti.

[24] Podle § 2 písm. d) zákona č. 69/2018 Z. z., o kybernetickej bezpečnosti, se pojmem kyberprostor rozumí: „*globální dynamický otevřený systém sítí a informačních systémů, který tvoří aktivované prvky kybernetického prostoru, osoby vykonávající aktivity v tomto systému a vztahy a interakce mezi nimi*".

[25] Nařízení Evropského parlamentu a Rady (EU) 2019/881 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií (akt o kybernetické bezpečnosti).

Otázka kybernetické bezpečnosti se pochopitelně dostala i mezi agendu OSN, a to již v roce 1998.[26] Od té doby působilo v rámci OSN celkem pět skupin složených z vládních expertů (*Groups of Governmental Experts, GGEs*), jejichž úkolem bylo posoudit existující i potenciální hrozby v kyberprostoru a prostředky, kterými by jim bylo možné čelit.[27] Obavy z možného zneužití informačních a komunikačních technologií vyjádřil i generální tajemník OSN António Guterres, pro kterého představuje pokojné užívání kyberprostoru jednu z jeho klíčových priorit. Za tímto účelem bude ve spolupráci se členskými státy usilovat zejména o zvýšení povědomí o nových normách a principech regulujících chování v kyberprostoru, nutnosti jejich dodržování a případné odpovědnosti za jejich porušení.[28]

Přestože lze spatřovat určitou podobnost mezi vesmírem a kybernetickým prostorem,[29] už na první pohled je mezi nimi patrný jeden zcela zásadní rozdíl, který významně ovlivnil právě způsob právní úpravy regulující chování v nich učiněné. Zatímco do výzkumu a dobývání vesmíru se zapojily převážně (pokud ne jen a pouze) státy, kyberprostor je zatím spíše doménou nestátních aktérů – jednotlivců. Právo kybernetického prostoru se mohlo vyvinout stejným způsobem jako právo kosmické, tedy prostřednictvím mezinárodních smluv a jiných dokumentů mezinárodního práva,[30] nicméně právě kvůli účasti subjektů od států převážně odlišných, se na mezinárodněprávní scéně objevují dokumenty, které upravují pouze určité dílčí aspekty jednání v kyberprostoru (zejména počítačovou kriminalitu) a které jsou převážně výsledkem činnosti regionálních organizací,[31] nebo takové, které nejsou právně závazné.[32]

---

[26] UNGA. Resolution 53/70. *Developments in the field of information and telecommunications in the context of international security*. 4 January 1999, UN Doc. A/RES/53/70.

[27] V současné době ustavilo Valné shromáždění OSN jak novou skupinu vládních expertů, tak i pracovní skupinu (*Open-Ended Working Group, OEWG*), které mají za úkol pokračovat v tomto výzkumu v období 2019-2021, resp. 2019-2020.

[28] UNODA. Developments in the field of information and telecommunications in the context of international security. [online]. [cit. 2019-10-20]. Dostupné z: https://www. un. org/disarmament/ict-security/.

[29] Výzkum vesmíru znamenal začátek úplně nové doby, ve které lidstvo vstoupilo (stejně jako v případě kyberprostoru) do oblasti, kde pozemské hranice nehrají žádnou roli.

[30] NYMAN METCALF, K. A Legal View on Outer Space and Cyberspace: similarities and differences. *Tallinn Papers No. 10* [online]. CCDCOE, 2018, s. 1-2 [cit. 2019-10-10]. Dostupné https://ccdcoe. org/uploads/2018/10/Tallinn-Paper_10_2018. pdf

[31] COUNCIL OF EUROPE. *Convention on Cybercrime* (ze dne 23. 11. 2001, vstup v platnost dne 01. 07. 2004) ETS No. 185 (Úmluva o počítačové kriminalitě); COUNCIL OF EUROPE. *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* (ze dne 28. 01. 2003, vstup v platnost dne 01. 03. 2006) ETS No. 189 (Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů).

[32] Například UNGA. *Advancing responsible State behaviour in cyberspace in the context of international security*. 22 December 2018. UN Doc. A/RES/73/266; UNGGE. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. 22 July 2015. UN Doc. A/70/174; THE COMMONWEALTH. *Model Law on Computer and Computer Related Crime* [online]. 2017 [cit. 2019-10-20]. Dostupné z: https://thecommonwealth. org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime. pdf;

Vzhledem k tomu, že v současné době neexistuje žádná mezinárodní smlouva regulující chování v kyberprostoru, která by zavazovala větší počet států tvořících mezinárodní společenství, je na takové jednání nutné vztáhnout existující normy mezinárodního práva včetně mezinárodních obyčejů. S ohledem na povahu kybernetického prostoru, jako domény, která nemá hranice, jsou tato pravidla ovšem použitelná pouze v omezené míře.[33] V této souvislosti je nutné poukázat zejména na dva Tallinnské Manuály, které na půdě NATO připravila skupina mezinárodních expertů pod vedením profesora Michaela N. Schmitta, a které se pokouší osvětlit, jakým způsobem by měly být stávající normy mezinárodního práva aplikovány na jednání učiněná v kyberprostoru, a to jednak v době ozbrojeného konfliktu,[34] jednak v době míru.[35] Přestože se nejedná o mezinárodní smlouvy, ale pouze o nezávazné „soft law" dokumenty, autoři mají za to, že jejich práce odráží pozitivní právo („*lex lata*"), které se na jednání v kyberprostoru jednoznačně vztahuje. Ačkoli je možné rozporovat nestrannost autorů,[36] Tallinnské Manuály jsou doposud nejrozsáhlejšími díly, pojednávající o vztahu stávajících mezinárodněprávních norem a kybernetického prostoru. Vzhledem k tomu, že předmětem této práce je protiprávní jednání učiněné v době míru, základem pro tuto práci se stala pravidla obsažená v Tallinnském Manuálu 2.0, na který je na vhodných místech patřičně odkázáno.

SCHJOLBERG, S. *A Geneva Declaration for Cyberspace* [online]. 2016 [cit. 2019-10-20]. Dostupné z: https://www. cybercrimelaw. net/documents/Geneva_Declaration_2016. pdf.

[33] Nyman Metcalf, op. cit., s. 9.

[34] SCHMITT, M. N. *Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. New York: Cambridge University Press, 2013. ISBN 978-1-107-02443-4.

[35] SCHMITT, M. N. *Tallinn Manual 2.0 on the international law applicable to cyber operations*. 2. vyd. New York: Cambridge University Press, 2017. ISBN 978-1-107-17722-2 (Tallinn Manual 2.0).

[36] Činí tak například Papawadee Tanodomdej, podle kterého je z Manuálu patrný vliv NATO a podle kterého nelze přehlížet praxi jiných států, které se do kybernetických operací zapojují. Viz TANODOMDEJ, P. The Tallinn Manuals and the Making of the International Law on Cyber Operations. *Masaryk University Journal of Law and Technology* [online]. 2019, 13 (1), s. 67-86 [cit. 2019-10-11]. DOI: 10. 5817/MUJLT2019-1-4. ISSN 1802-5951. Dostupné z: https://journals. muni. cz/mujlt/article/view/11810.

2. Obecně o mezinárodněprávní odpovědnosti

Pro každý právní systém je příznačné, že porušení právně závazného pravidla chování (*primární povinnosti*) s sebou neodmyslitelně přináší negativní následky (*sekundární povinnosti*), které se liší v závislosti na povaze porušené normy. Zatímco ve vnitrostátním právu se může jednat například o trestní stíhání nebo nucený výkon primární povinnosti za pomoci státní moci, v právu mezinárodním, vzhledem k principu svrchované rovnosti mezi státy,[37] nepřipadají takové postupy v úvahu a na scénu nastupuje institut mezinárodněprávní odpovědnosti.[38]

Mezinárodněprávní odpovědnost tvoří soubor norem, které stanoví, za jakých okolností bude stát stižen právní odpovědností za porušení mezinárodního závazku a následky s tím spojené. Nejdůležitější principy mezinárodněprávní odpovědnosti nalezneme v Článcích o odpovědnosti státu za mezinárodně protiprávní chování (ARSIWA), které vypracovala Komise OSN pro mezinárodní právo a jejichž finální návrh byl Komisí přijat v roce 2001. Dokument sestává z 59 článků rozdělených do čtyř částí, které upravují předpoklady a náležitosti vzniku mezinárodněprávní odpovědnosti (obecné zásady mezinárodněprávní odpovědnosti, přičitatelnost chování státu, porušení mezinárodního závazku, odpovědnost státu ve spojení s chováním jiného státu, okolnosti vylučující protiprávnost), její obsah a provádění. Část čtvrtá kromě standardních závěrečných ustanovení obsahuje i důležitý čl. 58, který stanoví, že aplikace článků nebrání jakékoli individuální odpovědnosti podle mezinárodního práva jakékoli osoby jednající v zájmu státu. Přestože se jedná o dokument, který není právně závazný,[39] obecně panuje shoda, že většina pravidel v něm obsažených odráží mezinárodní obyčejové právo mezinárodněprávní odpovědnosti,[40] čemuž přisvědčuje i bohatá judikatura mezinárodních soudů.[41]

---

[37] Jedná se o obecnou zásadu mezinárodního práva, podle které jsou si „*všechny státy právně rovny, mají rovná práva a povinnosti a jsou rovnými členy mezinárodního společenství*." Blíže viz POTOČNÝ, M. Zásada svrchované rovnosti států. *Mezinárodní vztahy*. Praha: Ústav mezinárodních vztahů. 1968, 3 (4), s. 3-9.

[38] MALENOVSKÝ, J. *Mezinárodní právo veřejné: obecná část a poměr k jiným právním systémům*. 6., upr. a dopl. vyd. Brno: Doplněk, 2014, s. 286. ISBN 978-80-7380-531-9.

[39] Přestože dokument nemá formu závazné mezinárodní úmluvy, Valné shromáždění OSN ho přijalo alespoň ve formě rezoluce č. 56/83 a nadále průběžně sleduje, jak se dokument v praxi uplatňuje (viz například UNGA. *Responsibility of States for internationally wrongful acts. Compilation of decisions of international courts, tribunals and other bodies. Report to the Secretary-General*. 21 April 2016. UN Doc A/71/80), přičemž stále považuje za vhodné, aby články byly vtěleny do závazné mezinárodní smlouvy (viz například UNGA. *Summary record of the 31st meeting*. 2 December 2016. UN Doc A/C. 6/71/SROV. 31).

[40] BORDIN, F. L. Reflections of Customary International Law: The Authority of Codification Conventions and ILC Draft Articles in International Law. *International and Comparative Law Quarterly* [online]. 2014, 63 (3), s. 535-568 [cit. 2019-10-13]. ISSN 14716895. Dostupné z: http://heinonline. org/HOL/Page?handle=hein. journals/incolq63&div=33.

[41] Srov. zprávu Valného shromáždění generálnímu tajemníkovi OSN č. A/71/80, op. cit.

Vzhledem k tomu, že analýza mezinárodněprávní odpovědnosti by značně přesáhla meze této práce, budou v následujících kapitolách pouze stručně představeny úhelné kameny tohoto institutu, na kterých bude poté stavět i výklad o odpovědnosti státu v kyberprostoru, který naváže v části třetí.

2.1. Porušení mezinárodního závazku

O mezinárodně protiprávní chování státu se jedná, pokud je chování státu přičitatelné podle mezinárodního práva a zakládá porušení mezinárodního závazku státu.[42] Protiprávní chování může být způsobeno aktivním jednáním i opomenutím konat tam, kde to bylo vyžadováno,[43] přičemž vznik újmy ani zavinění nepředstavují samostatný prvek mezinárodněprávní odpovědnosti, protože ty už představují „*inherentní náležitost pojmu protiprávní chování*".[44] Aby tedy došlo k nástupu mezinárodněprávní odpovědnosti, postačí, že došlo k mezinárodně protiprávnímu jednání, které je státu přičitatelné.

Porušení mezinárodněprávního závazku je považováno za tzv. objektivní prvek mezinárodně protiprávního chování.[45] Stát poruší mezinárodní závazek, když jeho chování není ve shodě s tím, co se od něho tímto závazkem požaduje, bez ohledu na jeho původ a povahu.[46] Porušená povinnost tedy může vyplývat z mezinárodní smlouvy, mezinárodního obyčeje nebo může spočívat v neplnění závazného rozhodnutí soudu, popř. v pomoci nebo podpoře jiného státu při spáchání mezinárodně protiprávního chování.[47] V každém případě se však musí jednat o porušení normy mezinárodního práva. Nejedná se o mezinárodně protiprávní chování, pokud stát poškozuje zájmy jiného státu, avšak neporušuje žádnou mezinárodněprávní normu (*nevlídný akt*), nebo pokud svým jednáním porušuje pouze normu vnitrostátní.[48]

V důsledku porušení primárního pravidla tak k původní povinnosti, která porušením nezaniká, přistupuje další závazek, který takový stát nepřímo odrazuje od pokračování v protiprávním jednání a od dalšího porušování mezinárodněprávních norem.[49]

---

[42] ČEPELKA, Č. a P. ŠTURMA. *Mezinárodní právo veřejné*. 2. vydání. Praha: C. H. Beck, 2018, s. 381. Academia iuris (C. H. Beck). ISBN 978-80-7400-721-7.
[43] DAVID, V., P. SLADKÝ a F. ZBOŘIL. *Mezinárodní právo veřejné s kazuistikou*. Praha: Leges, 2008, s. 309. Student (Leges). ISBN 978-80-87212-08-0.
[44] Čepelka a Šturma, op. cit., s. 383.
[45] Malenovský, op. cit., s. 294.
[46] Články o odpovědnosti státu za mezinárodně protiprávní chování, čl. 12 (ARSIWA). Text článků včetně komentáře dostupný z http://legal. un. org/ilc/texts/instruments/english/commentaries/9_6_2001. pdf.
[47] DIXON, M. *Textbook on international law*. 6th ed. New York: Oxford University Press, 2007, s. 244. ISBN 978-0-19-920818-0.
[48] David, Sladký a Zbořil, op. cit., s. 310-311.
[49] Malenovský, op. cit., s. 286.

2.2. Přičitatelnost jednání

Stát, jakožto abstraktní entita, není schopen skutečně fyzicky jednat, své funkce tak vykonává „zprostředkovaně“ prostřednictvím svých orgánů.[50] Jako „přičitatelnost“ se pak označuje proces, na základě kterého mezinárodní právo určí, zda jednání té které fyzické osoby nebo jiného „zprostředkovatele“ může být považováno za jednání státu, a může být tudíž schopné založit jeho odpovědnost podle mezinárodního práva.

Základy přičitatelnosti chování státu jsou upraveny v kapitole II. ARSIWA a dají se rozčlenit do tří kategorií. První zahrnuje články 4 – 7 a hovoří o orgánech nebo organismech státu, kteří vykonávají jeho svrchovanou moc; druhá zahrnuje čl. 8 a týká se tzv. *de facto* orgánů, tedy osob jednajících na základě pokynu nebo nařízení nebo pod kontrolou státu; a konečně články 9 – 11, které se týkají některých zvláštních způsobů přičitatelnosti jednání učiněných nestátními aktéry bez předchozího pokynu nebo nařízení ze strany státu.

2.2.1. Orgány státu *de iure*

Základní předpoklad mezinárodněprávní odpovědnosti, tedy pravidlo že stát odpovídá za jednání svých orgánů, je vyjádřen v čl. 4 ARSIWA,[51] který tedy kodifikuje to, co již představuje součást mezinárodního obyčejového práva.[52] Dosah článku je poměrně široký, a to zejména s ohledem na skutečnost, že klasická tripartita státní moci není ve všech právních řádech důsledně reflektována, ať už *de facto* či dokonce *de iure*.

Většina protiprávních jednání bude tradičně pocházet od orgánů moci výkonné, které nejčastěji slouží k přímému výkonu státních funkcí. Protiprávního jednání se nicméně mohou dopustit i orgány moci zákonodárné, a sice prostřednictvím přijímání zákonů, nařízení a jiných aktů, které budou v rozporu s přijatými mezinárodními závazky; nebo orgány moci soudní, kdy

[50] *German Settlers in Poland*, (1923) PCIJ Ser. B No. 6, para. 22: „*States can only act by and through their agents and representatives*“

[51] Čl. 4 zní: (1) *Chování jakéhokoli orgánu státu se považuje za chování státu podle mezinárodního práva, ať jde o orgán vykonávající zákonodárnou, výkonnou, soudní nebo jakoukoli jinou funkci, ať zaujímá jakékoli postavení v organizaci státu a má jakoukoli povahu jako orgán ústřední vlády nebo územní jednotky státu.*
(2) Orgánem je jakákoli osoba nebo organizace, která má právní postavení v souladu s vnitrostátním právem státu.
České překlady ARSIWA převzaty z materiálu poskytnutého doc. JUDr. PhDr. Veronikou Bílkovou Ph.D., E.MA

[52] *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights*, ICJ Rep. 1999, p. 62, para. 87: „*According to a well-established rule of international law, the conduct of any organ of State must be regarded as an act of that State. This rule.. . is of a customary character*. “

se nejčastěji bude jednat o porušení zákazu *denegatio iustitiae* nebo chybný výklad mezinárodních smluv.[53]

Za určitých okolností ale stát může být shledán odpovědným i za chování entity, která není jeho orgánem. ARSIWA v této souvislosti rozlišuje dvě situace – první, která míří na případy, kdy je výkon vládní moci svěřen subjektu, který není orgánem tohoto státu, a druhou, kdy určité subjekty jednají na základě pokynu, nařízení nebo pod kontrolou státu, která je upravena v čl. 8 ARSIWA a která je popsána níže v bodu 2.2.2.

Prvně jmenovanou situaci upravuje čl. 5 ARSIWA,[54] který nabývá na významu se zvyšujícím se počtem států, které se rozhodnou vnitrostátním právem zmocnit určitý subjekt k výkonu jejich „vládních funkcí". Co se konkrétně rozumí pojmem „vládní funkce", je předmětem diskuzí, nicméně jako nejtypičtější příklady bývá uváděno zmocnění k výkonu kontroly nad imigrací nebo správa věznic.[55]

Kromě výše uvedených situací pamatuje ARSIWA i na situaci, kdy orgán státu A vykonává vládní moc pro stát B. Chování orgánu státu, který byl dán státu k dispozici jiným státem, je tedy považováno za chování tohoto státu, jestliže tento orgán jedná při výkonu funkcí vládní povahy státu, kterému byl dán k dispozici.[56] Musí se pochopitelně jednat o orgán ve smyslu čl. 4 ARSIWA, který vykonává vládní moc pro zmocněný stát.[57] Takový orgán musí být nejenom zmocněn k výkonu funkcí náležejících jinému státu, nýbrž musí být i součástí státního aparátu zmocněného státu a podléhat řízení a kontrole tohoto státu, nikoli státu-zmocněnce.[58]

Jednání orgánu státu, osoby nebo organismu, kterému je svěřen výkon funkcí vládní povahy, je považováno za jednání státu i v případě, kdy takový orgán, osoba nebo organismus překročí svou pravomoc nebo poruší služební pokyny.[59] Není tomu tak ovšem vždy, ale pouze v situaci, kdy takový subjekt jedná jménem státu a nikoli jménem svým. Najít hranici mezi

[53] *La Grand Case (Germany v. U. S.*), ICJ Rep. 2001, p. 466. V této věci byli bratři LaGrandovi odsouzeni k trestu smrti, aniž by bylo přihlédnuto k jejich právům, které jim zaručuje Vídeňská úmluva o konzulárních stycích.
[54] Čl. 5 zní: „*Chování osob nebo organismů, které není orgánem státu podle čl. 4, který ale byl zmocněn právem státu k výkonu vládní moci, je považováno za chování státu podle mezinárodního práva, za předpokladu, že tato osoba nebo organismus, jednala v rámci své působnosti*. "
[55] CRAWFORD, J. *State Responsibility: The General Part*. New York: Cambridge University Press, 2013, s. 127-128. ISBN 978-0-521-82266.
[56] ARSIWA - komentář, čl. 6 odst. 1.
[57] ARSIWA - komentář, čl. 6 odst. 5.
[58] ARSIWA - komentář, čl. 6 odst. 4.
[59] ARSIWA, čl. 7.

jednáním v soukromé záležitosti dané entity a jednáním *ultra vires* ovšem může být někdy skutečně obtížné.[60]

V závislosti na povaze primárního závazku, orgán samotný nemusí být přímým pachatelem protiprávního jednání, ale postačí, že o protiprávním jednání věděl a nepokusil se mu zabránit.[61]

2.2.2. Orgány státu *de facto*

Jak již bylo popsáno shora, situace, kdy je určitá entita vnitrostátním právem přímo jako státní orgán označena, nečiní při založení odpovědnosti státu větší potíže.[62] Zajímavou otázku ovšem představuje situace, která je reflektována v čl. 8 ARSIWA, a která míří na případy, kdy určitá entita jedná na základě pokynu, nařízení nebo pod kontrolou státu.[63] Pokud by mezinárodní právo nebralo v potaz možnost svěření státních pravomocí soukromým subjektům, státy by se své odpovědnosti mohly velice snadno zbavovat.[64]

Ačkoli teoreticky se situace, kdy stát udělí určité osobě nebo skupině osob pokyn, aby obstaraly určitou záležitost jeho jménem,[65] jeví jako poměrně srozumitelná, aplikace tohoto pravidla v praxi přináší celou řadu otázek, například zda musí být orgán zmocněn k určitému konkrétnímu jednání, či zda postačí zmocnění generální.[66] Ještě problematičtější je potom přičtení státu chování osob, které nejsou jeho orgány a které jednaly na základě jeho nařízení nebo pod jeho kontrolou, neboť ARSIWA blíže nespecifikuje stupeň řízení nebo standard kontroly, který je k založení odpovědnosti státu za takové jednání vyžadován. Tyto otázky se proto staly předmětem výkladu jak ze strany MSD, tak ze strany ICTY či jiných mezinárodních

[60] CRAWFORD, J., A. PELLET a S. OLLESON (eds.). *The law of international responsibility*. New York: Oxford University Press, 2010, s. 263. ISBN 978-0-19929697-2.
[61] V notoricky známé věci Korfského průlivu byla Albánie shledána odpovědnou za přítomnost min ve svých pobřežních vodách, přestože je tam sama neumístila, a to na základě skutečnosti, že ačkoli o jejich přítomnosti věděla, neinformovala o této skutečnosti lodě proplouvající tímto územím. Tato povinnost se v doktríně označuje též jako závazek „due diligence". *Corfu Channel Case (UK v. Albania)*, ICJ Rep. 1949, p. 4 (Korfský průliv).
[62] ARSIWA – komentář, čl. 4 odst. 11.
[63] ARSIWA, čl. 8.
[64] Crawford, op. cit., s. 141.
[65] *Case concerning U. S. Diplomatic and Consular Staff in Tehran (U. S. v. Iran*), ICJ Rep. 1980, p. 3, paras. 29–30 (Diplomatický a konzulární personál USA v Teheránu).
[66] Crawford, op. cit., s. 145.

soudních orgánů. Zatímco ve věci Nicaragua[67] použil MSD tzv. „test efektivní kontroly“,[68] v kontextu věci Tadić[69] byl tento test shledán nepřesvědčivým a odvolací senát ICTY se přiklonil k tzv. „testu celkové kontroly“.[70] Nicméně po dalších osmi letech se MSD v případě Bosenské genocidy, tedy případu který se odehrál v kontextu stejných skutkových okolností jako případ Tadić, opět přiklonil k testu efektivní kontroly a rozhodnutí odvolacího senátu ICTY podrobil ostré kritice.[71] Vzhledem k tomu, že mezi jednotlivými případy uplynulo třináct let, byl tento odlišný postup obou soudů brán jako důkaz vývoje mezinárodního práva.[72] Co se týče regionálních soudů, tak ESLP ve věci *Loizidou proti Turecku* rozhodl o odpovědnosti Turecka za jednání severokyperských jednotek za použití testu „efektivně-celkové kontroly“[73] a ve spojených věcech *Behrami* a *Saramati* rozhodl za použití testu „nejvyšší pravomoci a kontroly“.[74]

Uvedené dokládá, že názory odborníků se na tyto otázky liší a že ke ztotožnění *de facto* orgánů se státními orgány bude docházet pouze ve výjimečných případech, neboť oba soudy ve své judikatuře vymezily poměrně striktní pravidla takové přičitatelnosti.[75] Test efektivní a celkové kontroly bude blíže rozebrán níže v kapitole 3.3.3 pojednávající o konceptu kontroly v kyberprostoru.

---

[67] V této věci musel Mezinárodní soudní dvůr zodpovědět otázku, zda jsou Spojené státy americké odpovědné za porušování mezinárodního práva ze strany povstaleckých jednotek (*contras*), které materiálně podporovaly. Vzhledem k tomu, že jednotky nebyly na USA zcela závislé, MSD shledal, že USA nemohou být shledány odpovědnými za veškeré jejich jednání bez dalšího, protože nad nimi nedisponovaly dostatečným stupněm kontroly. Blíže viz *Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America*). Merits (Judgment). ICJ Rep. 1986, p. 14. (Některé vojenské a polovojenské činnosti v Nikaragui a proti ní).

[68] MSD se nepokoušel blíže definovat standard kontroly, pouze se omezil na konstatování, že k založení odpovědnosti je nutné prokázat, že stát vykonával „efektivní kontrolu“ nad daným jednáním. Viz *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, op. cit., para. 65.

[69] Přestože jurisdikce ICTY byla omezena na souzení jednotlivců a nikoli států, otázku přičitatelnosti ICTY posoudil jako předběžnou v rámci zjištění, zda se jednalo o mezinárodní nebo vnitrostátní konflikt. *Prosecutor v. Dusko Tadić*. ICTY Case No. IT-94-1-T, Trial Chamber, 7 May 1997.

[70] Podle ICTY je nejprve nutné prokázat, že stát disponuje „celkovou kontrolou“ nad určitou osobou nebo skupinou osob. Celková kontrola pak nespočívá v pouhém financování nebo logistické podpoře, ale zahrnuje i koordinaci a plánování jednání takových osob. K založení odpovědnosti ovšem není nutné, aby stát plánoval veškeré operace takových osob. *Prosecutor v. Dusko Tadić, Decision on the Defense Motion for Intercutory Appeal on Jurisdiction*. ICTY Case No. IT-94-1-AR, Appeals Chamber.

[71] *Case concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Yugoslavia*). ICJ Rep. 2007 (Bosenská genocida).

[72] GREENWOOD, CH. The Development of International Humanitarian Law by the International Criminal Tribunal for the Former Yugoslavia. *Max Planck Yearbook of United Nations Law* [online]. 1998, 2, s. 97-140 [cit. 2019-10-19]. ISSN 13894633. Dostupné z: https://www. mpil. de/files/pdf2/mpunyb_greenwood_2. pdf.

[73] ESLP. *Loizidou v. Turkey* (merits), 18 December 1996, Reports of Judgments and Decisions 1996-VI.

[74] ESLP. *Behrami and Behrami v. France* and *Saramati v. France, Germany and Norway*, nos. 71412/01 and 78166/01, 2 May 2007.

[75] ÁLVAREZ ORTEGA, E. L. The attribution of international responsibility to a State for conduct of private individuals within the territory of another State. *InDret: Revista para el análisis del derecho* [online]. 2015, (1), s. 10 [cit. 2019-10-20]. Dostupné z: http://www. indret. com/pdf/1116_es. pdf.

2.2.3. Zvláštní případy přičitatelnosti jednání státu

Ještě zajímavější otázku představují situace, kdy určité entity jednají zcela bez předchozího pokynu nebo nařízení ze strany státu, a které jsou upraveny v čl. 9 – 11 ARSIWA.

Čl. 9 ARSIWA se v praxi aplikuje velmi zřídka.[76] Komise pro mezinárodní právo přesto přibližuje tři podmínky, za kterých je možné jej použít - za prvé, nestátní aktéři musí vykonávat vládní moc ze své vlastní iniciativy; k jednání musí docházet v případě, kdy oficiální úřady neplní své úkoly nebo vůbec neexistují; a konečně zde musí být přítomny takové okolnosti, které vyžadují výkon těchto prvků úřední moci.[77] Toto ustanovení nemíří na situace, kdy se občanům podaří zformovat novou vládu *de facto*, protože má-li taková vláda efektivní kontrolu nad územím, aniž by byla vládou *de iure*, je přesto považována za orgán státu ve smyslu čl. 4 ARSIWA.

Naproti tomu v případě, kdy je výkon vládní moci zajišťován povstaleckým hnutím, které zároveň nevykonává efektivní kontrolu nad celým územím státu, odpovědnost státu nebude založena, protože obecně platí, že takové hnutí nemůže být ztotožňováno se státem, proti kterému bojuje. Pokud by se ovšem povstalecké hnutí stalo novou vládou, bude se aplikovat čl. 10 ARSIWA, který rozlišuje dvě situace - první, kdy se povstalecké hnutí stane novou vládou; a druhou, kdy chování povstaleckého hnutí vyústí v založení nového státu na části území předchozího státu nebo na území pod jeho správou. Pro obě situace čl. 10 ARSIWA stanoví, že v takových případech se chování povstaleckého hnutí považuje za chování státu, resp. tohoto nového státu. V praxi ale často budou nastávat situace, kdy bude na státním území operovat více než jedno povstalecké hnutí, přičemž ustavit novou vládu, resp. vytvořit nový stát, se může podařit pouze jednomu nebo vůbec žádnému z nich.

V případě kdy není jednání přičitatelné podle žádného z výše uvedených článků, je takové chování považováno za chování státu v rozsahu, ve kterém stát uzná a přijme dané chování jako své vlastní. Typickým příkladem aplikace tohoto článku je případ *Diplomatického a konzulárního personálu USA v Teheránu*, kdy Írán přešel od opomenutí konat k oficiálnímu potvrzení nastalé situace a jejímu vědomému udržování,[78] nebo případ *Gabčíkovo-Nagymaros*

[76] Crawford, op. cit., s. 168.
[77] ARSIWA - komentář, čl. 9 odst. 3 – 6.
[78] Ozbrojená skupina několika set osob obsadila budovu velvyslanectví USA a zajala všechny členy diplomatické i konzulární mise, přičemž íránské orgány nejprve nepodnikly žádné kroky k tomu, aby takové situaci zabránily, a posléze dokonce tuto situaci potvrdily a dále vědomě udržovaly. (*Case concerning U. S. Diplomatic and Consular Staff in Tehran*, op. cit., para. 91).

v kontextu sukcese států.[79] K přijetí jednání ovšem nemusí pokaždé dojít výslovně, za určitých okolností je přípustné i nepřímé vyjádření takového uznání nebo převzetí.[80]

2.3. Okolnosti vylučující protiprávnost

V některých situacích nedojde ke vzniku mezinárodněprávní odpovědnosti, přestože se může zdát, že objektivní i subjektivní prvek byl naplněn. Jedná se o případy, v nichž nastane některá z okolností, které vylučují protiprávnost daného chování. Tyto nemají vliv na platnost ani trvání mezinárodního závazku, neboť odpovědnost nenastává pouze po dobu, po níž některá z těchto okolností trvá.[81] Mezi takové okolnosti se řadí souhlas, sebeobrana, protiopatření, vyšší moc, tíseň a nouze.[82]

Zatímco při standardních situacích leží důkazní břemeno na státu, který se dovolává mezinárodní odpovědnosti jiného státu, v případě okolností vylučujících protiprávnost musí jejich existenci prokázat stát, který se jich dovolává.[83]

2.4. Právní následky mezinárodně protiprávního jednání

Vzhledem k tomu, že vznik škody není podstatnou náležitostí vzniku mezinárodní odpovědnosti, nelze se domnívat, že by tato obsahovala pouze povinnost státu odčinit způsobenou škodu. Obecně, následky protiprávního chování se budou lišit v závislosti na povaze porušeného primárního pravidla. Tak například jedná-li se o protiprávní chování pokračujícího charakteru, vzniká v první řadě povinnost takové chování ukončit. Pokud to odůvodňují okolnosti, může být rovněž vyžadováno, aby stát poskytl ujištění a záruky, že se protiprávní chování nebude opakovat. Až posléze se přikročí k reparaci, která může mít, opět v závislosti na okolnostech, formu restituce, kompenzace nebo satisfakce. Jak již ale bylo naznačeno výše, porušení primárního závazku v žádném případě nezbavuje stát povinnosti tento závazek splnit.

[79] *Gabčíkovo-Nagymaros Project (Hungary v. Slovakia*), ICJ Rep. 1997, p. 7.
[80] Crawford, op. cit., s. 187.
[81] Sladký, David a Zbořil, op. cit., s. 316.
[82] ARSIWA, čl. 20 – 25.
[83] Malenovský, op. cit., s. 300.

3. Mezinárodněprávní odpovědnost v kyberprostoru

Zatímco dříve docházelo ke vzniku vážných a rozsáhlých škod pouze působením tak velkých aktérů, jako jsou státy, dnes v důsledku kyberneticko-technické revoluce mohou obrovské škody způsobit i mnohem méně sofistikovaní aktéři, jako např. více či méně organizované skupiny jednotlivců či i jednotlivci samotní,[84] neboť v porovnání s kinetickými útoky, kybernetické zbraně jsou dostupnější než zbraně konvenční a navíc, většina kybernetických operací nevyžaduje až tak vysoké investice ani speciální zařízení.[85] Po zkušenostech z nedávných let[86] je již nepochybné, že kybernetické operace mohou porušovat nejen národní práva jednotlivých států, ale též právo mezinárodní. Zájem na regulaci jednání v kyberprostoru by tak mělo mít celé mezinárodní společenství, neboť přestože nám na jedné straně kyberprostor poskytuje nebývalé výhody, na straně druhé jeho anonymní prostředí představuje dokonalý ráj pro pachatele, které se velice často nepodaří vůbec identifikovat, což přináší problémy zejména pro určení státu, který za danou kybernetickou operaci ponese odpovědnost. Lze očekávat, že v následujících letech bude se stále zvyšující se úrovní provedení jednotlivých kybernetických operací i odhalení skutečného původce, a v souvislosti s tím i přičtení jeho jednání konkrétnímu státu, ještě obtížnější. Z tohoto důvodu je nutné si vypomoci právními konstrukcemi, aby se kyberprostor nestal „šedou zónou", tedy bezpečným úkrytem, kam by se státy uchylovaly k páchání protiprávních činů, za které by jim fakticky nehrozily žádné negativní následky.[87]

Následující kapitoly se pokouší aplikovat stávající pravidla mezinárodní odpovědnosti na jednání učiněné v kyberprostoru. Pozornost je nejprve věnována pojmům suverenita a výsost a poté se přesouvá již k samotné otázce mezinárodní odpovědnosti. Nejdříve bude diskutován

---

[84] PAYNE, T. Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations. *Lewis & Clark Law Review* [online]. 2016, 20 (2), s. 684-685 [cit. 2019-10-21]. ISSN 1557-6582. Dostupné z: http://heinonline. org/HOL/Page?handle=hein. journals/lewclr20&div=22.

[85] Přestože se jistě objeví technologie, jejichž vývoj i „obsluha" bude nákladnější, obecně platí, že kybernetická operace bude pro stát pravděpodobně výhodnější než klasická kinetická operace, provedená např. za pomoci těžké bojové techniky, přičemž může být stejně efektivní, ne-li efektivnější. Srov. ROSCINI, M. World Wide Warfare - Jus ad Bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law* [online]. 2010, 14 (1), s. 86-87 [cit. 2019-11-27]. ISSN 13894633. Dostupné z: https://www.mpil.de/files/pdf3/mpunyb_03_roscini_141.pdf.

[86] Vzpomeňme zejména útoky na Estonsko v roce 2007 (NATO. Six Colours: War in cyberspace. In: *YouTube* [online]. 27 April 2009 [cit. 2019-11-09]. Dostupné z: https://www. youtube. com/watch?v=oGZkCdpPLBE), nebo virus Stuxnet v roce 2010, který Íránu způsobil rozsáhlé škody na jeho jaderném programu (HAATAJA, S. a A. KHTAR-KHAVARI. Stuxnet and International Law on the Use of Force: An Informational Approach. *Cambridge International Law Journal* [online]. 2018, 7 (1), s. 99-121 [cit. 2019-11-04]. Dostupné z: https://heinonline. org/HOL/LandingPage?handle=hein. journals/cajoincla7&div=8&id=&page=).

[87] SCHMITT, M. N. Grey Zones in the International Law of Cyberspace. *Yale Journal of International Law* [online]. 2017, 42 (2) [cit. 2019-10-27]. Dostupné z: https://ssrn. com/abstract=3180687.

prvek objektivní (ve vztahu ke kyberprostoru se jedná o vybraná porušení pravidel primárního práva) a poté i prvek subjektivní, tedy otázka přičitatelnosti jednání konkrétnímu státu. Stručně bude nastíněna též problematika protiopatření.

3.1. Suverenita, územní a osobní výsost v kyberprostoru

Než přikročím k samotné analýze mezinárodní odpovědnosti za jednání v kyberprostoru, dovolím si úvodem ještě několik poznámek k pojmům suverenita, územní a osobní výsost a jejich uplatnění v kyberprostoru, neboť poslouží jako základní stavební kámen při výkladu, který bude následovat.

Státní suverenita je tradičně popisována jako „*samostatnost a nezávislost jak uvnitř, tak i vně státu při uskutečňování vnitřní i zahraniční politiky"*.[88] Od pojmu suverenita je pak nutné odlišit jednotlivá oprávnění, kterými stát v rámci své svrchované moci disponuje. Čepelka a Šturma je označují též jako tzv. kompetence a definují je jako „*mezinárodněprávní oprávnění k výkonu určitých pravomocí jednak vzhledem k prostoru, uvnitř kterého vykonává svrchovanou moc (území), jednak vzhledem k osobám spojeným s ním právním svazkem občanství"*,[89] což významově odpovídá pojmům územní a osobní výsost (*territorial and personal jurisdiction*).

Přestože je mezinárodní právo tradičně „teritoriálně zaujaté"[90] a kyberprostor je považován za sféru, která postrádá jakékoli hranice, mohlo by se snadno zdát, že nad ním státy svou svrchovanou moc nemohou uplatňovat. S takovým tvrzením se ovšem nelze ztotožnit a je zapotřebí vycházet z premisy, že „*kybernetické operace se odehrávají na určitých územích, protože vždy budou buď prováděny z určitého zařízení, které se ve světě skutečně fyzicky nachází, anebo budou vedeny alespoň určitou osobou, nad kterou státy mohou svou svrchovanou moc uplatňovat*".[91] Žádný stát sice nemůže uplatnit svou suverenitu nad kyberprostorem jako celkem, může však vykonávat některá svá dílčí oprávnění, některé své „kompetence", vůči jeho součástem, a sice buď z titulu územní výsosti vůči zařízením nebo osobám, které se na jeho území nacházejí, anebo z titulu výsosti osobní, vůči pachatelům nebo

[88] KÖNIGOVÁ, L. Teorie státní suverenity a praxe intervence. *Mezinárodní vztahy* [online]. 2001, (3), 41-58 [cit. 2019-10-31]. Dostupné z: https://mv. iir. cz/article/view/691/736.
[89] Čepelka a Šturma, s. 39.
[90] BÍLKOVÁ V. Území státu a územní změny. In: ŠTURMA P. (ed.) a kol. *Mezinárodní právo a státní území*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2015, s. 15. ISBN 978-80-87975-42-8.
[91] Tallinn Manual 2.0, Rule 1, paras. 3 – 5.

obětem, kteří budou jeho občany.[92] I v souvislosti s kyberprostorem může docházet k uplatňování pravomocí státu mimo jeho území, jejich rozsah se však bude, mimo jiné, lišit v závislosti na tom, „*zda se jedná o výkon moci zákonodárné, výkonné, nebo soudní*“.[93]

Vzhledem k výše uvedenému tak i kybernetické operace mohou představovat narušení suverenity určitého státu, neboť tento vykonává své svrchované pravomoci nad některými jeho součástmi.[94] Jednotlivá narušení suverenity, ke kterým může v kyberprostoru docházet, jsou předmětem výkladu v následující kapitole.

3.2. Porušení mezinárodního závazku

První nezbytnou podmínkou k tomu, aby bylo vůbec možné o mezinárodněprávní odpovědnosti státu uvažovat, je existence porušení mezinárodního závazku, tedy naplnění tzv. objektivního prvku mezinárodní odpovědnosti.[95] V mezinárodním právu obecně platí, že stát nese odpovědnost za protiprávní jednání zakládající porušení mezinárodního závazku, které je mu přičitatelné.[96] Ve vztahu ke kyberprostoru Tallinnský Manuál stanoví, že stát odpovídá „*za veškeré jednání s kyberprostorem související, pakliže je mu takové chování přičitatelné a zakládá porušení mezinárodněprávního závazku“*.[97] Pojem „jednání s kyberprostorem související“ byl použit záměrně s cílem zdůraznit skutečnost, že za určitých okolností státy odpovídají i za jednání, které buď nevykonaly samy, anebo ho nevykonaly přímo v kybernetickém prostoru – konkrétně může jít například o „*jednání jiných států nebo nestátních aktérů, kterým daný stát poskytl určitý software, anebo kterým umožnil užívání jeho kybernetické infrastruktury*“,[98] či o situace, kdy stát nepodnikl kroky nezbytné k zamezení tomu, aby jeho území bylo využíváno pro jednání odporující právům jiného státu.[99]

Vzhledem k tomu, že neexistuje žádný ucelený právní předpis, který by stanovil mezinárodněprávní povinnosti všech států, závazky jednotlivých států se liší v závislosti na obsahu a množství uzavřených mezinárodních smluv nebo jiných dokumentů mezinárodního

[92] KITTICHAISAREE, K. *Public International Law of Cyberspace*. Springer, 2017, s. 23-25. DOI https://doi.org/10.1007/978-3-319-54657-5. ISBN 978-3-319-54657-5. ISSN 2352-1910.
[93] Srov. blíže Tallinn Manual 2.0, Rule 10 a 11.
[94] Tallinn Manual 2.0, Rule 4. Blíže viz SCHMITT, M. a L. VIHUL. Respect for Sovereignty in Cyberspace. *Texas Law Review* [online]. 2017, 95 (7), s. 1639 – 1676 [cit. 2019-10-27]. Dostupné z: http://heinonline.org/HOL/Page?handle=hein. journals/tlr95&div=61.
[95] Srov. výše kapitolu 2.1.
[96] Čepelka a Šturma, op. cit., s. 381–383.
[97] Tallinn Manual 2.0, Rule 14.
[98] Tallinn Manual 2.0, Rule 14, paras. 4 – 10.
[99] Tallinnský Manuál tuto povinnost označuje též jako tzv. povinnost *due diligence*. Srov. Tallinn Manual 2.0, Rules 6 and 7.

práva.[100] I přes tyto rozdíly ovšem existují určitá pravidla, která zavazují všechny státy, přičemž níže budou rozebrána pouze ta z nich, jejichž porušení připadá ve vztahu ke kyberprostoru nejčastěji v úvahu. Jedná se zejména o různé stupně narušení suverenity jednotlivých států.[101] Kromě odpovědnosti státu za protiprávní jednání vůči jinému státu může v kyberprostoru docházet též k odpovědnosti za protiprávní jednání vůči jednotlivci z titulu porušování mezinárodního práva lidských práv. V této souvislosti bude pravděpodobně nejčastěji docházet k porušování práva na soukromí osob, které se staly obětí hromadného sledování ze strany státu.[102] S ohledem na rozsah této práce nebude tato otázka blíže řešena.

Porušení mezinárodního závazku má pro odpovědnost státu relevanci, pokud bude naplněn též subjektivní prvek. Níže uvedené závěry se tedy pochopitelně uplatní pouze v případě, že dané protiprávní jednání bude státu přičitatelné.[103]

3.2.1. Zákaz hrozby a použití síly

Článek 2 odst. 4 Charty OSN ukládá členským státům povinnost vystříhat se „*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*“.[104] Toto pravidlo je považováno též za výraz mezinárodního obyčejového práva a za kogentní normu,[105] přičemž úzce souvisí též s čl. 51 Charty OSN, který přiznává právo na sebeobranu vůči ozbrojenému útoku,[106] které představuje, vedle opatření Rady bezpečnosti podle kapitoly VII Charty OSN, jedinou výjimku ze zákazu použití síly. Vzhledem

[100] DAVID, V. a kol. *Mezinárodní právo veřejné s kazuistikou*. 2., aktualiz. a přeprac. vyd. Praha: Leges, 2011, s. 328. Student (Leges). ISBN 978-80-87212-86-8.
[101] Tallinn Manual 2.0, Rule 4.
[102] Srov. blíže např. HUXTABLE, H. E.T. Phoned Home...They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance. *Security* [online]. 2019, 28 (1-4), s. 92-112 [cit. 2019-11-29]. DOI: 10.1163/18750230-02801010. ISSN 18747337. Dostupné z: https://brill.com/view/journals/shrs/28/1-4/article-p92_92.xml?lang=en; nebo WATT, E. The role of international human rights law in the protection of online privacy in the age of surveillance. In: *2017 9th International Conference on Cyber Conflict (CyCon)* [online]. IEEE, 2017, s. 93-107 [cit. 2019-11-29]. DOI: 10.23919/CYCON.2017.8240330. ISSN 2325-5374. Dostupné z: http://ieeexplore.ieee.org/document/8240330/.
[103] O přičitatelnosti ve vztahu ke kyberprostoru je blíže pojednáno v kapitole 3.3.
[104] Čl. 2 odst. 4 přílohy k vyhlášce ministra zahraničních věcí č. 30/1947 Sb., o chartě Spojených národů a statutu Mezinárodního soudního dvora (Charta OSN).
[105] BÍLKOVÁ, V. *Úprava vnitrostátních ozbrojených konfliktů v mezinárodním humanitárním právu*. Praha: Univerzita Karlova v Praze, Právnická fakulta v nakl. IFEC, Beroun, 2007, s. 246. Prameny a nové proudy právní vědy. ISBN 80-85889-82-6.
[106] Čl. 51 Charty OSN zní: „*Žádné ustanovení této Charty neomezuje, v případě ozbrojeného útoku na některého člena Organizace spojených národů, přirozené právo na individuální nebo kolektivní sebeobranu, dokud Rada bezpečnosti neučiní opatření k udržení mezinárodního míru a bezpečnosti. Opatření učiněná členy při výkonu tohoto práva sebeobrany oznámí se ihned Radě bezpečnosti; nedotýkají se nikterak pravomoci a odpovědnosti Rady bezpečnosti, pokud jde o to, aby kdykoli podle této Charty podnikla takovou akci, jakou považuje za nutnou k udržení nebo obnovení mezinárodního míru a bezpečnosti*.“

k tomu, že pojmy „síla“ ani „ozbrojený útok“, se kterými daná ustanovení pracují, nejsou v Chartě OSN nikterak definovány, činí na jednu stranu jejich výklad v praxi nemalé potíže,[107] na straně druhé ovšem otevírá prostor pro diskuzi, zda a za jakých okolností může být kybernetická operace považována za použití síly či dokonce za ozbrojený útok.

S ohledem na to, že čl. 2 odst. 4 Charty OSN zahrnuje též hrozbu silou, je nutné níže uvedené závěry vztáhnout analogicky i na tyto případy. Hrozba silou připadá v úvahu i ve vztahu ke kybernetickým operacím.[108]

Podle převažujících názorů se pojem síla nevztahuje na jakýkoli druh síly, nýbrž se jím rozumí pouze síla ozbrojená.[109] Někteří autoři tvrdí, že zahrnuje též fyzickou sílu nevojenské povahy, jako je např. „*(...) vypuštění velkého množství vody do údolí nebo šíření požáru přes mezinárodní hranice*“,[110] avšak přestože taková síla může stát zasáhnout stejně závažným způsobem jako síla vojenská, za standardních okolností na ní zákaz použití síly není nutné vztahovat, protože protiprávnost jejího použití stanoví ve většině případů jiné primární normy.[111]

Zatímco ozbrojený útok bude vždy představovat porušení čl. 2 odst. 4 Charty OSN, ne každé porušení tohoto článku bude zakládat ozbrojený útok.[112] Přestože všeobecně přijímaná definice ozbrojeného útoku neexistuje,[113] podle MSD „*panuje všeobecná shoda o povaze aktů, které je možno považovat za (...) ozbrojený útok*“[114] a MSD zahrnuje do jeho rámce nejen „*jednání pravidelných ozbrojených sil přes mezinárodní hranice“*, ale též „*vyslání státem ozbrojených band, skupin, nepravidelných jednotek nebo žoldnéřů, kteří provádějí činy ozbrojeného násilí proti jinému státu takové závažnosti, že se rovná skutečnému ozbrojenému útoku prováděnému pravidelnými jednotkami*“.[115] Finanční, logistická, nebo jiná podpora nebyla ze strany MSD shledána natolik závažná, aby mohla naplnit koncept ozbrojeného útoku.[116] MSD nicméně konstatoval, že takové jednání by mohlo představovat „*hrozbu nebo*

[107] ONDŘEJ, J. *Odzbrojení: prostředek k zajištění mezinárodní bezpečnosti*. 2., rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2008, s. 53. ISBN 978-80-7380-129-8.
[108] SCHMITT, M. N. The Use of Cyber Force and International Law. In: WELLER, M., A. SOLOMOU a J. W. RYLATT. *The Oxford handbook of the use of force in international law*. Oxford: Oxford University Press, 2015, s. 1115. Oxford handbooks. ISBN 978-0-19-967304-9.
[109] Ondřej, op. cit., s. 54.
[110] RANDELZHOFER, A. Article 2 (4). In: SIMMA, B. (ed.). *The Charter of the United Nations: a commentary. Vol. I*. 2. Oxford: Oxford University Press, 2002, s. 118. ISBN 0199244499.
[111] Tamtéž, s. 119.
[112] Ondřej, op. cit., s. 125.
[113] DUFFY, H. *The 'war on terror' and the framework of international law.* 2. Cambridge: Cambridge University Press, 2015, s. 254. ISBN 9781107601727.
[114] *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, op. cit., para. 195.
[115] Ondřej, op. cit., s. 125.
[116] *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, op. cit., para. 195.

použití síly, nebo se rovnat vměšování se do vnitřních či vnějších záležitostí jiných států".[117] Použití ozbrojené síly státem vůči suverenitě, územní celistvosti nebo politické nezávislosti jiného státu, nebo jiným způsobem neslučitelným s cíli OSN, je ze strany OSN považován též za akt agrese.[118] Koncept ozbrojeného útoku je podle Randelzhofera naplněn jedině tehdy, pokud je síla použita ve větším rozsahu a se značnými účinky (*relatively large scale and substantial effect*).[119]

3.2.2. Zákaz hrozby a použití síly v kyberprostoru?

Přestože dnes již většina autorů akceptuje, že kybernetická operace za určitých okolností může představovat použití síly či ozbrojený útok opravňující napadený stát k výkonu sebeobrany, stále nepanuje shoda o tom, v jakých konkrétních případech tomu tak bude. Jinými slovy, jaká je hranice mezi kybernetickou operací, která bude považována za ozbrojený útok, použití síly či „pouze" za mírnější případy narušení suverenity?[120]

Jak jsme viděli výše v bodu 3.2.1, přestože zcela přesná definice použití síly neexistuje, „*některé její prvky jsou velmi dobře známy*".[121] Doktrína je vcelku jednotná v názoru, že kybernetická operace bude považovaná za použití síly, resp. ozbrojený útok, pokud způsobí fyzickou škodu, jejíž rozsah a následky budou srovnatelné s rozsahem a následky kinetického útoku zakládajícího použití síly, resp. ozbrojený útok, podle obecných pravidel mezinárodního práva.[122]

Přestože se pojmem síly tradičně myslí síla ozbrojená,[123] doktrína nevidí důvod, proč by se tato charakteristika nedala vztáhnout též na kybernetické operace a poukazuje přitom na posudek MSD týkající se jaderných zbraní,[124] který stanoví, že se ustanovení Charty „*nezmiňují o specifických zbraních. Týkají se jakéhokoli užití síly bez ohledu na použité zbraně. Charta ani*

---

[117] *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, op. cit., para. 195.
[118] UNGA. Resolution 3314 (XXIX). *„Definition of Agression*". 14 December 1974, UN Doc A/RES/3314(XXIX).
[119] RANDELZHOFER, A. Article 51. In: SIMMA, B. (ed.). *The Charter of the United Nations: a commentary. Vol. I*. 2. Oxford: Oxford University Press, 2002, s. 796. ISBN 0199244499.
[120] FOCARELLI, C. Self-defence in cyberspace. In: TSAGOURIAS, N. a R. BUCHAN (eds.). *Research handbook on international law and cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 2015, s. 263. ISBN 978-1-78254-738-9.
[121] HOISINGTON, M. Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. *Boston College International and Comparative Law Review* [online]. 2009, 32 (2), s. 447 [cit. 2019-11-28]. ISSN 02775778. Dostupné z: http://heinonline.org/HOL/Page?handle=hein.journals/bcic32&div=28.
[122] BUCHAN, R. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions. *Journal of Conflict and Security Law* [online]. 2012, 17 (2), s. 211 [cit. 2019-11-28]. ISSN 14677962. Dostupné z: http://heinonline.org/HOL/Page?handle=hein.journals/jcsl17&div=16.
[123] Ondřej, op. cit., s. 54.
[124] Focarelli, op. cit., s. 265.

výslovně nezakazuje ani nedovoluje použití jakékoli specifické zbraně (…)".[125] Takto se například většina odborné veřejnosti shodla, že virus Stuxnet byl zakázaným použitím síly ve smyslu čl. 4 odst. 2 Charty OSN.[126]

Jako nejčastější ilustrativní příklady kybernetických operací, které by bylo téměř nade vší pochybnost možné kvalifikovat jako použití síly, resp. ozbrojený útok, doktrína uvádí operace, které způsobí poškození kritické infrastruktury jiného státu.[127] Přestože Roscini konstatuje, že je tomu tak pravděpodobně proto, že většina závažných narušení fungování kritické infrastruktury způsobí újmu na zdraví, smrt osob nebo škodu na majetku, sám je toho názoru, že by „*déletrvající přerušení fungování systémů kritické infrastruktury*" mělo být považováno za použití síly, pokud způsobí více než jen pouhou nepříjemnost.[128]

Pokud kybernetická operace způsobí „*smrt nebo zranění značného počtu osob anebo značnou škodu na majetku*", bude takovou operaci možné považovat za ozbrojený útok.[129] Hranice „značné" újmy není přesně stanovena, podle Schmitta tak bude za ozbrojený útok nutné považovat „*všechny kybernetické operace, které přesáhnou tzv. hranici de minimis*".[130]

Kybernetické operace nicméně nemusí mít žádné fyzické následky,[131] což v doktríně budí kontroverze, zda i takové operace je možné považovat za použití síly, resp. ozbrojený útok. Zatímco Schmitt na tuto otázku odpovídá kladně, neboť následky mnohých z nich jsou neméně závažné v porovnání s následky útoků kinetických,[132] Buchan celkem jednoznačně říká, že ne.[133] Jádrem sporu je podle názoru autorky skutečnost, zda použití síly, resp. ozbrojený útok, vyžaduje, aby újma na zdraví či škoda na majetku vznikla v jejich přímém důsledku či nikoli. Vzhledem k tomu, že Schmitt způsobení škody v přímém důsledku nevyžaduje, lze dle jeho

[125] *Legality of the Threat or Use of Nuclear Weapons,* ICJ. Rep. 1996, p. 226, para. 39 (Advisory Opinion) (Legalita hrozby nebo použití jaderných zbraní).

[126] Operace ovšem způsobila nemalou (fyzickou) škodu íránskému jadernému programu. I přes tento závěr se ale stejně nepodařilo naplnit subjektivní prvek mezinárodní odpovědnosti. Srov. DEV, P. R. Use of Force and Armed Attack Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response. *Texas International Law Journal* [online]. 2015, 50 (2-3), s. 396 [cit. 2019-11-27]. ISSN 01637479. Dostupné z: http://heinonline.org/HOL/Page?handle=hein.journals/tilj50&div=16.

[127] Půjde např. o narušení počítačových kontrolních systémů, v jehož důsledku dojde k rozsáhlému výpadku dodávky elektrického proudu; uvolnění vody z přehrady, které způsobí zaplavení osídlených oblastí; srážce letadel apod. Srov. např. DINSTEIN, Y. Computer Network Attacks and Self-Defense. *International Law Studies Series. US Naval War College* [online]. 2002, 76, s. 105 [cit. 2019-11-16]. ISSN 23752831. Dostupné z: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1397&context=ils.

[128] ROSCINI, M. Cyber operations as a use of force. In: TSAGOURIAS, N. a R. BUCHAN (eds.) *Research handbook on international law and cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 2015, s. 245 - 249. ISBN 978-1-78254-738-9.

[129] Schmitt, s. 1119-1120.

[130] Tamtéž.

[131] Např. smazání nebo pozměnění důležitých dat uložených na počítačových serverech.

[132] Schmitt, op. cit., s. 1120.

[133] Buchan, op. cit., s. 214.

interpretace pod použití síly, resp. ozbrojený útok, zahrnout též kybernetické operace, které fyzické škody nezpůsobí přímo, ale až sekundárně.[134] Podívejme se nyní na v literatuře často citovaný příklad burzy cenných papírů tradičním pohledem, který vyžaduje, aby škoda byla způsobena v přímém důsledku použití síly, resp. ozbrojeného útoku - „*zatímco bombový útok státu A na budovu burzy cenných papírů státu B bude považován přinejmenším za použití síly, kybernetická operace státu A na burzu cenných papírů státu B, který způsobí její úplné ochromení ovšem nikoli fyzickou škodu, za použití síly ve smyslu čl. 2 odst. 4 Charty OSN považován nebude*“.[135]

Většina autorů se vzácně shodne, že současný právní stav je nežádoucí, neboť právo adekvátně nereaguje na aktuální technologický vývoj, a proto je potřeba ho změnit.[136] Nakolik je přijetí mezinárodní úmluvy, která by tuto otázku autoritativně upravila, spíše nepravděpodobné,[137] bude nutné čl. 2 odst. 4 Charty OSN vykládat extenzivně, aby do jeho rámce bylo možné zahrnout i kybernetické operace, které nepůsobí přímou fyzickou škodu, ale které způsobí újmu až sekundárně.[138] Do doby, než se tato sporná otázka autoritativně vyřeší, doporučuje Schmitt posuzovat každou kybernetickou operaci „*tak, jak by ji pravděpodobně hodnotilo mezinárodní společenství*“. Za tímto účelem předkládá hodnotící škálu, kde každé jednotlivé okolnosti přisuzuje jinou váhu.[139]

Vzhledem k tomu, že kybernetické operace jsou často dílem nestátních aktérů, jejichž jednání nemusí být přičitatelné konkrétnímu státu, je závěrem ještě třeba odpovědět na otázku, zda je možné (za předpokladu, že taková operace bude představovat ozbrojený útok) legálně použít sílu proti nestátním aktérům operujícím z území jiného státu. Mezinárodní právo tradičně

[134] Přestože přímým důsledkem kybernetické operace na burzu cenných papírů bude úplné ochromení její funkčnosti, jejím sekundárním důsledkem bude ztráta hodnoty investičních nástrojů (doslova „*elimination of billions in wealth*“). S ohledem na propojenost dnešních ekonomik představuje tato skutečnost jistě závažnou situaci, která by, pokud škoda dosáhne určitého rozsahu, si jistě zasloužila kvalifikaci jako použití síly. Srov. Schmitt, op. cit., s. 1120.

[135] Roscini, op. cit., s. 247.

[136] DELIBASIS, D. The Right of States to Use Force in Cyberspace: Defining the Rules of Engagement. *Information & Communications Technology Law* [online]. 2002, 11 (3), s. 265-266 [cit. 2019-11-28]. ISSN 13600834. Dostupné z: http://heinonline.org/HOL/Page?handle=hein.journals/infctel11&div=21.

[137] CANCA, H. S. Prohibition against the use of force and the coercive uses of the cyberspace. *Journal of Naval Science and Engineering* [online]. 2017, 13 (1), s. 63 [cit. 2019-11-28]. ISSN 13042025. Dostupné z: https://doaj.org/toc/1304-2025.

[138] Takovému názoru přisvědčují například Roscini nebo Tsagourias, dle nichž by zákaz hrozby a použití síly měl zahrnovat i kybernetické operace, které sice fyzické účinky nezpůsobí, ale jejich následek bude pro stát zároveň představovat více než pouhou „nepříjemnost“. Srov. Roscini, op. cit., s. 249.

[139] Schmitt, op. cit., s. 1114.

vyžaduje, aby „*ozbrojený útok zahrnoval účast státu*“.[140] Problémy nečiní situace, kdy je jednání nestátních aktérů přičitatelné státu. V takových případech může stát A legálně použít sílu vůči státu B, z jehož území provedla hackerská skupina kybernetickou operaci zakládající ozbrojený útok ve smyslu čl. 51 Charty OSN, pokud je její jednání přičitatelné státu B na základě některého z článků ARSIWA. Mohl by ale stát A uplatnit právo na sebeobranu vůči nestátním aktérům operujícím z území státu B, pokud by jejich jednání se státem B zjevně nebylo spojeno? Odpověď na tuto otázku mezinárodní právo zcela jasně neposkytuje. Někteří autoři zastávají názor, že to možné není, a to ani v případě, kdy by taková opatření trvala jen po krátkou dobu a zasáhla výlučně skupinu těchto nestátních aktérů,[141] jiní mají za to, že judikatura MSD nevylučuje uplatnění práva na sebeobranu, pokud bude směřovat jen a pouze vůči nestátním aktérům, neboť výklad MSD naznačuje, že „*přičtení jednání nestátních aktérů je nutné jen v případě, kdy by právo sebeobrany bylo uplatňováno vůči jinému státu*“.[142] Později uvedenému pojetí přisvědčuje i Schmitt, podle kterého je možné právo na sebeobranu vůči státu B uplatnit, pokud tento nechce nebo není schopen (*unwilling or unable*) zajistit ukončení provádění protiprávních kybernetických operací ze svého území ze strany nestátních aktérů, jejichž jednání mu není přičitatelné.[143] Schmitt též připouští výkon sebeobrany v reakci na ozbrojený útok ve formě kybernetické operace směřující vůči objektům, které se na území poškozeného státu nenachází, pokud tento nad nimi vykonává svá svrchovaná práva.[144]

3.2.3. Vměšování se do vnitřních nebo vnějších záležitostí států

Jak již bylo naznačeno výše, případy, které nebude možné kvalifikovat jako použití síly či ozbrojený útok, bude za určitých okolností možné zhodnotit jako zakázané vměšování se do vnitřních nebo vnějších záležitostí států. Přestože tato zásada není v Chartě OSN výslovně uvedena,[145] můžeme ji dovodit z principu svrchované rovnosti států, který je vyjádřen v čl. 2 odst. 1 Charty OSN,[146] a která je ze strany MSD považována též za součást obyčejového

[140] HÝBNEROVÁ, S. Použití extrateritoriální síly proti nestátním aktérům v kontextu mezinárodního práva. In: *Nové trendy odpovědnosti a řešení sporů v mezinárodním právu: (vliv nestátních aktérů)*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2012, s. 29. ISBN 978-80-87146-73-6.
[141] Tamtéž, s. 29.
[142] TRAPP, K. N. Can Non-State Actors Mount to an Armed Attack? WELLER, M., A. SOLOMOU a J. W. RYLATT (eds.). *The Oxford handbook of the use of force in international law*. Oxford: Oxford University Press, 2015, s. 689. Oxford handbooks. ISBN 978-0-19-967304-9.
[143] Schmitt, op. cit., s. 1124.
[144] Tamtéž, s. 1123.
[145] Charta OSN obsahuje pouze čl. 2 odst. 7 zakazující vměšování samotné OSN.
[146] Ondřej, op. cit., s. 57.

mezinárodního práva.[147] Zakázané vměšování se sestává ze tří prvků – a) musí jít o jednání, které obsahuje prvek donucení; b) který se týká vnitřních nebo vnějších záležitostí, o kterých je stát na základě principu suverenity oprávněn svobodně rozhodovat; a c) je vyžadována příčinná souvislost mezi nimi.[148]

Rozsah pojmu „vnitřní a vnější záležitosti" je poměrně široký, jedná se o tzv. *domaine réservé* jednotlivých států, kam spadá například volba politického nebo ekonomického systému, formulace zahraniční politiky, uznání vlád jiných států, členství v mezinárodních organizacích apod.[149] Co se týče elementu donucení, nemusí jít vždy o použití fyzické síly ve smyslu ozbrojeného útoku či použití síly, což, jak jsme viděli výše v kapitole 3.2.2, má zvláštní význam právě v kybernetickém prostoru, kde se může velice často stávat, že kybernetická operace ani nebude působit žádné fyzicky viditelné následky a nebude ji proto možné (podle některých autorů) takto kvalifikovat.[150] Kybernetická operace nemusí dosáhnout kýžených výsledků, aby ji bylo možné posoudit jako vměšování do vnitřních záležitostí. Postačí, že bude „*schopná donutit jiný stát, aby učinil něco, co by za jiných okolností neučinil, nebo aby se naopak zdržel činnosti, kterou by jinak vykonal"*, čímž zřetelně odlišuje *donucení* od pouhého ovlivnění chování jiného státu bez jakéhokoli zvláštního cíle.[151]

Případy nedovoleného vměšování se v praxi rozhodně nejsou ojedinělé, a s ohledem na propojenost kybernetického světa lze očekávat, že ani v kyberprostoru nebude k porušování této zásady docházet pouze ve výjimečných případech. Otázka, zda se bude jednat o vměšování se do vnitřních nebo vnějších záležitostí, se točí kolem elementu donucení. Při kvalifikaci určitého jednání je tak nutné si zodpovědět, zda je daná kybernetická operace schopná „přemoci" (*overbear*) vůli jiného státu.[152] V doktríně jsou velice často citovány příklady politického a ekonomického donucení, přičemž ve vztahu ke kybernetickému prostoru se v současné době stále častěji skloňuje fenomén „fake news" a útoků na volební proces.

Jako „fake news" se označují „*prokazatelně nepravdivé nebo zavádějící informace, kterou jsou vytvářeny, prezentovány a šířeny (…) s úmyslem klamání veřejnosti a které mohou*

[147] *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, op. cit., para. 202.
[148] Ondřej, op. cit., s. 58-59.
[149] Tamtéž.
[150] Buchan, op. cit., s. 221.
[151] Tallinn Manual 2.0, Rule 66, para. 19.
[152] JAMNEJAD, M. a M. WOOD. The Principle of Non-intervention. *Leiden Journal of International Law* [online]. 2009, 22 (2), s. 371 [cit. 2019-11-28]. ISSN 09221565. Dostupné z: http://heinonline.org/HOL/Page?handle=hein.journals/lejint22&div=24.

způsobit veřejnou újmu“.[153] Jejich cílem je rodit pochybnosti, zmást občany a oslabit jejich víru v instituce a zavedené politické postupy.[154] To, co odlišuje „fake news“ od běžných nepravdivých či zavádějících informací, které se pravidelně objevují například v bulvárním tisku, je právě jejich množství a účel, který je sledován jejich uveřejněním, tedy snaha ovlivnit vnitřní záležitosti. Do hledáčku mezinárodního práva se pak dostávají ve chvíli, kdy za jejich šířením stojí cizí stát, anebo cizí nestátní aktér, jehož jednání je jinému státu přičitatelné. Fake news nepochybně představují narušení suverenity jiných států. Pokud by ale informace šířené státem A způsobily změnu politického režimu, nebo ovlivnily voliče a zmanipulovaly tak volby ve státě B, půjde velmi pravděpodobně též o nedovolené vměšování se do jeho vnitřních záležitostí. K závěru o naplnění konceptu vměšování se do vnitřních záležitostí bude přispívat například také okolnost, zda byly informace šířeny v předvolebním období.[155]

Tak závažné situace, jako je například napadení elektronického systému sčítání hlasů či přinucení ke změně vnitrostátní regulace internetu, bude nepochybně možné označit za vměšování se do vnitřních záležitostí.[156] Pokud by ale došlo pouze k útoku na webovou stránku zprostředkovávající volební výsledky, nikoli přímo o útok na systém sčítání hlasů, jedná se jistě o závažnou situaci, která zasahuje do suverenity státu, neboť může ovlivnit veřejné mínění a důvěru v konečný stav voleb, o vměšování se do vnitřních záležitostí nicméně nepůjde.[157] Jinými slovy, čím více donucující kybernetická operace bude, tím spíše se bude jednat o projev protiprávního vměšování se do vnitřních záležitostí státu.[158]

Vměšování se ale pochopitelně nemusí týkat pouze volebního procesu. Doktrína se shoduje, že vměšováním se do vnitřních záležitostí byla například kybernetická operace vůči Estonsku v roce 2007, jejímž cílem měla být změna postoje Estonska k odstranění sochy vojáka Rudé armády z Tallinnu. Zasaženy byly jak státní úřady, tak finanční instituce a celá operace významně zasáhla též estonskou ekonomiku.[159]

V této souvislosti je velice zajímavá otázka, zda si stát vůbec musí být vědom toho, že se stal obětí donucující kybernetické operace, neboť v kyberprostoru jistě nejsou

[153] Rada EU. *Společné sdělení Evropskému parlamentu, Evropské Radě, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Zpráva o provádění akčního plánu proti dezinformacím*. Brusel, 17. června 2019. JOIN(2019) 12 final.
[154] Tamtéž.
[155] Jamnejad a Wood, op. cit., s. 361.
[156] Tallinn Manual 2.0, Rule 66, paras. 1 – 4.
[157] POHJANPALO, K. Finland Detects Cyber Attack on Online Election-Results Service. *Bloomberg* [online]. 10 April 2019 [cit. 2019-11-09]. Dostupné z: https://www. bloomberg. com/news/articles/2019-04-10/finland-detects-cyber-attack-on-online-election-results-service.
[158] Schmitt, op. cit., s. 1116.
[159] Focarelli, op. cit., s. 261.

nepředstavitelné situace, kdy se bude zdát, že poškození vzniklo v důsledku běžné mechanické dysfunkce, a přitom bylo způsobeno softwarem, který měl takový dojem pouze navodit a zatajit tak skutečnou škodlivou kybernetickou operaci.[160] Autoři Tallinnského Manuálu se domnívají, že „*s ohledem na tuto skutečnost na požadavku vědomosti jistě nelze trvat*“.[161]

Přestože podmínkou není ani znalost identity původce kybernetického operace, protože v tomto aspektu nebudou mít oběti absolutní jistotu asi nikdy, je pochopitelně nutné, aby posuzované jednání bylo dříve nebo později některému státu přičteno.

3.2.4. Narušení suverenity

K narušení suverenity státu dojde, pokud ho kybernetická operace zbaví nebo nebude brát na zřetel jeho svrchovanou moc. Jednání, která budou postrádat prvek donucení, a nekvalifikují se tak buď jako vměšování se do vnitřních záležitostí státu, nebo použití síly, resp. ozbrojený útok, přesto mohou za určitých okolností být protiprávní, protože stále mohou alespoň narušovat suverenitu jiných států.

V souvislosti se suverenitou bývá často zmiňován též případ kyberšpionáže, neboť kybernetické operace se velice často soustředí právě na sběr citlivých údajů a přerušení poskytování služeb.[162] Státy si jsou moc dobře vědomy skutečnosti, že je téměř nemožné identifikovat konkrétního pachatele a mnoho kybernetických operací zůstává zcela nezpozorováno, a proto se státy v kyberprostoru vzájemně tajně sledují.[163]

Jako špionáž se označuje jakékoli jednání, které slouží, anebo se pokouší o „*shromažďování, třídění a zpracování utajovaných informací, přičemž tak činí utajovaným způsobem*“.[164] Pojem kyberšpionáž poté odkazuje na špionáž prováděnou prostřednictvím kybernetických prostředků, jedná se tedy zejména o případy sledování, monitorování, zachycování nebo odklonění elektronicky přenášené nebo uložené komunikace, dat nebo jiných informací.[165] Špionáž v době míru je tradičně považována za oblast, která není mezinárodním

[160] Tallinn Manual 2.0, Rule 66, para. 25.
[161] Tamtéž, paras. 19 – 20.
[162] KSHETRI, N. *Cybersecurity and International Relations: The U. S. Engagement with China and Russia* [online]. [cit. 2019-11-16]. Dostupné z: http://web. isanet. org/Web/Conferences/FLACSO-ISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf. pdf.
[163] KREMLING, J. a A. M. SHARP PARKER. Cyberspace, Cybersecurity, and Cybercrime. *Cyberspace, cybersecurity, and cybercrime*. Los Angeles: SAGE, 2018, s. 113. ISBN 978-1-506-347257.
[164] CHURAŇ, M. *Encyklopedie špionáže: ze zákulisí tajných služeb, zejména Státní bezpečnosti*. 2. přeprac. a aktualiz. vyd. Praha: Libri, 2000, s. 409 - 410. ISBN 8072770209.
[165] Tallinn Manual 2.0, Rule 32, para. 2.

právem vůbec regulována, a protože není zakázána, je obecně považována za dovolenou.[166] Ke stejnému závěru došli i autoři Tallinnského Manuálu ve vztahu ke kybernetické špionáži učiněné v době míru, podle kterých kyberšpionáž sama o sobě (ve smyslu pouhého tajného sledování a sběru dat) mezinárodní právo neporušuje, ale „*způsob, jakým je vedena, by už tak činit mohl*".[167]

Nakolik se názory na dovolenost tradiční špionáže liší, i závěr o charakteru kyberšpionáže není zcela jednoznačný. Praxe států i názor doktríny nicméně svědčí o tom, že samotný akt sledování a sběru informací o jiném státu narušení suverenity nepředstavuje. Zda se nejedná o porušení jiných závazků (například lidskoprávních ve vztahu ke konkrétním sledovaným osobám), už je otázka jiná.

3.2.5. Due diligence

Kromě výše uvedených závazků, ukládá mezinárodní právo státům též povinnost *due diligence*, která vychází z principu územní suverenity každého státu, tedy že „*žádný stát nemůže vědomě připustit, aby jeho území bylo využíváno pro jednání odporující právům jiného státu*".[168] Toto pravidlo se nepochybně uplatní i v kybernetickém kontextu, neboť již na počátku nového tisíciletí byly státy vyzvány „*aby neposkytovaly bezpečné útočiště těm, kteří informační technologie trestuhodně zneužívají*".[169] Jak vyplynulo z kapitoly 1.1, kyberprostor, jako nehmotné médium, může fungovat jen v rámci hmotné infrastruktury, prostřednictvím počítačových sítí a informačních systémů, které se ve světě fyzicky nacházejí. Státy tak mají povinnost zajistit, „*aby jejich kybernetická infrastruktura nebo kybernetická infrastruktura pod jejich kontrolou*" nebyla využívána v rozporu s touto zásadou.[170]

Vzhledem k tomu, že se jedná o povinnost činnostní a nikoli výsledečnou,[171] cílem tohoto závazku není za všech okolností uspět v zamezení protiprávnímu jednání, ale jde spíše „*o povinnost využít všech dostupných prostředků, aby mu pokud možno bylo zabráněno*".[172] Opatření, která budou státy povinny přijmout, se budou lišit v závislosti na jejich

[166] BAKER, CH. D. Tolerance of International Espionage: A Functional Approach. *American University International Law Review* [online]. 2003, 19 (5), s. 1091-1114 [cit. 2019-11-12]. ISSN 1520460X. Dostupné z: http://heinonline. org/HOL/Page?handle=hein. journals/amuilr19&div=33.
[167] Tallinn Manual 2.0, Rule 32.
[168] Kittichaisaree, op. cit., s. 39-40.
[169] UNGA. Resolution 55/63. *Combating the criminal misuse of information technologies*. 22 January 2001. UN Doc. A/RES/55/63.
[170] Tallinn Manual 2.0, Rule 6.
[171] Čepelka a Šturma, op. cit., s. 381.
[172] *Case concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Yugoslavia)*, ICJ Rep. 2007, para. 430.

technologickém vybavení i finančních možnostech,[173] státy jsou tak povinny přijmout pouze taková opatření, která by „*po zralé úvaze na jejich místě přijal stát v obdobném postavení*“ [174] – tedy za určitých okolností nemusí přijímat opatření vůbec žádná. Na rozdíl od názorů, které se objevovaly před vydáním Tallinnského Manuálu,[175] tento staví najisto, že státy nejsou povinny přijímat opatření preventivní.[176]

Tallinnský Manuál závazek due diligence ukládá dvěma typům států, které označuje jako stát „územní“ (*territorial*), jehož kybernetická infrastruktura je využívána k provedení kybernetické operace, a stát tranzitní,[177] tedy takový, skrze jehož kybernetickou infrastrukturu operace pouze prochází.[178] Povinnost due diligence zahrnuje jednání všech osob a užití všech kybernetických infrastruktur, nad kterými státy vykonávají jurisdikci,[179] přičemž se uplatní i extrateritoriálně na území, nad kterými státy vykonávají kontrolu, a to i v případě, kdy „*nad nimi neuplatňují svou svrchovanou moc*“.[180] Požadovaný stupeň kontroly autoři označují jako „skutečnou kontrolu“, která nastává v případech, kdy „*stát kybernetickou infrastrukturu provozuje, anebo pokud se nachází na území, v prostorách či objektech, které fakticky kontroluje*“.[181] Povinnost due diligence se vztahuje pouze na ty kybernetické operace, které, pokud by je provedl sám povinný stát, zakládají porušení mezinárodního závazku a způsobují závažné následky jinému státu.[182] Přesná mezní hodnota způsobené újmy není stanovena,[183] vznik fyzické škody ale není vyžadován.[184]

Vzhledem k tomu, že kybernetické operace jsou často prováděny zcela nepozorovaně a zaznamenány mohou být až v okamžiku, kdy způsobí zamýšlené následky, je povinnost

[173] CHIRCOP, L. A Due Diligence Standard of Attribution in Cyberspace. *International and Comparative Law Quarterly* [online]. 2018, 67 (3), s. 650 [cit. 2019-11-12]. ISSN 14716895. Dostupné z: http://heinonline.org/HOL/Page?handle=hein. journals/incolq67&div=34.
[174] Kittichaisaree, op. cit., s. 40.
[175] ZIOLKOWSKI, K. General Principles of International Law as Applicable in Cyberspace. In: ZIOLKOWSKI, K (ed.). *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* [online]. Tallinn: NATO CCDCOE, 2013, s. 167 [cit. 2019-11-29]. ISBN 978-9949-9211-8-8. Dostupné z: https://ccdcoe.org/uploads/2018/10/PeacetimeRegime.pdf.
[176] Tallinn Manual 2.0, Rule 6, para. 42.
[177] Tamtéž, para. 8 a 13.
[178] REINISCH, A. a M. BEHAM. Mitigating Risks: Inter-State Due Diligence Obligations in Case of Harmful Cyber-Incidents and Malicious Cyber-Activity – Obligations of the Transit State. *German Yearbook of International Law* [online]. 2015, 48, s. 101-112 [cit. 2019-11-29]. Dostupné z: https://ssrn.com/abstract=2664322.
[179] K pojmu jurisdikce srov. kapitolu 3.1 výše.
[180] Tallinn Manual 2.0, Rule 6, para. 9.
[181] Tamtéž, Rule 6, para. 11.
[182] LIU, I. Y. The due diligence doctrine under Tallinn Manual 2.0. *Computer Law* [online]. 2017, 33 (3), s. 392 [cit. 2019-11-30]. DOI: 10.1016/j.clsr.2017.03.023. ISSN 02673649.
[183] Tallinn Manual 2.0, Rule 6, para. 25.
[184] Tamtéž, para. 28.

tranzitních států omezena pouze na případy, kdy tyto měly skutečné nebo konstruktivní[185] povědomí o tom, že operace probíhá prostřednictvím kybernetické infrastruktury, nad kterou jsou povinny dbát požadavku due diligence; operace dosáhne v cílovém státě určitého stupně závažnosti; a tranzitní stát je schopen přijmout „proveditelná" (*feasible*) opatření.[186] Tyto podmínky musí být naplněny kumulativně.[187] Lze konstatovat, že skutečné povědomí o protiprávním jednání budou státy mít pouze v případě, kdy je útok přímo prováděn jejich orgány, anebo v případě, kdy státy jeho páchání strpí.[188] Konstruktivní povědomí Liu charakterizuje jako situaci, kdy „*objektivní důkazy svědčí o tom, že stát o kybernetické operaci vědět měl a mohl*".[189] V praxi může být poměrně obtížné prokázat, že stát měl skutečné povědomí o tom, že je z nebo přes jeho území kybernetická operace vedena.[190] Standard konstruktivního povědomí tak zajistí, že se závazek due diligence nestane pouze teoretickým pojmem, neboť stát může být shledán odpovědným za jeho porušení, pokud by se „*jiný stát v obdobném postavení za normálních okolností o páchání protiprávního jednání dozvěděl*".[191]

Jak bude ukázáno níže v kapitole 3.3, přičtení protiprávního jednání konkrétnímu státu činí v souvislosti s kyberprostorem nemalé potíže. Jistě nebude ojedinělá situace, kdy stát A provede kybernetickou operaci prostřednictvím kybernetické infrastruktury státu B, přičemž cílem útoku bude stát C. Přestože stát C pravděpodobně odhalí, že tato přichází ze státu B, nebude schopen identifikovat skutečného pachatele, tedy stát A. Pokud by neexistovala povinnost due diligence, stát C by nemohl provést protiopatření vůči státu B, neboť ten není skutečným pachatelem dané operace. V důsledku porušení závazku due diligence už ale stát B určitý stupeň odpovědnosti ponese, a proto mohou protiopatření státu C směřovat i vůči němu. V kyberprostoru má tak povinnost due diligence nezastupitelnou úlohu, neboť nakolik se státy potýkají s nedostatkem důkazů nutných pro prokázání porušení některého z mezinárodněprávních závazků, které byly popsány výše v předchozích bodech, dostupné důkazy zpravidla budou stačit k prokázání porušení závazku due diligence. Mezi státy se ale

[185] S termínem konstruktivní povědomí poprvé přišel ESLP ve věci Osman proti Spojenému království. Srov. ESLP. *Osman v. the United Kingdom*, 28 October 1998, Reports of Judgments and Decisions 1998-VIII.
[186] Tamtéž, para. 13.
[187] Tamtéž.
[188] Jedná se o případy, kdy stát útok zaznamená, nebo je mu oznámen, ten ale přesto vědomě/záměrně nepodnikne žádné kroky, aby se mu pokusil zabránit.
[189] LIU, I. Y. State Responsibility and Cyberattacks: Defining Due Diligence Obligations. *Indonesian Journal of International* [online]. 2017, 4 (2), s. 233 [cit. 2019-11-12]. ISSN 23387602. Dostupné z: http://heinonline.org/HOL/Page?handle=hein.journals/indjicl4&div=15.
[190] LIU, I. Y. op. cit. (176), s. 392.
[191] Chircop, op. cit., s. 650.

pochopitelně stále najde celá řada odpůrců tohoto pravidla, neboť se obávají, že na ně uvalí příliš velké břemeno.[192]

3.2.6. Dílčí shrnutí

Je možné uzavřít, že v kyberprostoru může docházet k různorodým porušováním primárních pravidel, tedy zejména různých stupňů narušení suverenity jednotlivých států. V doktríně není zcela jednoznačně stanovena hranice, kdy určité chování bude považováno za tu či onu úroveň narušení suverenity, jednoznačně je ale připuštěno, že v kyberprostoru může docházet i k vměšování se do vnitřních a vnějších záležitostí států, hrozbě nebo použití síly, či k ozbrojenému útoku. V této souvislosti je nejvíce problematická otázka kybernetických operací, které nezpůsobují fyzicky viditelné následky.

Doktrína uznává též existenci závazku due diligence, plnění této povinnosti ovšem podmiňuje splněním různých kritérií. Závazek due diligence má v kyberprostoru nezastupitelnou úlohu, jak bude blíže prokázáno v následující kapitole.

3.3. Přičitatelnost jednání

Samotné porušení mezinárodního závazku není dostačující. Aby za něj stát nesl odpovědnost, musí mu být jednání též přičitatelné. Vůle států jako abstraktních útvarů je tvořena chováním fyzických osob. Okolnosti, za kterých bude jejich jednání považované za chování státu, stanoví obecné mezinárodní právo v oblasti mezinárodní odpovědnosti, jehož základy byly popsány výše v části druhé, a které pochopitelně platí i v kyberprostoru.[193] I zde tak můžeme rozlišovat jednání orgánů státu *de iure* dle čl. 4,[194] orgánů v přenesené působnosti dle čl. 5[195] až 7,[196] orgánů *de facto* dle čl. 8[197] či další případy dle čl. 9 – 11 ARSIWA.[198] O zvláštní aplikaci článku 10 ARSIWA Tallinnský Manuál nehovoří.

---

[192] I proto jsou negativní ohlasy slyšet zejména ze strany těch, kteří jsou nejčastěji kybernetickými operacemi atakováni, protože se obávají, že jejich kybernetická infrastruktura bude často využívána k provádění protiprávních operací vůči jiným státům, a ponesou tak často povinnost due diligence. Srov. SCHMITT, M. N. In Defense of Due Diligence in Cyberspace. *Yale Law Journal Forum* [online]. 2015, 22 June 2015, 125 (68), s. 74 [cit. 2019-11-29]. Dostupné z: http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace.

[193] DELERUE, F. Reinterpretation or Contestation of International Law in Cyberspace? *Israel Law Review* [online]. Cambridge University Press, 2019, 52 (3), s. 304 [cit. 2019-11-24]. ISSN 00212237. Dostupné z: https://search.ebscohost.com/login.aspx?authtype=shib&custid=s1240919&profile=eds.

[194] Tallinn Manual 2.0, Rule 14.

[195] Tamtéž, Rule 15.

[196] Tamtéž, Rule 16.

[197] Tamtéž, Rule 17 lit. (a).

[198] Tamtéž, Rule 15, para. 17, Rule 17 lit. (b) a Rule 18.

3.3.1. Orgány státu *de iure*

Koncept orgánů státu je poměrně široký, a to zejména z toho důvodu, aby se státy nevyhýbaly odpovědnosti například tím, „*že by určitému subjektu takový status nepřiznaly ve svém vnitrostátním právu*“.[199] Chování státních orgánů, kupř. národních úřadů pro kybernetickou a informační bezpečnost, je vždy přičitatelné státu, pokud bylo učiněno jménem takového orgánu nebo na jeho účet, a to i v případě kdy jednání vybočuje z rámce úkolů, které takovému orgánu byly svěřeny (tzv. jednání *ultra vires*),[200] například pokud člen takového úřadu provede, v rozporu s pokynem svého nadřízeného, kybernetickou operaci, která bude zakládat porušení mezinárodněprávního závazku, jeho jednání bude státu přičitatelné, přestože k jeho provedení nebyl zmocněn.[201] V případech, kdy by ale zneužil kybernetickou infrastrukturu k „*jednání čistě soukromé povahy, například trestněprávní činnosti přinášející mu soukromý užitek*“, k přičtení jednání danému státu nedojde.[202]

V kybernetickém kontextu jistě mohou nastat i případy, kdy státy vnitrostátním právem zmocní jiný subjekt k výkonu vládní moci. Státní orgány nemusí disponovat dostatečnými technologickými znalostmi, a proto je v jejich kompetenci svěřit například ochranu kybernetické infrastruktury soukromé společnosti.[203] Obdobně jako v případě orgánů státu, dokud bude tato entita jednat v rámci své svěřené působnosti, nikoli jménem svým a ve svých soukromých záležitostech, bude stát za její jednání odpovídat, a to i v případě, kdy tato překročí pravomoci jí svěřené,[204] tedy například pokud „*při obraně kybernetické infrastruktury provede kromě pasivní obrany též aktivní kybernetický protiútok (hack-back)*“, a to z toho důvodu, že „*takové jednání je k obraně vládní kybernetické infrastruktury nezbytné*“.[205]

V situaci, kdy stát nedisponuje dostatečnými technologickými znalostmi či vybavením, se kromě zmocnění soukromé entity otevírá prostor i pro aplikaci čl. 6 ARSIWA, tedy situace, kdy je orgán státu A dán státu B k dispozici. Jednání orgánu státu A je pak považováno za chování státu B, jestliže bylo vykonáno při výkonu funkcí vládní povahy státu B, pokud byl orgán výlučně řízen a kontrolován státem B.[206] Základním kritériem pro posouzení

[199] ARSIWA komentář, čl. 4 odst. 2 – bod 11 komentáře.
[200] Kittichaisaree, op. cit., s. 37.
[201] Tallinn Manual 2.0, Rule 15, para. 6.
[202] Tamtéž, para. 7.
[203] Tamtéž, para. 11.
[204] Čl. 5 ve spojení s čl. 7 ARSIWA.
[205] Tallinn Manual 2.0, para. 12.
[206] ARSIWA komentář, čl. 6, bod 1 komentáře.

přičitatelnosti dle tohoto článku je tak identifikace předmětu jednání orgánu státu A a jeho vztahu k naplnění zájmů a cílů, které stát B touto „spoluprací“ sledoval.[207]

Stejně jako k založení odpovědnosti státu nestačí, že byla kybernetická operace provedena ze zařízení nacházejícího se na jeho území,[208] ani pouhá skutečnost, že byl útok proveden z vládního kybernetického zařízení, není dostatečným důvodem pro závěr, že by takové jednání bylo státu přičitatelné, neboť kyberprostor je příznačný nejen anonymitou, kterou svým uživatelům poskytuje, ale též příznivým prostředím k maskování či provádění útoků za pomoci vzdáleného přístupu.[209] Uvedené svádí k závěru, že lokalizace zařízení, ze kterého byla kybernetická operace vedena, je jen jedním z logických kroků, nikoli však jediným kritériem, na základě kterého by bylo možné učinit závěr o (ne)přičitatelnosti jednání státu,[210] a že záměrem by tak vždy mělo být též zjištění osoby, která kybernetickou operaci provedla, zosnovala, nebo řídila, aby bylo možné identifikovat její vztah/spojení s podezřelým státem.[211] To je ovšem, právě s ohledem na výše uvedené charakteristiky kyberprostoru, často velice obtížné, ne-li nemožné, obzvláště pokud pachatelem bude zkušený hacker.[212] O této problematice bude pojednáno níže v souvislosti s přičitatelností jednání nestátních aktérů.[213]

3.3.2. Přičitatelnost jednání nestátních aktérů

Otázka přičitatelnosti jednání nestátních aktérů je ve vztahu ke kyberprostoru velice důležitá, neboť v této oblasti se více než kdekoli jinde angažují soukromé subjekty, protože státní aparát mnohdy nedisponuje dostatečnými znalostmi či dokonce vybavením, které by bylo

[207] Tallin Manual 2.0, Rule 16., para. 4.
[208] Tallinn Manual 2.0, Rule 15., paras. 13 – 14.
[209] YANNAKOGEORGOS, P. A. *Strategies for resolving the cyber attribution challenge* [online]. Maxwell Air Force Base, Alabama: Air University Press, Air Force Research Institute, 2013, s. 9 - 14 [cit. 2019-11-23]. ISBN 978-1-58566-226-5. Dostupné z: https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/cpp_0001_yannakogeorgos_cyber_Attribution_challenge.PDF.
[210] ANTONOPOULOS, C. State responsibility in cyberspace. In: TSAGOURIAS, N. a R. BUCHAN (eds.). *Research handbook on international law and cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 2015, s. 62. ISBN 978-1-78254-738-9.
[211] TANYILDIZI, M. E. STATE RESPONSIBILITY IN CYBERSPACE: THE PROBLEM OF ATTRIBUTION OF CYBERATTACKS CONDUCTED BY NON-STATE ACTORS. *Law & Justice Review* [online]. 2017, 8 (14), s. 156 [cit. 2019-10-27]. Dostupné z: https://ssrn. com/abstract=3047076.
[212] Zkušený hacker svou identitu zamaskuje nejen v aplikační, ale též v kyberpersonální vrstvě, přičemž svůj útok provede ve více etapách, tak aby stopy vedly k více zařízením nacházejícím se ideálně v různých státech, aby značně ztížil pátrání, neboť při něm bude nutná mezinárodní spolupráce. Srov. CLARK, D. D. a S. LANDAU. The Problem isn't Attribution; It's Multi-Stage Attacks. In: *ACM ReArch 2010* [online]. Philadelphia, USA, 2010 [cit. 2019-11-23]. Dostupné z: https://conferences.sigcomm.org/co-next/2010/Workshops/REARCH/ReArch_papers/11-Clark.pdf.
[213] Stát pochopitelně za určitých podmínek nese odpovědnost za to, aby jeho území (a tedy i kybernetická zařízení, která se na něm nachází) nebylo využito ke způsobení škody jinému státu. O otázce due diligence bylo pojednáno výše v bodě 3.2.5.

k vedení nebo odražení kybernetického útoku zapotřebí.[214] V posledních letech jsme navíc svědky zajímavého posunu, kdy motivem kybernetických operací přestává být vidina finančního zisku jednotlivců, ale spíše snaha o získání politické nebo vojenské převahy ze strany států.[215] Kybernetické operace tak přestávají být výhradní doménou vnitrostátního trestního práva a stále více se dostávají do hledáčku práva mezinárodního. Lze též očekávat, že státy budou postupně upouštět od konvenčních způsobů k dosažení výhod a stále častěji se budou uchylovat ke kybernetickým metodám, neboť opatřit si zkušeného hackera už dnes není takový problém[216] a kybernetické operace vychází mnohonásobně levněji.[217] Proto je důležité, aby státy nemohly uniknout své odpovědnosti pouhým zmocněním jednotlivců k provedení „*špinavé práce*".[218] Státem sponzorované skupiny představují nejvýznamnější hrozbu, neboť „*mají k dispozici lidské, finanční a časové prostředky, díky kterým jsou jejich operace v kyberprostoru technicky sofistikované a perzistentní*".[219] Pokud budou pravidla přičitatelnosti nastavena příliš přísně, hrozí, že státy budou za jednání nestátních aktérů v kyberprostoru odpovídat jen ojediněle, což zajisté není žádoucí.[220]

Jak vyplývá z kapitoly 2.2, přestože státy obecně za jednání nestátních aktérů odpovědnost nenesou, za určitých okolností tomu tak bude. Řeč je o teorii tzv. *de facto* orgánů, tedy subjektů, které fakticky vykonávají státní moc.[221] Určujícím kritériem dle čl. 8 ARSIWA není právní vztah mezi subjektem a státem (jako v případech posuzovaných dle čl. 4 – 6 ARSIWA), ale vztah faktický, existující *„do té míry, že tyto osoby jednají na základě jeho pokynů, nebo že jejich chování stát alespoň řídí či kontroluje*".[222]

Přičitatelnost jednání podle článku 8 ARSIWA ještě není zcela ustálena, a proto nadále představuje velice obtížnou otázku. Problémy přináší zejména prokazování existence řízení

---

[214] ALLAN, C. S. Attribution Issues in Cyberspace. *Chicago-Kent Journal of International and Comparative Law* [online]. 2013, 13 (2), s. 57 [cit. 2019-11-24]. Dostupné z: https://ssrn.com/abstract=2617870.

[215] Zatímco dříve byly kybernetické útoky spojeny spíše s krádežemi přístupových údajů k bankovním účtům, dnes se pachatelé stále častěji soustředí na mnohem významnější cíle, jako je například ovládnutí kritické infrastruktury, nebo ovlivnění vojenské navigace v ozbrojených konfliktech.

[216] Srov. reportáž CURRAN, D. My terrifying deep dive into one of Russia's largest hacking forums. *The Guardian* [online]. 24 July 2018 [cit. 2019-11-23]. Dostupné z: https://www.theguardian.com/commentisfree/2018/jul/24/darknet-dark-web-hacking-forum-internet-safety.

[217] Allan, op. cit., s. 78.

[218] MAČÁK, K. Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law* [online]. 2016, 21 (3), 405-428 [cit. 2019-10-28]. ISSN 14677954. Dostupné z: https://heinonline. org/HOL/Page?handle=hein. journals/jcsl21&div=29.

[219] NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2018.* (2019) s. 8.

[220] Tanyildizi, op. cit., s. 168.

[221] Malenovský, op. cit., s. 321.

[222] Tamtéž, s. 323.

nebo kontroly ze strany daného státu.[223] Požadovaný stupeň kontroly se stal předmětem nejednoho rozhodnutí mezinárodních soudních orgánů, kdy se standardy přičitatelnosti lišily v závislosti na skutkových okolnostech každého jednotlivého případu.[224] Jinými slovy „*míra odpovědnosti státu za činnost soukromých osob je odvislá od dosaženého stupně jeho faktické kontroly v každém posuzovaném případě mezinárodní odpovědnosti*“.[225] Jaká míra kontroly je ale nezbytná k tomu, aby jednání nestátního aktéra učiněné v kyberprostoru mohlo být státu přičteno?

3.3.3. Koncept kontroly v kyberprostoru

Jak bylo představeno výše v kapitole 2.2, mezinárodní soudní orgány ve své judikatuře přišly postupně s testem efektivní kontroly, celkové kontroly (*overall control*), efektivně-celkové kontroly (*effective overall control*) a s testem konečné pravomoci a kontroly (*ultimate authority and control test*).[226] Mezinárodní soudní i jiné orgány využívají hojně test efektivní i celkové kontroly, proto bude pozornost věnována právě jim.[227] Cassese potvrzuje, že tyto dva testy existují vedle sebe a v závislosti na okolnostech bude vhodné použít ten či onen.[228]

Test efektivní kontroly byl poprvé použit ve věci Nicaragua, kde MSD rozlišil dvě skupiny nestátních aktérů – jedince, kteří jsou zcela závislí na podpoře státu a jejich jednání je tedy státu jasně přičitatelné; a jedince, kteří si udrželi alespoň určitý stupeň nezávislosti a u kterých je pak nutné prokázat tzv. „efektivní kontrolu“ ze strany státu, aby tento za jejich jednání nesl odpovědnost. Za efektivní kontrolu MSD považoval situaci, kdy stát „*řídí anebo vynucuje spáchání protiprávního jednání*“,[229] z čehož vyplývá, že stát musí buď vydat pokyn ke konkrétnímu jednání, anebo vynutit konkrétní protiprávní jednání ze strany nestátního

[223] Tamtéž.
[224] COSTA, F. G. D. a V. L. H. BENN. The Challenges of Attribution of Internationally Wrongful Acts in the Cyberspace: A Critical Analysis of Control Tests and the Standard of Proof in International Courts. *Revista do CEPEJ* [online]. Salvador, 2016, 19 (Ed. Especial), s. 126 a 130 [cit. 2019-11-24]. Dostupné z: https://portalseer.ufba.br/index.php/CEPEJ/article/download/22043/14199.
[225] Malenovský, op. cit., s. 324.
[226] Srov. blíže kapitolu 2.2.
[227] Costa a Benn, op. cit., s. 132. Pro konkrétní judikaturu srov. CASSESE, A. The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia. *European Journal of International Law* [online]. 2007, 18 (4), s. 658 - 659 [cit. 2019-11-24]. ISSN 09385428. Dostupné z: https://heinonline.org/HOL/Page?handle=hein.journals/eurint18&div=41.
[228] Tamtéž, s. 657.
[229] *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, op. cit., para. 115.

aktéra.[230] Naproti tomu pouhé financování či materiální podpora o efektivní kontrole dle MSD nesvědčí.[231]

Test celkové kontroly je dílem odvolacího senátu ICTY ve věci Tadić, který rozlišil dvě situace a tedy i dva stupně kontroly – zatímco jedinci, kteří operují na území jiného státu, musí vždy obdržet pokyn ke konkrétnímu jednání (zde je tedy vyžadováno naplnění konceptu efektivní kontroly); u organizovaných a hierarchicky členěných skupin dalšího zvláštního pokynu k jednotlivým operacím není zapotřebí a postačí, že stát vykonával celkovou kontrolu nad takovou skupinou, protože tím vyjadřuje, že obecně její chování schvaluje.[232]

Ve vztahu k protiprávnímu jednání učiněnému v kyberprostoru v době míru věnuje doktrína největší pozornost testu efektivní kontroly.[233] Nejeden autor ovšem potvrzuje, že prokázání efektivní kontroly staví laťku poměrně vysoko a její naplnění je v kybernetickém kontextu více než obtížné, neboť stupeň kontroly bez identifikace konkrétní osoby či skupiny osob není možné stanovit.[234] Je tedy charakter kyberprostoru důvodem pro snížení standardu kontroly?

Podle Mačáka[235] a Tanyildiziho[236] spíše ne, neboť dle jejich názoru, je v kyberprostoru k naplnění konceptu kontroly nutné posoudit, „*zda je činnost útočníků závislá na financích a vybavení sponzorujícího státu, či zda je jejich existence závislá na zapojení, organizaci, výběru cílů a plánovaní celé operace ze strany státu*“. V případě kladné odpovědi je dle nich nutné tyto útočníky považovat za *de facto* orgány sponzorujícího státu. Jimi uvedená kritéria v podstatě opisují to, co mezinárodní soudní orgány považují za koncept efektivní kontroly. Prokázat naplnění konceptu efektivní kontroly ale činí problémy i v reálném světě, natož ve světě kybernetickém.[237] Bylo by tedy v kybernetickém kontextu možné se při prokazování naplnění konceptu kontroly spolehnout na nepřímé důkazy?

Costa a Benn, připouští, že prokázat určitý stupeň kontroly není v kyberprostoru jednoduché, nicméně, odkazujíce na rozhodnutí MSD ve věci Korfského průlivu, se spíše

[230] Cassese, op. cit., s. 653.
[231] *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, op. cit., para. 115. Toto pravidlo se uplatní i v kyberprostoru – srov. Tallinn Manual 2.0, Rule 17, para. 9.
[232] Cassese, op. cit., s. 661.
[233] Srov. Kittichaisaree, op. cit., s. 37 – 38.
[234] Costa a Benn, op. cit., s. 132. Toto tvrzení zastává též například francouzská vláda. Viz Droit international appliqué aux opérations dans le cyberspace. In: *Ministère des Armées* [online]. 4 Novembre 2019 [cit. 2019-11-24]. Dostupné z: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international.
[235] Mačák, op. cit., s. 407.
[236] Tanyildizi, op. cit., s. 160.
[237] Costa a Benn, op. cit., s. 136.

přiklání k názoru, že nepřímé důkazy přijatelné nejsou. V doktríně je nicméně možné pozorovat nárůst autorů, kteří se k přípustnosti nepřímých důkazů alespoň zčásti přiklání. Tak například Pagliery doporučuje podívat se na strukturu viru, neboť každý tvůrce má svůj zvláštní styl programovacího kódu; zaměřit se na načasování útoku, které může prozradit skutkový podklad pro jeho vedení; a identifikovat, kdo byl útokem poškozen a kdo z něj naopak těží, neboť všechny tyto okolnosti mohou svědčit o tom, odkud útok skutečně pochází.[238] O využití nepřímých důkazů hovoří též Kadlecová.[239]

V této souvislosti Margulies též upozorňuje, že mezi jednotlivými státy existují obrovské rozdíly v přístupu k informačním technologiím a že pro poškozený stát je mnohem obtížnější vypátrat pachatele kybernetického útoku, který byl podporován jiným státem. Proto namísto výše uvedených postupů navrhuje tzv. test *virtuální kontroly*, který převrací důkazní břemeno a uvaluje ho na podezřelý stát, který by tak měl prokázat, že za jednání odpovědný není, přestože finančně nebo jinak pachatele kybernetického útoku podporoval.[240] Převrácení důkazního břemene podporuje též Antonopoulos, podle kterého je dostatečným indikátorem skutečnost, že se podaří vypátrat, že kybernetická operace přichází z území určitého státu. Pokud je totiž tento informován ze strany oběti o takové protiprávní činnosti, je povinen provést opatření, kterými zamezí jeho pokračování, a to i přestože není schopen vypátrat skutečného pachatele.[241] Přestože se s tímto postupem ztotožňuje i Crootof, podle které test efektivní kontroly není příléhavý a klade na poškozený stát příliš vysoké nároky,[242] Roscini obrácení důkazního břemene kategoricky odmítá a připomíná, že „*pravidla přičitatelnosti neslouží ke znevýhodnění stěžovatele, ale též k ochraně podezřelého před falešným obviněním*“.[243]

Obtíže s důkazy se týkají většiny mezinárodních sporů obecně, nikoli tedy pouze těch, které se týkají jednání v kyberprostoru. Je nicméně pravdou, že s ohledem na jeho

[238] PAGLIERY, J. It looks like Russia and smells like Russia. .. but is it Russia?. *CNN* [online]. 31 October 2014 [cit. 2019-10-21]. Dostupné z: https://money. cnn. com/2014/10/31/technology/security/russia-hackers/index. html.

[239] KADLECOVÁ, L. State Responsibility in the Cyber Age: The Course towards Indirect Evidence. *Mezinárodní vztahy* [online]. 2019, 53 (4), s. 35-46 [cit. 2019-11-24]. ISSN 03231844. Dostupné z: https://mv.iir.cz/article/view/1585/1482.

[240] MARGULIES, P. Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. *Melbourne Journal of International Law* [online]. 2013, 14 (2), s. 496-519 [cit. 2019-10-21]. ISSN 14448602. Dostupné z: http://heinonline. org/HOL/Page?handle=hein. journals/meljil14&div=19.

[241] Antonopoulos, op. cit., s. 64.

[242] CROOTOF, R. International Cybertorts: Expanding State Accountability in Cyberspace. *Cornell Law Review* [online]. 2017, 103 (3), s. 619 [cit. 2019-10-21]. ISSN 00108847. Dostupné z: http://heinonline. org/HOL/Page?handle=hein. journals/clqv103&div=18.

[243] ROSCINI, M. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas International Law Journal* [online]. 2015, 50 (2-3), s. 251 [cit. 2019-11-22]. ISSN 01637479. Dostupné z: http://heinonline.org/HOL/Page?handle=hein.journals/tilj50&div=12.

technologická specifika je v této oblasti dostupnost, přímost a věrohodnost důkazů ještě více rozporuplná. V kyberprostoru též velmi vážně hrozí, že důkazy mohou být falšované nebo účelově vytvořené. Vzhledem k tomu, že v současné době neexistuje žádná obecně uznávaná praxe států nebo mezinárodní smlouva, která by určovala, kolik důkazů a jakého typu je nutné mít pro založení mezinárodněprávní odpovědnosti určitého státu,[244] bude věcí příslušných orgánů, aby rozhodly, které důkazy budou přesvědčivé pro jejich rozhodnutí.[245]

Pro některé autory představuje řešení této ožehavé situace též závazek due diligence, o kterém bylo pojednáno výše v kapitole 3.2.5. Za současného stavu ale k naplnění článku 8 ARSIWA bude pravděpodobně docházet velice ojediněle, jako kupříkladu v následujícím ilustrativním příkladu: Informační společnost Omega se sídlem ve státě A, kde tento v ní vlastní i většinový podíl, provedla kybernetickou operaci vůči zařízení nacházejícímu se ve státě B, která by zakládala narušení suverenity později jmenovaného státu a způsobila mu tak nemalou fyzickou škodu. Samotný vlastnický podíl státu A nesvědčí o efektivní kontrole vykonávané nad společností Omega, žádné jiné přímé důkazy stát B nemá. Jednání společnosti Omega, tak státu A přičitatelné nebude. Poté co bývalý zaměstnanec společnosti Omega emigruje do státu B, tento mu předloží celou řadu elektronické korespondence mezi vládními představiteli státu A a zaměstnanci společnosti Omega, kteří provedli kybernetickou operaci. Součástí dokumentů jsou i přímé důkazy svědčící o poskytnutí škodlivého počítačového programu a udělení konkrétních pokynů k jeho využití při škodlivé kybernetické operaci vůči státu B. Dostupné důkazy nyní přímo svědčí o skutečném zapojení státu A, který tak za protiprávní jednání společnosti Omega ponese odpovědnost a stát B vůči němu bude moci uplatnit své nároky.

3.3.4. Dílčí shrnutí

Z kapitoly 3.3 zcela jasně vyplývá, že stanovení mezinárodní odpovědnosti za protiprávní jednání v kyberprostoru ve většině případů ztroskotá právě na prvku přičitatelnosti, jehož koncepty je s ohledem na povahu kyberprostoru velice těžké naplnit. V této oblasti tedy současná právní úprava zcela jednoznačně nereflektuje aktuální technologický stav a významně za ním zaostává.

Největší potíže činí zejména přičitatelnost podle článku 8 ARSIWA, kde ze současného stavu vyplývá, že k prokázání skutečného spojení mezi nestátním aktérem a konkrétním státem

[244] BANKS, W. State Responsibility and Attribution of Cyber Intrusions after Tallinn 2. 0. *Texas Law Review* [online]. 2016, 95 (7), s. 1504 [cit. 2019-10-28]. ISSN 00404411. Dostupné z: http://heinonline.org/HOL/Page?handle=hein. journals/tlr95&div=54.
[245] Srov. Costa a Benn, op. cit., s. 133.

chybí důkazy, které bude, jak jsme viděli v ilustrativním příkladě výše, ve většině případů muset vynést někdo zevnitř (*leak*). Lze se ale s takovým stavem spokojit?

Vzhledem k tomu, že i zde platí, že se přijetí mezinárodní úmluvy, která by autoritativně upravila pravidla přičitatelnosti pro kyberprostor, zdá v nejbližších letech přinejmenším nepravděpodobné, navrhuje doktrína několik variant řešení, jak problému s přičitatelností čelit. Přestože se obrácení důkazního břemene a spoleh na nepřímé důkazy může s ohledem na povahu kyberprostoru zdát jako přijatelné řešení, autorka této práce nenabyla dojmu, že by se tyto varianty těšily široké podpoře, a to ani ze strany doktríny, ani ze strany států. Nakolik se současný stav může zdát vůči obětem kybernetických operací nespravedlivý, právo musí poskytovat záruky jak obětem, tak podezřelým, což převrácení důkazního břemene ani nepřímé důkazy nezajistí. Tak jako většina doktríny se tedy autorka této práce přiklání k řešení této situace skrze závazek due diligence, který byl popsán výše v bodě 3.2.5.

3.4. Reakce na kybernetickou operaci

Pokud se stát stane obětí kybernetického útoku, pravděpodobně bude na něj, tak jako na jakékoli jiné protiprávní jednání, chtít reagovat, aby pachatele odradil od pokračování v něm.[246] Vzhledem k tomu, že hledání viníka, tedy státu odpovědného za danou kybernetickou operaci, je často velice časově náročné, mezinárodní právo staví poškozené státy do neudržitelné pozice, pokud chtějí efektivně, ovšem nikoli protiprávně, reagovat na kybernetickou operaci, která nedosahuje úrovně použití síly.[247] Aby totiž poškozený stát mohl uplatnit obranu vůči určitému státu, musí nejprve určit, vůči kterému konkrétnímu státu se má vymezit.[248] V této souvislosti tak jistě nelze vyloučit situace, kdy se stát z důvodu časové tísně spolehne na aktuálně dostupné informace, učiní si chybný úsudek a podrobí protiopatřením stát, který za útok odpovědnost neponese. V takovém případě se původně poškozený stát sám dopustí mezinárodně protiprávního jednání. Pokud ale poškozený stát bude čekat na odpověď příliš dlouho, jeho protiopatření mohou být buď zcela neefektivní, za dané situace již nepotřebná, anebo jeho reakce bude mít represivní charakter, což je v mezinárodním právu rovněž zakázáno.

Přestože se jedná o odpověď na mezinárodně protiprávní jednání, tato nemůže být bezbřehá. K jejímu uskutečnění mezinárodní právo vyžaduje „*a) předchozí oznámení pachateli, a b)*

[246] Tallinn Manual 2.0, Rule 20, paras. 1 – 2.
[247] TSAGOURIAS, N. Cyber Attacks, Self-Defence and the Problem of Attribution. *Journal of Conflict and Security Law* [online]. 2012, 17 (2), s. 230 [cit. 2019-10-27]. ISSN 14677962. Dostupné z: http://heinonline.org/HOL/Page?handle=hein. journals/jcsl17&div=17.
[248] Banks, op. cit., s. 1493 – 1497.

poskytnutí příležitosti, aby od protiprávního jednání upustil; přičemž protiopatření musí být jednak přiměřené původnímu porušení a jednak jejich cílem musí být znovunastolení souladu s mezinárodním právem, nikoli represe nebo odveta".[249]

Kybernetické útoky jsou využívány zejména z důvodu jejich nepředvídatelnosti, rychlému a efektivnímu zásahu cíle a obtížnému vypátrání skutečného pachatele. Již z jejich samotné povahy tedy plyne, že neposkytují dostatek času nejen ke zjištění pachatele a přičtení jeho jednání konkrétnímu státu, natož pak k oznámení pachateli a poskytnutí příležitosti k zastavení jeho protiprávního jednání. Trvat nekompromisně na pravidlech, která pro učinění protiopatření vyžadují předchozí oznámení státu-pachateli a poskytnutí možnosti, aby od protiprávního jednání dobrovolně upustil, se tedy v kybernetickém kontextu zdá přinejmenším jako neefektivní.[250] V kybernetickém prostoru se tak, co se týče možných protiopatření směřujících vůči protiprávnímu jednání, které nedosahuje úrovně použití síly, s ohledem na příliš přísná pravidla jejich použití, dostáváme do patové situace, kdy státy buď nemohou protiopatření učinit z důvodů právních anebo z důvodů politických.[251]

V návaznosti na předchozí bod 3.3.3 bych ještě ráda upozornila na skutečnost, že míra dokazování se bude lišit v závislosti na jeho účelu. Zatímco v případech, kdy je účelem pouhé odsouzení státu ve vnitrostátních sdělovacích prostředcích bez dalších souvisejících následků, rozsáhlé dokazování nebude nutné provádět; při identifikaci státu, proti kterému je třeba provést protiopatření, bude zpravidla stačit, pokud poškozený stát zjistí, ze kterého státu byla kybernetická operace vedena a že tento zanedbal svůj závazek due diligence; je-li cílem sebeobrana, bude zapotřebí prokázat mnohem více okolností.[252]

[249] Tallinn Manual 2.0, Rules 20 – 23.
[250] Banks, op. cit., s. 1502.
[251] DAVIS II, J. S., J. W. WELBURN, B. BOUDREAUX a J. AGUIRRE. When Cyber Attacks Occur, Who Should Investigate? *The Rand Blog* [online]. 6 December 2018 [cit. 2019-11-04]. Dostupné z: https://www.rand.org/blog/2018/12/when-cyber-attacks-occur-who-should-investigate.html.
[252] Roscini, op. cit., s. 239.

Závěr

Přestože se nám kybernetický svět může zdát na míle vzdálený, přicházíme s ním do styku každý den. K prvnímu setkání dochází hned ráno po probuzení, kdy vypínáme budíky na svých chytrých telefonech a kontakt pokračuje v průběhu celého dne, ať už ve chvíli, kdy platíme za kávu v našem oblíbeném podniku prostřednictvím platebního terminálu, přecházíme silnici na pokyn semaforu, či když při cestě do školy nebo do práce v metru na světelné tabuli kontrolujeme, za jak dlouho přijede náš spoj. Práci bez počítačů si dnes už umíme představit jen stěží. Žádná z námi využívaných zařízení by pochopitelně nefungovala bez přívodu energie, jejíž distribuce je řízena, *jak jinak*, než prostřednictvím kybernetických zařízení.

Kyberprostor se tedy dotýká téměř každého aspektu našich životů. Přináší nám obrovské výhody, které ale ruku v ruce s sebou přináší i zcela zásadní rizika. To jakým způsobem jsme se naučili v kyberprostoru pohybovat a využívat všech jeho benefitů, zároveň přináší i velké možnosti k páchání škodlivých kybernetických operací. Zneužití informačních a komunikačních technologií má stoupající tendenci, přičemž jejich stále zvyšující se sofistikovanost je až dechberoucí. Škodlivé kybernetické operace tak nadále neznamenají pouze krádeže identity a přístupových údajů k bankovním účtům, ale stále častěji narušují též suverenitu jednotlivých států a v konečném důsledku mohou představovat i obrovské nebezpečí pro mezinárodní mír a bezpečnost.

Nástup informačních a komunikačních technologií přišel tak rychle, že zastihl právo zcela nepřipravené, které na nastalou situaci stíhá jen stěží adekvátně reagovat. Kromě regionálních mezinárodních smluv upravujících kybernetickou kriminalitu, výstupů z práce skupiny vládních expertů v oblasti informací a telekomunikací ve vztahu k mezinárodní bezpečnosti, dvou Tallinnských Manuálů a několika rezolucí Valného shromáždění OSN neposkytují primární prameny mezinárodního práva bližší pohled na propojení mezinárodního práva a kyberprostoru. O interpretaci stávajících norem obecného mezinárodního práva se tak stará především doktrína, která sice soustavně apeluje na mezinárodní společenství, aby zvážilo přijetí mezinárodní úmluvy, která by sporné otázky autoritativně vyřešila, zatím ale bez úspěchu.

První výzkumná otázka cílila na popsání způsobu aplikace pravidel obecného mezinárodního práva na jednání učiněné v kyberprostoru. Předkládaná práce jednoznačně prokázala, že presumovaný závěr o uplatnění pravidel obecného mezinárodního práva v kyberprostoru, je pravdivý, neboť i zde se uplatní primární pravidla vyplývající jak z mezinárodních obyčejů, tak z Charty OSN či ARSIWA. Na ilustrativních příkladech bylo

dostatečně demonstrováno, že aspekty, které se zdají problematické i v reálném světě, například otázka použití síly v sebeobraně vůči nestátním aktérům, jejichž jednání není státu přičitatelné, či přičitatelnost jednání nestátních aktérů obecně, přináší v kyberprostoru problémy ještě větší.

S první výzkumnou otázkou je neodmyslitelně spjata druhá výzkumná otázka, která si kladla ambice na zhodnocení efektivity některých stávajících pravidel obecného mezinárodního práva na jednání v kyberprostoru. Vzhledem k tomu, že až doposud nebyl oficiálně žádný stát shledán odpovědným za porušení mezinárodního práva v souvislosti s jednáním v kyberprostoru, uvedené značí pouze dvě možné odpovědi – buď k protiprávnímu jednání v kyberprostoru vůbec nedochází, nebo obecné mezinárodní právo neposkytuje dostatečný podklad pro aplikaci v kyberprostoru.

Prvně uvedené tvrzení se bezpochyby nezakládá na pravdě, jak prokazuje kapitola 3.2, která zcela jasně ukázala, že státy v kyberprostoru porušují zejména suverenitu jiných států a činí tak různými způsoby s různou intenzitou narušení. V této souvislosti byla shledán neefektivním zejména současný výklad hrozby a použití síly, který i v kyberprostoru vyžaduje způsobení fyzické škody, což je s ohledem na skutečnost, že většina kybernetických operací takové následky nemá, velice nešťastné.

Neuspokojivým byl shledán též stávající koncept kontroly vyžadovaný k prokázání faktického spojení mezi jednáním nestátních aktérů a konkrétním státem, neboť s ohledem na skutečnost, že v kyberprostoru je ve většině případů nemožné identifikovat konkrétního pachatele kybernetické operace, lze jen těžko prokázat faktické spojení mezi ním a státem, jemuž má být jeho jednání přičteno.

Jak na daný stav reagovat se tázala třetí výzkumná otázka. Ve vztahu k hrozbě a použití síly bylo navrženo vykládat čl. 2 odst. 4 Charty OSN extenzivně tak, aby do jejího rámce byly zahrnuty nejen kybernetické operace, které způsobí škody srovnatelné s následky kinetické operace zakládající použití síly, ale i kybernetické operace, které ji způsobí až sekundárně.

V souvislosti s přičitatelností jednání nestátních aktérů byla navržena celá řada řešení, od převrácení důkazního břemene, přes upřednostnění nepřímých důkazů, snížení standardu vyžadované kontroly až po závazek due diligence, který v současnosti představuje pravděpodobně nejlepší řešení. Ačkoli se i tato povinnost aplikuje pouze za splnění určitých podmínek, tyto se zdají rozumně nastavené.

Bylo shledáno, že ačkoli doktrína považuje celou řadu otázek spojených s mezinárodní odpovědností v kyberprostoru neuspokojivě řešenými, státy nemají příliš velký zájem na její bližší úpravě, neboť se obávají, že by na ně mohla klást příliš vysoké nároky a zatížit je dalšími povinnostmi. I v případech, kdy se státy stanou obětí závažné škodlivé protiprávní kybernetické

operace, tyto zůstávají spíše zdrženlivé při „obvinění“ jiného státu z jejího spáchání a s nastalou situací se snaží vyrovnat samostatně, což dokládá i skutečnost, že o většině takových událostí je veřejně známo jen málo informací a kromě případu Estonska, které se s žádostí o pomoc obrátilo na NATO, nebyl až doposud žádný z případů závažných škodlivých kybernetických operací předložen žádnému z mezinárodních orgánů. Dokud se tedy státy budou striktně držet tohoto postoje, nelze očekávat, že by se v této oblasti něco výrazně změnilo.

Kromě odpovědnosti státu za protiprávní jednání v kyberprostoru vůči jiným státům, je ve světě i u nás stále častěji diskutována též otázka odpovědnosti za protiprávní jednání státu vůči jednotlivci, a to v důsledku nástrojů hromadného sledování osob, které ve většině případů závažně narušuje právo na soukromí. Přestože je tento fenomén nejčastěji ospravedlňován poukazem na boj proti terorismu, je tato otázka jistě zajímavým tématem k dalšímu výzkumu, neboť zajisté není možné každé porušování lidských práv ospravedlňovat takto alibisticky. Další zajímavé odvětví pak představuje i využití kyberprostoru v rámci ozbrojeného konfliktu a s tím související aplikace mezinárodního humanitárního práva.

Na úplný závěr bych ráda dodala, že předkládané téma je relevantní též pro Českou republiku, která sice v porovnání s jinými státy světa není častým cílem kybernetických operací, ale i zde má kyberzločin stoupající tendenci a v minulosti již došlo k několika pokusům například o narušení našeho volebního procesu ze strany jiného státního aktéra. Ačkoli se zdá, že doposud nelze žádnou z kybernetických operací, jimž byla Česká republika podrobena, kvalifikovat jako porušení některého z mezinárodních závazků, je zapotřebí se mít na pozoru, protože to, že zatím k takové situaci nedošlo, neznamená, že k ní nemůže dojít kdykoli v budoucnu.

Seznam zkratek

ARSIWA	Články o odpovědnosti států za mezinárodně protiprávní chování
ESLP	Evropský soud pro lidská práva
IAEA	Mezinárodní agentura pro atomovou energii
ICTY	Mezinárodní trestní tribunál pro bývalou Jugoslávii
MSD (ICJ)	Mezinárodní soudní dvůr
Nicaragua	Rozsudek Mezinárodního soudního dvora ve věci Nicaragua
Tadić	Rozsudek odvolacího senátu Mezinárodního trestního tribunálu pro bývalou Jugoslávii ve věci Tadić č. IT-94-1-AR
Tallinnský Manuál	Tallinn Manual 2.0

Seznam použitých zdrojů

1. Seznam použité literatury

a. Odborné knihy

- BÍLKOVÁ, V. *Úprava vnitrostátních ozbrojených konfliktů v mezinárodním humanitárním právu*. Praha: Univerzita Karlova v Praze, Právnická fakulta v nakl. IFEC, Beroun, 2007, 333 s. Prameny a nové proudy právní vědy. ISBN 80-85889-82-6
- CRAWFORD, J. *State Responsibility: The General Part*. New York: Cambridge University Press, 2013, 831 s. ISBN 978-0-521-82266
- CRAWFORD, J., A. PELLET a S. OLLESON (eds.). *The law of international responsibility*. New York: Oxford University Press, 2010, 1296 s. ISBN 978-0-19929697-2
- ČEPELKA, Č. a P. ŠTURMA. *Mezinárodní právo veřejné*. 2. vydání. Praha: C. H. Beck, 2018, 549 s. Academia iuris (C. H. Beck). ISBN 978-80-7400-721-7
- DAVID, V. , P. SLADKÝ a F. ZBOŘIL. *Mezinárodní právo veřejné s kazuistikou*. Praha: Leges, 2008, 427 s. Student (Leges). ISBN 978-80-87212-08-0
- DAVID, V. a kol. *Mezinárodní právo veřejné s kazuistikou*. 2., aktualiz. a přeprac. vyd. Praha: Leges, 2011, 448 s. Student (Leges). ISBN 978-80-87212-86-8
- DIXON, M. *Textbook on international law*. 6th ed. New York: Oxford University Press, 2007, 372 s. ISBN 978-0-19-920818-0
- DUFFY, H. *The 'war on terror' and the framework of international law.* 2. Cambridge: Cambridge University Press, 2015, 993 s. ISBN 9781107601727
- GATTIKER, U. E. *The Information Security Dictionary: Defining the Terms that Define Security for E-Business, Internet, Information and Wireless Technology*. Springer US, 2004, 410 s. ISBN 978-1-4020-7927-6
- CHURAŇ, M. *Encyklopedie špionáže: ze zákulisí tajných služeb, zejména Státní bezpečnosti.* 2. přeprac. a aktualiz. vyd. Praha: Libri, 2000, 431 s. ISBN 8072770209
- KREMLING, J. a A. M. SHARP PARKER. Cyberspace, Cybersecurity, and Cybercrime. *Cyberspace, cybersecurity, and cybercrime*. Los Angeles: SAGE, 2018, s. 113. ISBN 978-1-506-347257
- MALENOVSKÝ, J. *Mezinárodní právo veřejné: obecná část a poměr k jiným právním systémům*. 6. , upr. a dopl. vyd. Brno: Doplněk, 2014, 499 s. ISBN 978-80-7380-531-9

- ONDŘEJ, J. *Odzbrojení: prostředek k zajištění mezinárodní bezpečnosti*. 2., rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2008, 343 s. ISBN 978-80-7380-129-8
- SCHMITT, M. N. *Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. New York: Cambridge University Press, 2013. ISBN 978-1-107-02443-4
- SCHMITT, M. N. *Tallinn manual 2. 0 on the international law applicable to cyber operations*. 2. vyd. New York: Cambridge University Press, 2017. ISBN 978-1-107-17722-2 (Tallinn Manual 2. 0)
- ŠTURMA, P. a kol. *Casebook: výběr případů z mezinárodního práva veřejného*. 4. upravené vydání. Praha: Univerzita Karlova, Právnická fakulta, 2019. Scripta iuridica. ISBN 978-80-87975-91-6.

b. Příspěvky ve sbornících

- ANTONOPOULOS, C. State responsibility in cyberspace. In: TSAGOURIAS, N. a R. BUCHAN (eds.). *Research handbook on international law and cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 2015, s. 55-72. ISBN 978-1-78254-738-9
- BÍLKOVÁ, V. Území státu a územní změny. In: ŠTURMA P. (ed.) a kol. *Mezinárodní právo a státní území*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2015, s. 9-26. ISBN 978-80-87975-42-8
- BRUNER, T. K podmínkám a způsobu aplikace mezinárodního humanitárního práva na kybernetické operace. In: BÍLKOVÁ, V. (ed.) *Mezinárodní humanitární právo: vznik, vývoj a nové výzvy*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2015, s. 159 - 171. ISBN 978-80-87975-35-0
- FOCARELLI, C. Self-defence in cyberspace. In: TSAGOURIAS, N. a R. BUCHAN (eds.). *Research handbook on international law and cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 2015, s. 255-284. ISBN 978-1-78254-738-9
- HÝBNEROVÁ, S. Použití extrateritoriální síly proti nestátním aktérům v kontextu mezinárodního práva. In: *Nové trendy odpovědnosti a řešení sporů v mezinárodním právu: (vliv nestátních aktérů)*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2012, s. 22-37. ISBN 978-80-87146-73-6

- RANDELZHOFER, A. Article 2 (4). In: SIMMA, B. (ed.). *The Charter of the United Nations: a commentary. Vol. I*. 2. Oxford: Oxford University Press, 2002, s. 117-136. ISBN 0199244499
- RANDELZHOFER, A. Article 51. In: SIMMA, B. (ed.). *The Charter of the United Nations: a commentary. Vol. I*. 2. Oxford: Oxford University Press, 2002, s. 788-806. ISBN 0199244499
- ROSCINI, M. Cyber operations as a use of force. In: TSAGOURIAS, N. a R. BUCHAN (eds.) *Research handbook on international law and cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 2015, s. 233-255. ISBN 978-1-78254-738-9
- SCHMITT, M. N. The Use of Cyber Force and International Law. In: WELLER, M., A. SOLOMOU a J. W. RYLATT. *The Oxford handbook of the use of force in international law*. Oxford: Oxford University Press, 2015, s. 1110-1131. Oxford handbooks. ISBN 978-0-19-967304-9
- TRAPP, K. N. Can Non-State Actors Mount to an Armed Attack? WELLER, M., A. SOLOMOU a J. W. RYLATT (eds.). *The Oxford handbook of the use of force in international law*. Oxford: Oxford University Press. 2015, s. 679-697. Oxford handbooks. ISBN 978-0-19-967304-9

c. Odborné články

- POTOČNÝ, M. Zásada svrchované rovnosti států. *Mezinárodní vztahy*. Praha: Ústav mezinárodních vztahů. 1968, 3 (4), s. 3-9

2. Seznam použitých elektronických zdrojů

a. Elektronické publikace

- Droit international appliqué aux opérations dans le cyberspace. In: *Ministère des Armées* [online]. 4 Novembre 2019 [cit. 2019-11-24]. Dostupné z: https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international
- Joint Chiefs of States. JP 3-12, Cyber Operations. In: *Federation of American Scientists* [online]. 2018 [cit. 2019-10-05]. Dostupné z https://fas. org/irp/doddir/dod/jp3_12. pdf.

- KITTICHAISAREE, K. *Public International Law of Cyberspace*. Springer, 2017, 376 s. DOI https://doi.org/10.1007/978-3-319-54657-5. ISBN 978-3-319-54657-5. ISSN 2352-1910
- NÚKIB. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2018 [online]. 2019, 67 s. [cit. 2019-11-24]. Dostupné z: https://www.nukib.cz/cs/informacni-servis/publikace/
- YANNAKOGEORGOS, P. A. *Strategies for resolving the cyber attribution challenge* [online]. Maxwell Air Force Base, Alabama: Air University Press, Air Force Research Institute, 2013, 85 s. [cit. 2019-11-23]. ISBN 978-1-58566-226-5. Dostupné z: https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/cpp_0001_yannakogeorgos_cyber_Attribution_challenge.PDF
- ZIOLKOWSKI, K. General Principles of International Law as Applicable in Cyberspace. In: ZIOLKOWSKI, K (ed.). *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* [online]. Tallinn: NATO CCDCOE, 2013, s. 135-184 [cit. 2019-11-29]. ISBN 978-9949-9211-8-8. Dostupné z: https://ccdcoe.org/uploads/2018/10/PeacetimeRegime.pdf

b. Odborné elektronické články

- ALLAN, C. S. Attribution Issues in Cyberspace. *Chicago-Kent Journal of International and Comparative Law* [online]. 2013, 13 (2), s. 55-83. [cit. 2019-11-24]. Dostupné z: https://ssrn.com/abstract=2617870
- ÁLVAREZ ORTEGA, E. L. The attribution of international responsibility to a State for conduct of private individuals within the territory of another State. *InDret: Revista para el análisis del derecho* [online]. 2015, s. 10 [cit. 2019-10-20]. Dostupné z: http://www. indret. com/pdf/1116_es. pdf
- BAKER, CH. D. Tolerance of International Espionage: A Functional Approach. *American University International Law Review* [online]. 2003, 19 (5), s. 1091-1114 [cit. 2019-11-12]. ISSN 1520460X. Dostupné z: http://heinonline. org/HOL/Page?handle=hein. journals/amuilr19&div=33
- BANKS, W. State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0. *Texas Law Review* [online]. 2016, 95 (7), s. 1487-1514 [cit. 2019-10-28]. ISSN 00404411. Dostupné z: http://heinonline. org/HOL/Page?handle=hein. journals/tlr95&div=54

- BARLOW, J. P. A Declaration of the Independence of Cyberspace. In: *EFF* [online]. 1996 [cit. 2019-10-05]. Dostupné z https://www. eff. org/cyberspace-independence
- BASTL, M. a Z. GRUBEROVÁ. Kyberprostor jako „pátá doména"?. *Vojenské rozhledy* [online]. 2013 (4), s. 10-21 [cit. 2019-10-05]. Dostupné z: http://vojenskerozhledy. cz/kategorie-clanku/bezpecnostni-prostredi/kyberprostor-jako-pata-domena
- BORDIN, F. L. Reflections of Customary International Law: The Authority of Codification Conventions and ILC Draft Articles in International Law. *International and Comparative Law Quarterly* [online]. 2014, 63 (3), s. 535-568 [cit. 2019-10-13]. ISSN 14716895. Dostupné z: http://heinonline. org/HOL/Page?handle=hein. journals/incolq63&div=33
- BUCHAN, R. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions. *Journal of Conflict and Security Law* [online]. 2012, 17 (2), s. 211-228 [cit. 2019-11-28]. ISSN 14677962. Dostupné z: http://heinonline.org/HOL/Page?handle=hein.journals/jcsl17&div=16
- CANCA, H. S. Prohibition against the use of force and the coercive uses of the cyberspace. *Journal of Naval Science and Engineering* [online]. 2017, 13 (1), s. 60-72 [cit. 2019-11-28]. ISSN 13042025. Dostupné z: https://doaj.org/toc/1304-2025
- CASSESE, A. The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia. *European Journal of International Law* [online]. 2007, 18 (4), s. 649-668 [cit. 2019-11-24]. ISSN 09385428. Dostupné z: https://heinonline.org/HOL/Page?handle=hein.journals/eurint18&div=41
- CLARK, D. D. a S. LANDAU. The Problem isn't Attribution; It's Multi-Stage Attacks. In: *ACM ReArch 2010* [online]. Philadelphia, USA, 2010. [cit. 2019-11-23]. Dostupné z: https://conferences.sigcomm.org/co-next/2010/Workshops/REARCH/ReArch_papers/11-Clark.pdf
- COSTA, F. G. D. a V. L. H. BENN. The Challenges of Attribution of Internationally Wrongful Acts in the Cyberspace: A Critical Analysis of Control Tests and the Standard of Proof in International Courts. *Revista do CEPEJ* [online]. Salvador, 2016, 19 (Ed. Especial), s. 121-146 [cit. 2019-11-24]. Dostupné z: https://portalseer.ufba.br/index.php/CEPEJ/article/download/22043/14199
- CROOTOF, R. International Cybertorts: Expanding State Accountability in Cyberspace. *Cornell Law Review* [online]. 2017, 103 (3), s. 565-644 [cit. 2019-10-21]. ISSN 00108847. Dostupné z: http://heinonline. org/HOL/Page?handle=hein. journals/clqv103&div=18

- DELERUE, F. Reinterpretation or Contestation of International Law in Cyberspace? *Israel Law Review* [online]. Cambridge University Press, 2019, 52 (3), s. 295-326 [cit. 2019-11-24]. ISSN 00212237. Dostupné z: https://search.ebscohost.com/login.aspx?authtype=shib&custid=s1240919&profile=eds
- DELIBASIS, D. The Right of States to Use Force in Cyberspace: Defining the Rules of Engagement. *Information & Communications Technology Law* [online]. 2002, 11 (3), s. 255-268 [cit. 2019-11-28]. ISSN 13600834. Dostupné z: http://heinonline.org/HOL/Page?handle=hein.journals/infctel11&div=21
- DEV, P. R. Use of Force and Armed Attack Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response. *Texas International Law Journal* [online]. 2015, 50 (2-3), s. 381-402 [cit. 2019-11-27]. ISSN 01637479. Dostupné z: http://heinonline.org/HOL/Page?handle=hein.journals/tilj50&div=16
- DINSTEIN, Y. Computer Network Attacks and Self-Defense. *International Law Studies Series. US Naval War College* [online]. 2002, 76, s. 99-119 [cit. 2019-11-16]. ISSN 23752831. Dostupné z: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1397&context=ils
- GREENWOOD, CH. The Development of International Humanitarian Law by the International Criminal Tribunal for the Former Yugoslavia. *Max Planck Yearbook of United Nations Law* [online]. 1998, 2, s. 97-140 [cit. 2019-10-19]. ISSN 13894633. Dostupné z: https://www. mpil. de/files/pdf2/mpunyb_greenwood_2. pdf
- HAATAJA, S. a A. KHTAR-KHAVARI. Stuxnet and International Law on the Use of Force: An Informational Approach. *Cambridge International Law Journal* [online]. 2018, 7 (1), s. 99-121 [cit. 2019-11-04]. Dostupné z: https://heinonline. org/HOL/LandingPage?handle=hein. journals/cajoincla7&div=8&id=&page=
- HOISINGTON, M. Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. *Boston College International and Comparative Law Review* [online]. 2009, 32 (2), s. 439-454 [cit. 2019-11-28]. ISSN 02775778. Dostupné z: http://heinonline.org/HOL/Page?handle=hein.journals/bcic32&div=28
- HUXTABLE, H. E.T. Phoned Home...They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance. *Security* [online]. 2019, 28 (1-4), s. 92-112 [cit. 2019-11-29]. DOI: 10.1163/18750230-02801010. ISSN 18747337. Dostupné z: https://brill.com/view/journals/shrs/28/1-4/article-p92_92.xml?lang=en

- CHIRCOP, L. A Due Diligence Standard of Attribution in Cyberspace. *International and Comparative Law Quarterly* [online]. 2018, 67 (3), s. 643-668 [cit. 2019-11-12]. ISSN 14716895. Dostupné z: http://heinonline. org/HOL/Page?handle=hein. journals/incolq67&div=34
- JAMNEJAD, M. a M. WOOD. The Principle of Non-intervention. *Leiden Journal of International Law* [online]. 2009, 22 (2), s. 345-382 [cit. 2019-11-28]. ISSN 09221565. Dostupné z: http://heinonline.org/HOL/Page?handle=hein.journals/lejint22&div=24
- JOHNSON, D. R. a D. POST. Law and boarders: The rise of law in cyberspace. *Stanford Law Review* [online]. 1996, 48 (5), s. 1367 - 1402 [cit. 2019-10-07]. Dostupné z https://heinonline. org/HOL/P?h=hein. journals/stflr48&i=1385
- KADLECOVÁ, L. State Responsibility in the Cyber Age: The Course towards Indirect Evidence. *Mezinárodní vztahy* [online]. 2019, 53 (4), s. 35-46 [cit. 2019-11-24]. ISSN 03231844. Dostupné z: https://mv.iir.cz/article/view/1585/1482
- KOLOUCH, J. Kyberprostor. In: *Teorie informační bezpečnosti* [online]. 2016 [cit. 2019-10-05]. Dostupné z http://www. teorieib. cz/pbi/files/281-Kyberprostor-Kolouch. pdf
- KÖNIGOVÁ, L. Teorie státní suverenity a praxe intervence. *Mezinárodní vztahy* [online]. 2001, (3), 41-58 [cit. 2019-10-31]. Dostupné z: https://mv. iir. cz/article/view/691/736
- KSHETRI, N. *Cybersecurity and International Relations: The U. S. Engagement with China and Russia* [online]. 2014 [cit. 2019-11-16]. Dostupné z: http://web. isanet. org/Web/Conferences/FLACSO-ISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf. pdf
- LIU, I. Y. State Responsibility and Cyberattacks: Defining Due Diligence Obligations. *Indonesian Journal of International* [online]. 2017, 4 (2), s. 191 - 260 [cit. 2019-11-12]. ISSN 23387602. Dostupné z: http://heinonline. org/HOL/Page?handle=hein. journals/indjicl4&div=15
- LIU, I. Y. The due diligence doctrine under Tallinn Manual 2.0. *Computer Law* [online]. 2017, 33 (3), s. 390-395 [cit. 2019-11-30]. DOI: 10.1016/j.clsr.2017.03.023. ISSN 02673649
- MAČÁK, K. Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law* [online]. 2016, 21 (3), 405-428 [cit. 2019-10-28]. ISSN 14677954. Dostupné z: https://heinonline. org/HOL/Page?handle=hein. journals/jcsl21&div=29

- MARGULIES, P. Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. *Melbourne Journal of International Law* [online]. 2013, 14 (2), s. 496-519 [cit. 2019-10-21]. ISSN 14448602. Dostupné z: http://heinonline.org/HOL/Page?handle=hein. journals/meljil14&div=19
- NYMAN METCALF, K. A Legal View on Outer Space and Cyberspace: similarities and differences. *Tallinn Papers No. 10* [online]. CCDCOE, 2018 [cit. 2019-10-10]. Dostupné https://ccdcoe. org/uploads/2018/10/Tallinn-Paper_10_2018. pdf
- PAYNE, T. Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations. *Lewis & Clark Law Review* [online]. 2016, 20 (2), s. 683-715 [cit. 2019-10-21]. ISSN 1557-6582. Dostupné z: http://heinonline.org/HOL/Page?handle=hein. journals/lewclr20&div=22
- REINISCH, A. a M. BEHAM. Mitigating Risks: Inter-State Due Diligence Obligations in Case of Harmful Cyber-Incidents and Malicious Cyber-Activity – Obligations of the Transit State. *German Yearbook of International Law* [online]. 2015, 48, s. 101-112 [cit. 2019-11-29]. Dostupné z: https://ssrn.com/abstract=2664322
- ROSCINI, M. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas International Law Journal* [online]. 2015, 50 (2-3), s. 233-274 [cit. 2019-11-22]. ISSN 01637479. Dostupné z: Grey Zones in the International Law of Cyberspace http://heinonline.org/HOL/Page?handle=hein.journals/tilj50&div=12
- ROSCINI, M. World Wide Warfare - Jus ad Bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law* [online]. 2010, 14 (1), s. 85-130 [cit. 2019-11-27]. ISSN 13894633. Dostupné z: https://www.mpil.de/files/pdf3/mpunyb_03_roscini_141.pdf
- SCHMITT, M. N. Grey Zones in the International Law of Cyberspace. *Yale Journal of International Law* [online]. 2017, 42 (2) [cit. 2019-10-27]. Dostupné z: https://ssrn.com/abstract=3180687
- SCHMITT, M. N. In Defense of Due Diligence in Cyberspace. *Yale Law Journal Forum* [online]. 2015, 22 June 2015, 125 (68), s. 68-81 [cit. 2019-11-29]. Dostupné z: http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace
- SCHMITT, M. a L. VIHUL. Respect for Sovereignty in Cyberspace. *Texas Law Review* [online]. 2017, 95 (7), s. 1639 – 1676 [cit. 2019-10-27]. Dostupné z: http://heinonline.org/HOL/Page?handle=hein. journals/tlr95&div=61

- TANODOMDEJ, P. The Tallinn Manuals and the Making of the International Law on Cyber Operations. *Masaryk University Journal of Law and Technology* [online]. 2019, 13 (1), s. 67-86 [cit. 2019-10-11]. DOI: 10. 5817/MUJLT2019-1-4. ISSN 1802-5951. Dostupné z: https://journals. muni. cz/mujlt/article/view/11810
- TANYILDIZI, M. E. STATE RESPONSIBILITY IN CYBERSPACE: THE PROBLEM OF ATTRIBUTION OF CYBERATTACKS CONDUCTED BY NON-STATE ACTORS. *Law & Justice Review* [online]. 2017, 8 (14), s. 119-176 [cit. 2019-10-27]. Dostupné z: https://ssrn. com/abstract=3047076
- TSAGOURIAS, N. Cyber Attacks, Self-Defence and the Problem of Attribution. *Journal of Conflict and Security Law* [online]. 2012, 17 (2), s. 229-244 [cit. 2019-10-27]. ISSN 14677962. Dostupné z: http://heinonline. org/HOL/Page?handle=hein. journals/jcsl17&div=17
- WATT, E. The role of international human rights law in the protection of online privacy in the age of surveillance. In: *2017 9th International Conference on Cyber Conflict (CyCon)* [online]. IEEE, 2017, s. 93-107 [cit. 2019-11-29]. DOI: 10.23919/CYCON.2017.8240330. ISSN 2325-5374. Dostupné z: http://ieeexplore.ieee.org/document/8240330/
- WATTS, S. a T. RICHARD. Baseline Territorial Sovereignty and Cyberspace. *Lewis & Clark Law Review*. 2018, 22 (3), s. 779-840 [cit. 2019-11-29]. ISSN 15576582. Dostupné z: http://heinonline.org/HOL/Page?handle=hein.journals/lewclr22&div=28
- WU, T. S. Cyberspace sovereignty? – The Internet and the International System. *Harvard Journal of Law & Technology* [online]. 1997, 10 (3), s. 647-666 [cit. 2019-10-07]. Dostupné z http://jolt. law. harvard. edu/articles/pdf/v10/10HarvJLTech647. pdf

c. Novinové články

- CURRAN, D. My terrifying deep dive into one of Russia's largest hacking forums. *The Guardian* [online]. 24 July 2018 [cit. 2019-11-23]. Dostupné z: https://www.theguardian.com/commentisfree/2018/jul/24/darknet-dark-web-hacking-forum-internet-safety
- NAKASHIMA, E. a J. WARRICK. Stuxnet was work of U.S. and Israeli experts, officials say. *The Washington Post* [online]. 2 June 2012 [cit. 2019-12-01]. Dostupné z: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

- PAGLIERY, J. It looks like Russia and smells like Russia . . . but is it Russia?. *CNN* [online]. 31 October 2014 [cit. 2019-10-21]. Dostupné z: https://money. cnn. com/2014/10/31/technology/security/russia-hackers/index. html
- POHJANPALO, K. Finland Detects Cyber Attack on Online Election-Results Service. *Bloomberg* [online]. 10 April 2019 [cit. 2019-11-09]. Dostupné z: https://www. bloomberg.com/news/articles/2019-04-10/finland-detects-cyber-attack-on-online-election-results-service
- ZETTER, K. An Unprecedented Look at Stuxnet, the World's First Digital Weapon. *Wired* [online]. 03.11.2014 [cit. 2019-12-01]. Dostupné z: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/#

d. Jiné internetové zdroje

- DAVIS II, J. S., J. W. WELBURN, B. BOUDREAUX a J. AGUIRRE. When Cyber Attacks Occur, Who Should Investigate? *The Rand Blog* [online]. 6 December 2018 [cit. 2019-11-04]. Dostupné z: https://www.rand.org/blog/2018/12/when-cyber-attacks-occur-who-should-investigate.html
- ERBEN, L. Příchod hackerů: příběh Stuxnetu. In: *ROOT.CZ* [online]. 29.04.2014 [cit. 2019-11-30]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/
- GOLD, J. Two Incompatible Approaches to Governing Cyberspace Hinder Global Consensus. In: *Leiden Security and Global Affairs Blog* [online]. 2019 [cit. 2019-10-12]. Dostupné z: https://leidensecurityandglobalaffairs. nl/articles/two-incompatible-approaches-to-governing-cyberspace-hinder-global-consensus
- Master Table. *Hackmaggedon* [online]. [cit. 2019-10-18]. Dostupné z: https://www. hackmageddon. com/2018-master-table/
- NATO. Six Colours: War in cyberspace. In: *YouTube* [online]. 27 April 2009 [cit. 2019-11-09]. Dostupné z: https://www. youtube. com/watch?v=oGZkCdpPLBE
- Phishing, Ransomware and Co. – An increasing threat. In: *OneClick Blog* [online]. 30 October 2017 [cit. 2019-10-18]. Dostupné z: https://oneclick-cloud. com/en/blog/trends-en/increasing-threat-of-cyber-crime
- SCHJOLBERG, S. *A Geneva Declaration for Cyberspace* [online]. 2016 [cit. 2019-10-20]. Dostupné z: https://www. cybercrimelaw. net/documents/Geneva_Declaration_2016. pdf

- UNODA. Developments in the field of information and telecommunications in the context of international security. [online]. [cit. 2019-10-20]. Dostupné z: https://www. un. org/disarmament/ict-security/.
- THE COMMONWEALTH. *Model Law on Computer and Computer Related Crime* [online]. 2017 [cit. 2019-10-20]. Dostupné z: https://thecommonwealth. org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime. pdf

3. Seznam použitých právních předpisů

a. Právní předpisy České republiky

- Vyhláška ministra zahraničních věcí č. 30/1947 Sb., o chartě Spojených národů a statutu Mezinárodního soudního dvora (Charta OSN)
- Zákon č. 240/2000 Sb., o krizovém řízení (Krizový zákon)
- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

b. Právní předpisy Evropské unie

- Nařízení Evropského parlamentu a Rady (EU) 2019/881 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií (akt o kybernetické bezpečnosti)

c. Zahraniční právní předpisy

- Codice Penale, R. D. 19 ottobre 1930, n. 1938 (Trestní zákoník Italské republiky)
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (Trestní zákoník Španělského království)
- Wet van 3 maart 1881, Wetboek van Strafrecht (Trestní zákoník Nizozemského království)
- Zákon č. 69/2018 Z. z., o kybernetickej bezpečnosti (Slovenská republika)

d. Mezinárodní smlouvy

- COUNCIL OF EUROPE. *Convention on Cybercrime*. 23 November 2001. ETS No. 185 (Úmluva o počítačové kriminalitě)
- COUNCIL OF EUROPE. *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. 28 January 2003. ETS No. 189 (Dodatkový protokol k Úmluvě

o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů
- UN. *Charter of the United Nations and Statute of the International Court of Justice*. 24 October 1945. 1 UNTS XVI

e. Dokumenty mezinárodních organizací

- ILC. *State Responsibility*. In: Yearbook of the International Law Commission (Volume II Part Two): Report of the Commission to the General Assembly on the work of its fifty-third session. New York and Geneva: United Nations, 2007, s. 20-143. ISBN 978-92-1-133591-0
- Rada EU. *Společné sdělení Evropskému parlamentu, Evropské Radě, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Zpráva o provádění akčního plánu proti dezinformacím*. Brusel, 17. června 2019. JOIN(2019) 12 final
- Responsibility of States for Internationally Wrongful Acts (ARSIWA). Annex to UNGA. Resolution 56/83. 12 December 2001. UN Doc. A/56/49(Vol. I)/Corr.4
- UNGA. Advancing responsible State behaviour in cyberspace in the context of international security. 22 December 2018. UN Doc. A/RES/73/266
- UNGA. Resolution 53/70. *Developments in the field of information and telecommunications in the context of international security*. 4 January 1999, UN Doc. A/RES/53/70
- UNGA. Resolution 55/63. *Combating the criminal misuse of information technologies.* 22 January 2001. UN Doc. A/RES/55/63
- UNGA. Resolution 3314 (XXIX). *„Definition of Agression*". 14 December 1974, UN Doc A/RES/3314(XXIX)
- UNGA. *Responsibility of States for internationally wrongful acts. Compilation of decisions of international courts, tribunals and other bodies. Report to the Secretary-General*. 21 April 2016. UN Doc A/71/80
- UNGA. *Summary record of the 31st meeting*. 2 December 2016. UN Doc A/C. 6/71/SROV. 31
- UNGGE. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* 30 July 2010. UN Doc. A/65/201

- UNGGE. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* 24 June 2013. UN Doc. A/68/98
- UNGGE. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* 22 July 2015. UN Doc. A/70/174
- UNIDIR. *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century* [online]. 2017, s. 7 [cit. 2019-10-06]. Dostupné z https://www. unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691. pdf

4. Seznam použité judikatury

a. Evropský soud pro lidská práva

- *Behrami and Behrami v. France* and *Saramati v. France, Germany and Norway*, nos. 71412/01 and 78166/01, 2 May 2007
- *Loizidou v. Turkey* (merits), 18 December 1996, Reports of Judgments and Decisions 1996-VI
- *Osman v. the United Kingdom*, 28 October 1998, Reports of Judgments and Decisions 1998-VIII

b. Mezinárodní soudní dvůr

- *Case concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Yugoslavia*). ICJ Rep. 2007 (Bosenská genocida)
- *Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America*). Merits (Judgment). ICJ Rep. 1986, p. 14. (Některé vojenské a polovojenské činnosti v Nikaragui a proti ní).
- *Case concerning U. S. Diplomatic and Consular Staff in Tehran (U. S. v. Iran*), ICJ Rep. 1980, p. 3 (Diplomatický a konzulární personál USA v Teheránu).
- *Corfu Channel Case (UK v. Albania)*, ICJ Rep. 1949, p. 4 (Korfský průliv).
- *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights*, ICJ Rep. 1999, p. 62
- *Gabčíkovo-Nagymaros Project (Hungary v. Slovakia*), ICJ Rep. 1997, p. 7

- *La Grand Case (Germany v. U. S.*), ICJ Rep. 2001, p. 466
- *Legality of the Threat or Use of Nuclear Weapons,* ICJ. Rep. 1996, p. 226 (Advisory Opinion) (Legalita hrozby nebo použití jaderných zbraní)

c. Mezinárodní trestní tribunál pro bývalou Jugoslávii

- *Prosecutor v. Dusko Tadić*. ICTY Case No. IT-94-1-T, Trial Chamber, 7 May 1997
- *Prosecutor v. Dusko Tadić, Decision on the Defense Motion for Intercutory Appeal on Jurisdiction.* ICTY Case No. IT-94-1-AR, Appeals Chamber

d. Stálý dvůr mezinárodní spravedlnosti

- *German Settlers in Poland*, (1923) PCIJ Ser. B No. 6 (Advisory Opinion)

5. Jiné zdroje

- Překlad Návrhu článků o odpovědnosti států za mezinárodně protiprávní chování, poskytnutý doc. JUDr. PhDr. Veronikou Bílkovou Ph.D., E. MA v rámci výuky mezinárodního práva veřejného v akademickém roce 2015/2016

Odpovědnost státu za protiprávní jednání v kyberprostoru

Abstrakt

Tato diplomová práce se zabývá tématem odpovědnosti státu za protiprávní jednání v kyberprostoru. Předmětem jejího výzkumu je aplikace stávajících pravidel obecného mezinárodního práva vztahujících se k jednotlivým institutům mezinárodní odpovědnosti států a zhodnocení jejich efektivity při aplikaci v kyberprostoru. Diskutována je zejména otázka porušení mezinárodního závazku a přičitatelnosti jednání konkrétnímu státu v kyberprostoru, které v praxi činí největší obtíže.

V oblasti porušování mezinárodních závazků bylo shledáno, že ze strany států dochází v kyberprostoru nejčastěji k různým stupňům narušení suverenity jiných států. Diskutována je otázka ozbrojeného útoku, hrozby a použití síly, vměšování se do vnitřních nebo vnějších záležitostí jiných států, jakož i některá mírnější narušování suverenity. Prostor je věnován též závazku due diligence, kdy je vyzdvižena jeho nezastupitelná úloha zejména ve vztahu k odpovědnosti za protiprávní jednání v kyberprostoru.

V souvislosti s otázkou přičitatelnosti je prokázáno, že pravidla uvedená v Článcích o mezinárodní odpovědnosti států za mezinárodně protiprávní jednání se uplatní i na protiprávní jednání v kyberprostoru. Podrobně je rozebrána zejména otázka přičitatelnosti jednání nestátních aktérů, kdy jsou identifikována úskalí současné právní úpravy a jejího výkladu, použito je i několik ilustrativních příkladů.

Tato diplomová práce došla k závěru, že stávající pravidla mezinárodní odpovědnosti nejsou pro aplikaci v kyberprostoru dostačující, neboť valná většina škodlivých protiprávních kybernetických operací jejich sítem propadne. Přijetí mezinárodní úmluvy, která by tyto otázky autoritativně upravila by bylo žádoucí, za současného stavu a postoje jednotlivých států ale spíše nepravděpodobné. Prostor se tak otevírá spíše extenzivnímu výkladu stávajících pravidel.

Klíčová slova: Kyberprostor, protiprávní jednání státu, přičitatelnost

Responsibility of States for Unlawful Acts in Cyberspace

Abstract

This master's thesis addresses the topic of responsibility of states for unlawful acts in cyberspace. It examines the application of current international law rules regarding individual elements of international responsibility of states and it evaluates their effectivity when applied to cyberspace. In particular, this thesis discusses the issue of breach of an international obligation and its attribution to a particular state in cyberspace, which are considered the most challenging issues in practice.

In the field of breach of an international obligation, it has been found that states are mainly in breach of various levels of sovereignty of other states. The thesis has focused on an armed attack, threat or use of force, prohibited intervention and other selected issues of less severe violations of sovereignty. Particular emphasis has been put on the due diligence obligation, which has been considered irreplaceable in relation to unlawful acts in cyberspace.

With regard to the question of attribution it has been proved that rules contained in Articles on Responsibility of States for Internationally Wrongful Acts are to be applied also to unlawful acts in cyberspace. The issue of attribution of conduct by non-state actors has been discussed in detail, as well as the difficulties of current legislation and its interpretation. Various illustrative cases has been analysed as well.

This thesis has arrived to a conclusion that current international responsibility norms are not well suited for application to cyberspace, since most of malicious unlawful cyber operations do not fall within their wording. Adoption of an international treaty dealing with above mentioned issues in an authoritative manner would be desirable, however current state practice does not indicate that this could happen in the near future. Thus, the solution might be an extensive interpretation of current rules.

Key words: Cyberspace, Unlawful Act of a State, Attribution