UNIVERZITA KARLOVA

Právnická fakulta

Bc. Pavel Hrdý

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): 18.06.2021

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval/a 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 155 602 znaků včetně mezer.

Bc. Pavel Hrdý

V Praze dne 18. června 2021

Poděkování
Rád bych tímto poděkoval JUDr. Milanu Lipovskému, Ph.D., vedoucímu mé práce, za trpělivost, vstřícnost a poskytnuté rady, díky kterým bylo možné sepsání této práce.

Obsah

Úvod

„Budeme bránit náš ostrov za jakoukoli cenu, budeme bojovat na plážích, budeme bojovat na polích, ve městech i v kopcích, ale nikdy se nevzdáme“.[1] Takto zní úryvek z citátu Winstona Churchilla, který, až na moře a vzduch, jmenuje všechny tehdy známé vojenské oblasti. Od doby vyřčení tohoto citátu již uplynula řada let a lze v něm spatřovat odlišnosti vedení války. V dnešní době se s příchodem nových technologií otevírají další možné způsoby vedení války, terorismu, kriminality aj., a to za pomoci kyberprostoru.

4.54 miliard osob,[2] to je počet lidí na celém světě, kteří mají přístup k internetu. Tento počet narůstá každým dnem. Přístup k internetu značí rozvoj společnosti, v Evropě jej považujeme za samozřejmost. Volný přístup, jednoduché ovládání a celosvětový dosah, to činí z internetu nejen prostředek spojování lidí, ale také oblast, která může být zneužita. Internet je však jen jednou z vrstev a komponent kyberprostoru. Jednoduchost zařízení dnes umožňuje připojení k celosvětové síti téměř každému. Jakmile však má jedinec přístup a kapacitu, může prostřednictvím internetu provádět i cílené útoky kyberprostorem do fyzické složky světa.[3] Problematika kyberprostoru není však pouze otázkou právní, jedná se o technický obor a termín. Z pohledu technického laika se jedná o těžko uchopitelný, abstraktní pojem. Z právního hlediska je ale mnohé co zkoumat nejen na kyberprostoru, ale primárně na jednání v něm a skrze něj. Ačkoliv se jedná o prostor, který byl uměle vytvořen,[4] zatím nebyl řádně uchopen jako téma normotvůrci, kteří sice pro účely národních potřeb a zájmů přijali již řadu norem, ty však mají pramálo dočinění s přeshraničními prvky na úrovni mezinárodního práva veřejného. V mezinárodním právu nám stále jistota chybí. Dnešní doba je tak svědkem nárůstu kybernetické kriminality[5] a útoků, které míří na kritickou infrastrukturu[6], jejíž vyřazení může značně ohrozit chod států.

Od roku 2007 uplynulo již mnoho let, ale kybernetický útok na Estonsko,[7] který dokázal vyřadit celý státní aparát pořád rezonuje mezi státy,[8] které se rozhodují pro digitalizaci své

[1] Winston Churchill, Dolní sněmovna parlamentu Spojeného království dne 4. června 1940.
[2] Simon Kemp, „DIGITAL 2020: 3.8 BILLION PEOPLE USE SOCIAL MEDIA", 30. leden 2020, https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media.
[3] Todd G. Shipley, *Investigating internet crimes : an introduction to solving crimes in cyberspace.* (Waltham: Syngress, 2014). str. 1.
[4] Jennifer Bussel, „Cyberspace", in *Britannica*, 2. květen 2021, https://www.britannica.com/topic/cyberspace.
[5] Dan L. Dodson, „Cybercrime on the rise: Plotting a way forward", Security Magazine, 5. únor 2021, https://www.securitymagazine.com/articles/94527-cybercrime-on-the-rise-plotting-a-way-forward.
[6] Zákona č. 240/2000 Sb., o krizovém řízení.
[7] Stephen Herzog, „Revisiting the Estonian Cyber Attacks : Digital Threats and Multinational Responses", *Journal of Strategic Security* 4, č. 2 (ervenec 2011): 49–60. str. 50.

veřejné sféry. Vývoj využívání a také zneužívání kyberprostoru můžeme sledovat v čase, kdy nejprve dochází pouze k jednoduchým útokům pomocí DDoS (Distributed Denial of Service). Později jsou již sledovány vlastní zájmy, jako v případě Stuxnet. Tyto útoky mají za následek majetkové škody, v některých případech mohou přímo i nepřímo ohrozit lidské životy. Je dobré připomenout, že Estonsko nebylo samo v přímém ozbrojeném konfliktu s žádnou zemí, pouze se účastnilo misí NATO (War on Terror[9]), jednalo se tedy o útok v době míru.

Pro kyberprostor je specifická také jeho anonymita,[10] se kterou se také pojí možnost být kýmkoliv,[11] nemožnost dostatečně přičíst kriminální odpovědnost jedinci, natož provést dalekosáhle vyšetřování ve smyslu jednotlivých států, které jsou z útoků podezřívány a přiznat tak odpovědnost státu dle Článků o odpovědnosti států.[12] V dnešní době může člověk sledovat řadu kybernetických útoků, ať se již jedná o útoky na nemocnice,[13] vládní úřady,[14] či, jak již bylo zmíněno, celé digitální sítě.[15] Často se můžeme také setkávat s kyberútoky slabší povahy, které můžeme spíše identifikovat jako vměšování se do vnitřních záležitostí státu než analogii k použití síly. Následky těchto kyberútoků se liší, jedná se např. o únik dat, špionáž, nebo škodu na majetku. Kyberprostor a problémy, které z jeho existence vycházejí, existují již od 80. let 20. století, i přesto dnes nenacházíme mezinárodní úmluvu, jasně identifikované obyčejové právo či rozsudky mezinárodních soudů, které by otázku aplikace práva na tuto doménu komplexně konkretizovaly a určily jasné podmínky hry.

Tohoto právního vakua se chopila skupina expertů na pozvání CCDCE.[16] Výsledkem byl vznik Tallinnského manuálu,[17] počin řady expertů, který se snaží věcně a vyčerpávajícím způsobem argumentovat o možnosti aplikace Charty OSN na kyberprostor. Doktrína

---

[8] Hannes Grassegger a Mikael Krogerus, „Fake news and botnets: how Russia weaponised the web", The Guardian, 2. prosinec 2017, https://www.theguardian.com/technology/2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia.

[9] Renée de Nevers, „NATO's International Security Role in the Terrorist Era", *International Security* 31, č. 4 (2007): 34–66. str. 36.

[10] Stephen J Lukasik, „Protecting the global information commons", *Telecommunications Policy* 24, č. 6 (1. leden 2000): 519–31. str. 525.

[11] Alzbeta Krausova, „Identification in Cyberspace", *Masaryk University Journal of Law and Technology* 2, č. 1 (2008): 83–96. str. 84.

[12] Komise pro mezinárodní právo, „Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries" (Yearbook of the International Law Commission, 2001, vol. II, Part Two, 12. prosinec 2001).

[13] ČTK, „Kyberútok na nemocnici v Benešově způsobil škodu přes 59 milionů. Pachatele se vypátrat nepodařilo", 9. prosinec 2020, https://www.irozhlas.cz/zpravy-domov/kyberutok-kyberneticky-utok-nemocnice-v-benesove-skoda-pachatel-hacker_2008180912_ako. [přístup 18.4.2021].

[14] Deutsche Welle, „Coronavirus: Cyberattack blamed for delay in Germany's health data", 28. říjen 2020, https://p.dw.com/p/3kXzz. [přístup 18.4.2021].

[15] Viz poznámka č. 6.

[16] Cooperative Cyber Defence Centre of Excellence (česky: Centrum spolupráce pro kybernetickou obranu NATO). Pozn. autora.

[17] Schmitt, Michael N. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press, 2013. doi:10.1017/CBO9781139169288.

charakterizuje použití mezinárodního práva v době míru a také aplikaci v době války či jiného ozbrojeného konfliktu na kyberprostor. Jedná se o nejbližší ucelené dílo, které tuto problematiku v současnosti řeší a které vzniklo mimo akademickou obec. I přes to se jedná pouze o střípek mozaiky, který odpovídá na některé palčivé otázky ohledně právní úpravy kyberprostoru. V roce 2017 vznikla nová, rozšířená verze, a to Tallinnský manuál 2.0,[18] který se více soustředí na kyberoperace a na kyberútoky (ty které naplňují definici použití síly). Tato verze přichází s úpravou „due diligence“,[19] která dává za povinnost státům vyvíjet obranu proti kyberútokům a kyberoperacím.

Řada kyberútoků nebyla nikdy vyřešena a viník se nenašel,[20] a pokud byl viník vypátrán, bylo to až o řadu let později,[21] nebo se sám doznal.[22]

S ohledem na výše řečené si tato práce klade za cíl potvrdit či vyvrátit hypotézu: „Stát může být odpovědný za porušení mezinárodního práva v kyberprostoru, s důrazem na oblast lidských práv a kolektivní bezpečnosti“. Přičemž se odpovědností rozumí odpovědnost státu za mezinárodně protiprávní jednání, tedy za porušení závazků vyplývajících z mezinárodního práva, ve smyslu angl. *responsibility*.

Tato práce je rozdělena do tří částí. První část se věnuje definování pojmu kyberprostor v právu, ale i mimo něj. Představuje jednotlivé teorie pojetí kyberprostoru spolu s terminologickým slovníkem pojmů z oblasti IT a kyberbezpečnosti.

Druhá část pak představuje odpovědnost státu za protiprávní jednání obecně, s jistým zaměřením na kyberprostor. V této části je představen především postup jednání států a jejich orgánů, společně s přičitatelností za protiprávní jednání skupin navázaných na stát.

Třetí část se pak dělí na další části, ve kterých jsou představeny vybrané oblasti mezinárodního práva, přičemž dochází k rozboru, zda je možné aplikovat mezinárodní právo na porušení norem těchto oblastí v kyberprostoru. Třetí část ve svém celku tvoří stěžejní část této práce. Mezi vybrané oblasti patří použití síly a obecně kolektivní bezpečnost a lidská práva. Tato část je rozdělena do podkapitol z důvodu, že mezinárodní právo je komplexní systém a k

[18] Schmitt, Michael N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd ed. Cambridge: Cambridge University Press, 2017. doi:10.1017/9781316822524.

[19] Ian Yuying Liu, „The due diligence doctrine under Tallinn Manual 2.0", *Computer Law & Security Review: The International Journal of Technology Law and Practice* 33, č. 3 (1. červen 2017): 390–95.

[20] „The 10 most mysterious cyber crimes: Worms, hacks, satellites attacks, DNS spoofs and more unsolved computing crimes", Security InfoWatch, 26. září 2008, https://www.securityinfowatch.com/cybersecurity/information-security/article/10545883/the-10-most-mysterious-cyber-crimes.

[21] „Man Receives Maximum Sentence for DDoS Attack on Legal News Aggregator", 11. červen 2020, https://www.justice.gov/usao-ndtx/pr/man-receives-maximum-sentence-ddos-attack-legal-news-aggregator.

[22] Robert Coalson, „Behind The Estonia Cyberattacks", RFERL, 6. březen 2009, https://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html.

porušení norem může dojít v různých oblastech. Tato práce tak představuje výběr, který čtenáři dokáže nastínit v praktickém ohledu problematiku odpovědnosti států v kyberprostoru.

Tato práce vychází převážně z doktrinální práce různých autorů. V rámci analýzy dochází i k rozboru stávajících primárních pramenů, mezi které patří Charta OSN a platné mezinárodní smlouvy, ale také jednotlivé národní zákony. Práce pracuje i s analogií a komparací, a to v případě analýzy judikatury jednotlivých soudů. Pomocí dedukce jsou z těchto zdrojů vytvořeny závěry, o možnosti aplikace stávajících pravidel na kyberprostor. Judikatura byla využita z celé řady soudů, nejčastěji se objevují rozsudky Mezinárodního soudního dvora, Evropského soudu pro lidská práva, Mezinárodního trestního tribunálu pro bývalou Jugoslávii aj. K vypracování této práce posloužila řada sekundárních pramenů, jak elektronických, tak tištěných. Tato práce pracuje převážně s okolnostmi v době míru.

1. Pochopení kyberprostoru

Tato část představuje pojmy z prostředí informačních technologií. Jedná se o nejčastější způsoby, kterými dochází ke kyberoperacím či kyberútokům. Tato kapitola obsahuje také jednotlivé stručné vysvětlení pojmů, které se striktně váží k problematice kyberprostoru. Nejedná se o vyčerpávající výčet,[23] ale tento slovník slouží účelu této diplomové práce. Jak bude ilustrováno v následujících částech, k útokům stále dochází a nikdy to není stejným způsobem, jelikož útočníci svou strategii neustále upravují. V novinových článcích se často objevuje, že útok byl proveden např. DDoS. Jedná se však jen o jeden z možných způsobů, který je často viditelný jen proto, že přestane fungovat určitá webová stránka.

Kyberprostor

Medium, nosič dat, jehož vrstvy se skládají z fyzické, syntaktické, sémantické a pragmatické složky, kdy ta fyzická a pragmatická podléhá jurisdikci a kontrole některých svrchovaných států. Součástí kyberprostoru jsou i data, vytvořená, nebo měněná počítačem. Komunikací mezi jednotlivými fyzickými prvky lze dosáhnout k jinému zařízení, kdy fyzická a personální složka spolu musejí komunikovat a může tak dojít k změně, nebo výměně dat mezi jednotlivými zařízeními.

Součástí kyberprostoru je i fyzická složka, jedná se o zařízení různého typu, která mohou být součástí kritické infrastruktury státu, jako jsou nemocnice, elektrárny.[24]

Kyberoperace

Podle obecné označení dle manuálu z Oslo[25] se kyberoperacemi rozumí operace, které míří na dosažení cílů v kyberprostoru nebo skrze něj. Jedná se například o neoprávněný přístup k počítačům, měnění nebo mazání dat a další.

Kyberútoky

Kyberútoky lze rozumět ty operace, které vyústí v destrukci fyzické infrastruktury. Mají tedy dopad stejně jako kinetický, konvenční útok. Jedná se o „násilné“ operace v kyberprostoru. Je tedy možné pojem podřadit útoky podle práva ozbrojených konfliktů.[26]

---

[23] Je patrné, že dochází ke každoročnímu vývoji nových druhů virů a malware, není proto smyslem ani cílem této práce obsáhnout všechny. „Malware trends 2017", GData, 4. říjen 2017, https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017.

[24] Viz další kapitola.

[25] Yoram Dinstein a Arne Willy Dahl, *Oslo Manual on Select Topics of the Law of Armed Conflict : Rules and Commentary* (Springer Nature, 2020), https://doi.org/10.1007/978-3-030-39169-0.

[26] Veronika Bílková, *Mezinárodní humanitární právo : vznik, vývoj a nové výzvy.*, Studie z lidských práv Studies in human rights: č. 9 = vol. 9 (Praha: Univerzita Karlova v Praze, Právnická fakulta, 2015). str. 159.

Hromadné sledování

Hromadným sledováním se rozumí získání obsahu komunikace, a to elektronickým, mechanickým nebo jiným sledovacím zařízením. Tato data se mohou být přesouvána pomocí radiové nebo jiné elektronické komunikace.[27] Nejedná se o přímé sledování, ale slouží primárně k prevenci terorismu a záchytu nebezpečných komunikací. Vyhledáváním a filtrováním dat zpráv, například emailových adres, dojde ke sběru těchto dat, která jsou dále tříděna a mohou být v konečné fázi analyzována člověkem. Hromadné sledování může mít mnoho podob.

IP adresa

IP adresa představuje unikátní číselnou kombinaci, kterou přidělují regionální organizace, sdružené pod organizací ICANN (Internet Corporation for Assigned Names and Numbers). Tato organizace se stará o dohlížení nad počtem a správou přidělených IP adres. IP adresa se skládá z bitového zápisu adresy sítě, podsítě a síťového rozhraní. Momentálně je ve světě rozšířen formát IPv4, který dovolí identifikaci pouze omezeného množství zařízení (adresa je zapisována ve zjednodušené formě). Každé zařízení, které se připojí k internetu tak činí pod svou unikátní číselnou kombinací, veškeré pakety (data), které toto zařízení odesílá a vytváří, mají pak v sobě obsaženou tuto IP adresu. Tím může dojít k relativně přesné zeměpisné identifikaci zařízení. Mimo to rozlišujeme IP adresy veřejné a neveřejné, kdy veřejné jsou snadněji zjistitelné pro ostatní uživatele internetu. Neveřejné IP adresy jsou nejčastější, poskytují je poskytovatelé internetu. IP adresy nejsou přímo zjistitelné a zachovávají částečnou anonymitu. Pro účely této práce je podstatné, že se jedná o unikátní identifikátor zařízení na internetu.[28]

Pakety

Přenos dat po internetu funguje pomocí tzv. paketů (packetů). Princip je takový, že veškerá data jsou zaslána do cíle postupně, v menších snáz přenositelných balíčcích. Důvodem je složitost posílaných dat. Všechny pakety pak do cíle dorazí v určitém pořadí, které dovolí následné složení celé zasílané zprávy. Pakety v sobě nesou údaje o IP adrese.[29]

[27] „50 U.S. Code § 1801 - Definitions ‚electronic surveillance´", viděno 12. červen 2021, https://www.law.cornell.edu/uscode/text/50/1801.

[28] „IP adresa", WIKISOFIA, viděno 7. červen 2021, https://wikisofia.cz/wiki/IP_adresa#cite_note-3.

[29] „What is a packet? | Network packet definition", Cloudflare, viděno 7. červen 2021, https://www.cloudflare.com/learning/network-layer/what-is-a-packet/.

Strojové učení

Automatické zlepšování zařízení nebo programů na základě zkušeností, které toto zařízení nebo program získají během svého fungování. Jedná se o učení nikoliv v obecné rovině, ale z příkladů, z pokynů aj.[30]

Umělá inteligence

Sestavování inteligentních zařízení a programů, které dovolí samostatné rozhodování a řešení určitých problémů. K tomuto nabírá umělá inteligence vědomosti na základě obecných přístupů. Jedná se o přístup programu, který dovolí komunikaci s uživatelem a dokáže se učit a vykonávat složitější úlohy nezávisle na zadání a pokynech.[31]

Malware

Spojením anglických slov malicious (zlomyslný) a software (program) vzniklo slovo malware. Jedná se o slovo nadřazené následujícím pojmům. Nelze jej však zaměnit se špatně fungujícím programem. Jedná se o program cíleně vytvoření k tomu, aby škodil. Kdykoliv bude v této práci odkazováno na malware, je tím myšlen jeden nebo více z následujících pojmů.[32]

DDoS

Distributed Denial of Service. Využití způsobu těchto útoků je stále populární pro jednoduchost v proveditelnosti. DDoS útok probíhá tak, že je vytvořena síť zařízení, která jsou řízena hlavním zařízením. V tomto souhrnu vystupují tři úrovně. Master, Handler, Agent. Tato síť zařízení je pak řízena na dálku. Agenti mohou být různého typu. Často v minulosti byl *modus operandi* takový, že Agenty tvořily převážně tzv. Zombies. Tyto zombies pak jsou sekundárními oběťmi daného útoku, protože se jedná zařízení, přes která k útoku dochází a dochází tak k převzetí zařízení jiné osoby. Dále těmito Agenty mohou být Bots. Bot je počítačový autonomní program, který může komunikovat s ostatními zařízeními v kyberprostoru. Tyto dohromady tvoří tzv. botnet. Čím více existuje Agentů, tím větší efekt má daný útok. Handler je poté „unesené" zařízení, skrz které komunikuje Master s Agenty, a to pomocí dalších programů.[33] Průběh daného útoku však není náhodný. Dochází převážně k vyhledávání zranitelných zařízení. V nejčastějších případech se jedná o strategické webové stránky, vládní programy pro účely Denial of Service (odepření služby). Klasifikace DDoS útoků je různá a je možné definovat

[30] Kristian Kersting, „Machine Learning and Artificial Intelligence: Two Fellow Travelers on the Quest for Intelligent Behavior in Machines", *Frontiers in Big Data* 1 (2018): 6, https://doi.org/10.3389/fdata.2018.00006.

[31] Kersting.

[32] Priyanka Nandal, *Malware Detection* (Hamburg: Anchor Academic Publishing, 2018). str.7.

[33] Rashmi V. Deshmukh a Kailas K. Devadkar, „Understanding DDoS Attack & its Effect in Cloud Environment", *Procedia Computer Science* 49 (1. leden 2015): str. 204.

Vyčerpání šířky pásma (Bandwith Depletion) při kterém dojde k zabránění toku dat do zařízení oběti, jedním z těchto útoků je také zaplavení. Jedná se tedy o vytvoření řady podnětů pro cílové zařízení, web, server nebo cloud, které vede k nedostupnosti této služby. V dnešní době již existují nástroje, které při přípravě k danému útoku mohou pomoci.[34] Je tak mnohem jednodušší vytvářet takovéto programy.

Ransomware

Tento typ malwaru slouží k zablokování přístupu k datům uloženým na zařízení. Tento program zašifruje data a jak název napovídá, požaduje výkupné.[35]

Worms – např. Stuxnet

Většinu červů můžeme znát jako nejčastější viry, které náš antivirus odstraní. Jedná se o počítačový program, který se dokáže „množit" a šířit kopie sebe sama[36] na připojená zařízení, a to buďto přes připojení síťové (LAN) nebo internet. Červ nemá omezení, může se množit donekonečna. Jakmile je tento červ v počítači vyloží svůj náklad (Payload). Ačkoliv počítačový červ nemá nutně fatální následky, jedná se o další způsob, jak zneškodnit cílené zařízení a potenciálně ohrozit velké množství uživatelů. Může dojít ke zpomalení systému, nebo smazání dat. V současné době se červi používají například tak, že když se tento program dostane k zařízení oběti, zašifruje její soubory a požaduje výkupné. Viry se tedy šíří primárně tak, že si je uživatel sám stáhne nebo jim dá prostor se do zařízení dostat. K jeho aktivaci může dojít za pomoci lidského přičinění založeného na určité aktivitě, nebo se může aktivovat sám. K šíření pak dochází z adresy napadeného uživatele, aby vir dostal na důvěryhodnosti. Stuxnet je označení jednoho z počítačových červů. Tento červ vešel v povědomost kvůli útoku na Íránský jaderný program. Jednalo se však o trochu jiný druh červa. Tento byl přímo naprogramován, aby byl spící do doby, než se dostane do cíle.[37] Červi obecně mohou, pokud jsou k tomu naprogramováni, napáchat značné škody, vyřadit celé systémy z provozu, zablokovat přístup k zařízení přetížením jeho toku dat nebo mohou být určeny i ke špionáži. K napáchání hlavní škody slouží tzv. náklad (Payload). Tento náklad může zpřístupnit zařízení k dálkovému přístupu.[38]

---

[34] Steve Mansfield-Devine, „DDoS goes mainstream: how headline-grabbing attacks could make this threat an organisation's biggest nightmare", *Network Security* 2016, č. 11 (1. listopad 2016): str. 12.
[35] Nandal, *Malware Detection*.str. 19.
[36] Michael Erbschloe, *Trojans, Worms, and Spyware : A Computer Security Professional's Guide to Malicious Code* (Amsterdam: Butterworth-Heinemann, 2005). str. 23.
[37] Dorothy E. Denning, „Stuxnet: What Has Changed?", *Future Internet* 4, č. 3 (ervenec 2012): 672–87, https://doi.org/10.3390/fi4030672. **str.** 672.
[38] Priyanka Nandal, *Malware Detection* (Hamburg: Anchor Academic Publishing, 2018). str. 12.

1.1.Kyberprostor

Ačkoliv si kyberprostor představovali již mnozí autoři science fiction v 80. letech 20. století,[39] fakticky došlo k jeho skutečnému naplnění až vznikem celosvětové počítačové sítě, internetu.[40] Hlavním středobodem této diplomové práce je právě kyberprostor a zejména jeho povaha v mezinárodním právu. Experti, mezinárodní organizace a další mezinárodní aktéři se snaží právně uchopit tento pojem a definovat[41] jej tak, aby bylo možné na něj použít již existující normy, nebo vytvořit nové normy mezinárodního práva, které by se aplikovaly na tuto relativně novou oblast. Když použijeme analogii, kyberprostor můžeme chápat jako nově vzniklý, uměle vytvořený prostor, a dále postupovat analogicky například ve spojení s právní úpravou vesmíru, moře, nebo Antarktidy.[42] Toto rozdělení naznačuje určitá specifika kyberprostoru. Je důležité si pojem kyberprostor správně pojmenovat již jen s ohledem na to, že byl vytvořen uměle, na rozdíl od výše zmíněných ostatních prostor.

V této části jsou představeny jednotlivé vybrané definice kyberprostoru tak, jak kyberprostor popisují z faktického hlediska nebo definice, které používají některé státy ve svých vojenských příručkách, nebo národních právních předpisech. Dále dochází k představení jednotlivých událostí spojených s kyberútoky. Primárně se jedná o kyberútok na Estonsko, Stuxnet, ale také například o kyberútok na Gruzii.

1.2. Právní definice

Problematika určení jednotné, mezinárodně platné definice kyberprostoru se odráží i na faktu, že v dnešní době se vyskytuje mnoho definic v různých právních řádech a s různou právní silou, které v celku nepřináší pevný právní základ. Někteří akademici se zabývají možností, že kyberprostor není pouze jen oblast, nad kterou může některý ze subjektů mezinárodního práva vykonávat suverenitu efektivně, ale považují ji za novou „oblast“, doménu, popřípadě oblast podobnou režimu moří.[43]

Jak bylo zmíněno již v úvodu, skupina expertů, kteří vypracovali Tallinnský manuál, definují kyberprostor takto: „*Prostředí tvořené z hmotných a nehmotných komponentů, charakterizováno používáním počítačů a elektromagnetického spektra k ukládání, upravování a*

[39] William Gibson, *Neuromancer.*, 28th print. (New York: Ace Books, 1984).
[40] Mark Pesce, „A brief history of cyberspace", viděno 2. květen 2021, https://www2.cs.duke.edu/courses/spring01/cps049s/class/html/mp.history.html.
[41] Nadia Diakun-Thibault, „Defining Cybersecurity", *Technology Innovation Management Review*, 10 2014.
[42] Jan Ondřej, *Právní režimy mořských oblastí : srovnání s kosmem a Antarktidou.*, Monografie (Praha: Vydavatelství a nakladatelství Aleš Čeněk, 2017), str. 55; str. 23; str. 150.
[43] William M. Stahl, „The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity", *Georgia Journal of International and Comparative Law*, č. 40 (2011): 247–74. str. 267.

směně dat za použití počítačových sítí“.[44] V této definici se daty rozumí „*základní složka, která může být zpracována a/nebo vyprodukována pomocí počítače*“.[45] Ačkoliv Tallinnský manuál není závazným pramenem práva, spíše jen prací skupiny expertů, lze tuto definici bez problémů používat v rámci všech pravidel stanovených v tomto manuálu. Je pouze otázkou, zda se z Tallinnského manuálu postupem času nestane závazný pramen, tj. např. zda se jeho pravidla stanou obyčejovým právem v oblasti použití síly v kyberprostoru, jako tomu bylo například u manuálu ze San Remo.[46] Doktrína je jedním ze zdrojů mezinárodního práva, ale o pramen sekundární.

Mezinárodní organizace se obecně snaží vyhnout publikaci závazné definice, v doktríně však můžeme sledovat rozdělení na dva hlavní proudy názorů na to, co je to kyberprostor. Spíše, než praktickým definováním se tyto organizace zabývají aplikací mezinárodního práva a tím, jak se proti nežádoucímu chování v kyberprostoru bránit. NATO například přikládá kyberprostoru váhu nového prostoru, staví ho vedle vzduchu a zemi,[47] tato definice však vychází spíše z praktického hlediska pro použití k účelům organizace, stejně jako například definice z veřejně přístupné vojenské příručky americké armády: „*Kyberprostor je globální doménou, která je součástí informačního prostředí, skládající se z provázaných sítí informačních zařízení a dat, které obsahují internet, telekomunikační sítě, počítačové systémy a zabudované procesory a ovladače*“.[48] Tato dvě pojetí lze shrnout jako definice pro vojenské účely. Jedná se o široké definice, které poté dovolují státům jednodušší orientaci a „bojeschopnost“. Pro fungování vojenských organizací a bojeschopnost států je důležité, aby tito aktéři měli pevně daná pravidla. Praktickým úskalím je však fakt, že např. posledně zmíněná definice pochází z vojenského manuálu, který stanovuje postupy USA v případě kybernetických útoků. Vnitřní limitace však určitě není cílem, kam by právo kyberprostoru mělo směřovat.

OSN, přesněji UNIDIR,[49] pracuje se složitější, konkretizující definicí. „*Dnes se tyto sítě, technologie a jejich systémy doručování stále více označují jako „kyberprostor“, tento technologický substrát moderní společnosti, který se skládá z několika propojených vrstev – fyzické, syntaktické, sémantické a pragmatické – kdy fyzická a pragmatická podléhá jurisdikci a*

[44] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013). str. 258.
[45] Ibidem.
[46] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: OUP Oxford, 2014). p. 32.
[47] „…and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea.“ („Cyber defence", NATO, 12. duben 2021, https://www.nato.int/cps/en/natohq/topics_78170.htm.).
[48] Department of the Army, „FM 3-12, Cyberspace and Electronic Warfare Operations" (Army Publishin Directorate, 2017). str. 98.
[49] „*United Nations Institute for Disarmament Research*“.

kontrole některých svrchovaných států. Ohraničen používáním elektronického a elektromagnetického spektra, kyberprostor umožňuje vytvoření, skladování, modifikaci, výměnu, zneužití informací skrze nezávislé a propojené sítě za použití informačních komunikačních technologií".[50]

Postup NATO se pak převážně soustředí na ochranu před kyberkriminalitou a bezpečnost. Ochranu před kyberkriminalitou můžeme spatřovat jak v právu Evropské unie,[51] tak i v národních předpisech. Tyto právní předpisy se soustředí výlučně na trestní odpovědnost, nelze tedy brát v potaz odpovědnost států a již vůbec ne odpovědnost za spáchání mezinárodního zločinu. Český zákon o elektronických komunikacích č. 181/2014 Sb. definuje kyberprostor jako „*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací*". Tato definice je pak užita pro účely trestního zákoníku České republiky v oblasti počítačové kriminality. Dále pak nalezneme mezinárodní úmluvu z pera Rady Evropy, o počítačové kriminalitě.[52] Tato úmluva však nepoužívá spojení „kyberprostor", ale pracuje s pojmy „počítačový systém" a „počítačová data". Počítačovým systémem se pak rozumí jakékoliv zařízení nebo skupina propojených nebo na sebe navazujících zařízení, kde alespoň jedno zařízení provádí automatické zpracování dat na základě svého programování.[53]

Definice můžeme najít v řadě právních řádů, na různých úrovních a pro různé účely. Z definic je však patrné určité propojení. Je patrné, že kyberprostor není definován jen zařízením, ze kterého jedinec komunikuje s ostatními zařízeními. Jedná se o propojený systém, digitální prostředí, který se skládá z vrstev. V tomto prostředí lze vytvářet, měnit, skladovat a vyměňovat data. Součástí kyberprostoru je i internet.

[50] UNIDIR, The United Nations, *Cyberspace and International Peace and Security* (UNIDIR resources, UN) str. 1. „Today, these networks, technologies, and their delivery systems are increasingly referred to as "cyberspace", the technological substrate of modern societies made up of several interconnected layers—physical, syntactic, semantic, and pragmatic, with the physical and pragmatic layers subject to certain sovereign governmental jurisdiction and controls. Framed by the use of electronics and the electromagnetic spectrum, cyberspace enables "the creation, storage, modification, exchange and exploitation of information via interdependent and interconnected networks using information communication technologies".

[51] 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).

[52] Council of Europe, ETS 185 *Convention on Cybercrime*, Budapest, 23.11.2001.

[53] Ibidem. čl. 1.

1.3. Teoretické přístupy

Dva teoretické přístupy k využití, nebo identifikaci kyberprostoru se dají nazvat jako „Effects principle“ a Společné dědictví lidstva (dále jen „SDL“).[54]

První zmíněný přístup mluví o suverenitě, nebo dokonce teritoriální integritě,[55] která se však nedá přímo aplikovat na kyberprostor. Tento princip by, brán doslovně, měl praktické dopady, když by došlo ke sporům ohledně vlastnictví a rozsahu jurisdikce nad kyberprostorem. Tento přístup stále počítá s výkonem teritoriality nad kyberprostorem.[56] Z toho pojetí je pak možné si obhájit národní úpravu chování, zřizování a přístupu ke kyberprostoru. V mezinárodním právu je však již všeobecně uznáváno, že je možné regulovat ty aktivity, které mají dopad na svrchované území státu. Tato teorie zastává názor, že i oblasti, nad kterými stát nemá jurisdikci, může podrobit svým právním řádům. Je pak už jedno na základě, jakého parametru tak učiní, jestli upraví chování a jednání osob, nebo vyloženě podřídí chování jednotlivců například přes státní domény (.cz). Pod tuto teorii se dají zařadit všechny definice zmíněné v předchozí části.

Kyberprostor je do určité míry neovladatelný prostor, ve kterém nelze určit stejná pravidla, jako je tomu například na územích pod tradiční jurisdikcí států. Proto dochází k argumentaci mnoha expertů, že kyberprostor je opravdu tzv. pátou doménou (vojenskou oblastí) a takto by se s ním mělo zacházet. Přístup, který toto pojetí favorizuje, spočívá v považování kyberprostoru za Společné dědictví lidstva (SDL).[57]Jedná se o oblasti, které je hodno zachovat pro budoucí generace. Tyto oblasti mohou něco poskytovat, ať je to rozmanitá flora či fauna, voda, nebo obdobné zdroje. Právní úprava těchto oblastí mezinárodní aktéry nejen omezuje, ale dává jim i určitá práva nakládat s tímto dědictvím. Všechny státy by měly profitovat z těchto prostorů a ty by a měly sloužit výlučně k mírovým účelům. Tímto účelem by podle maltského představitele měl být volný přístup k informacím.[58] Tuto úpravu můžeme najít v momentální mezinárodní úpravě např. vesmíru,[59] moře,[60] Antarktidy.[61] Jednotlivé charakteristiky těchto SDL se pak dají koncentrovat do pěti podmínek. Neexistuje soukromé

[54] Scott J. Shackelford, „From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law* 27, č. 1 (2009): 192–252., str. 211.
[55] Shackelford.
[56] Shackelford. str. 211.
[57] Ondřej, *Právní režimy mořských oblastí : srovnání s kosmem a Antarktidou.* str. 90
[58] Jean Buttigieg, „The Common Heritage of Mankind : From the Law of the Sea to the Human Genome and Cyberspace", 2012, https://www.um.edu.mt/library/oar/handle/123456789/6883. str. 90.
[59] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 610 U.N.T.S. 205, entered into force, Oct. 10, 1967.
[60] 1982 United Nations Convention on the Law of the Sea, 1833 UNTS 397, 21 ILM 1261 (1982).
[61] The Antarctic Treaty, 402 U.N.T.S. 71, *entered into force* June 23, 1961.

přivlastnění a vlastnictví těchto prostorů.[62] Všichni zúčastnění se musejí podílet na správě zdrojů těchto prostorů. Všechny státy musejí sdílet výhody z těchto prostorů. Není možné umístit zbraní, nebo vojenské instalace. A v neposlední řadě, mají být tyto prostory zachovány pro výhody budoucích generací lidstva.[63] Možnost pohybu a manévrů armády je možná s tím, že tyto prostory/domény mohou být mezi sebou propojeny počátkem a následkem.[64]

Dalším argumentem v teorii a určení kyberprostoru pro potřeby mezinárodního práva je, že kyberprostor je pouze sférou traversiální, tedy teorie tzv. Cross-domain enabler. Tato teorie není nijak nová, jedná se například o situaci raket odpálených ze země, které míří na letadlo. Raketa je tedy vypálena z jedné domény (země) do druhé domény (vzduchu). Tato teorie tak vychází z přesvědčení, že útok mající svůj počátek v kyberprostoru má za cíl zaměřit se na zařízení/systémy, které se v kyberprostoru nenacházejí.[65] Z mezinárodně právního hlediska se jedná o sféru, která spojuje všechny ostatní „domény", SDL a jiné. Kyberprostor je pouze prostředek k dosažení určitých cílů.[66] V angličtině se kyberprostor považuje za Cross-domain enabler,[67] tedy prostředí, které umožňuje přecházení mezi jednotlivými doménami. Tato teorie vystupuje jako kritika předchozích teorií a boří představu o tom, že kyberprostor je ovladatelný. Z vícero právních názorů je patrné, že ovladatelná je pouze jedna složka, ta fyzická, kterou představují počítače a technika, případně podmořské kabely.

Ostatní složky, například přenos dat, je pouze přesouvání packetů po síti, které mají ale dopad ve skutečném světě. Pod tuto teorii by se dala podřadit definice stanovená v Tallinnském manuálu, ten totiž vyloženě nepočítá se zařízeními jako přímou součástí kyberprostoru. Teorie Cross-domain enabler může přinášet úskalí v tom, že obrana proti útokům v kyberprostoru se může projevit i jinde. To je možné uvést na již zmíněném příkladu rakety vyslané na letadlo. Obrana státu může být, pokud se jedná o mezinárodní ozbrojený konflikt, útok na jiný možný cíl. Tato teorie tedy jde dohromady s teorií Cross-domain detterence, podle které by pak měla odrazovat od použití kybernetických útoků možnost hrozby útoku konvenčního. V tomto případě by se nedal kyberprostor definovat tak, aby mohl obsáhnout všechny hmotné i nehmotné složky. Jednalo by se pouze o tento prostor, který je vytvořen propojením jednotlivých zařízení. Dalším argumentem, který by vylučoval plošnou aplikaci této teorie je fakt, že například protiprávní jednání státu v oblasti lidských práv se odehrává celé v kyberprostoru. Tento teoretický přístup

[62] Shackelford, „From Nuclear War to Net War: Analogizing Cyber Attacks in International Law". str. 211.
[63] Shackelford., str. 212.
[64] Chris McGuffin a Paul Mitchell, „On Domains: Cyber and the Practice of Warfare", *International Journal* 69, č. 3 (2014): 394–412. str. 409.
[65] Vincent A. Manzo, „Deterrence and escalation in cross-domain operations : where do space and cyberspace fit?", Strategic forum, č. 272 (2011). str. 2.
[66] Daniel Ventre, *Cyber Conflict : Competing National Perspectives* (London: Wiley-ISTE, 2012). str. 234.
[67] McGuffin a Mitchell, „On Domains: Cyber and the Practice of Warfare"., str. 404.

by se mohl aplikovat na tato jednání, které nemají svůj počátek a následek v kyberprostoru, ale mimo něj.

Tato teorie dokazuje, že ačkoliv nelze vlastnit veškerý kyberprostor, nelze jej prohlásit za spadající celý pod něčí správou, nebo jurisdikci,[68] jak by tomu mohlo být v jiných případech.

1.1.1. Kritika

Kritika pojetí kyberprostoru podle „Effects principle" vychází z toho, že tento přístup slouží prostředku, tedy je ovlivněn politikou. Tato teorie stanovuje závěry, které jsou vítané pro většinu států, ale neposkytuje odpověď na povahu kyberprostoru. Nabízí přímo možnost úpravy a bez zbytečných vedlejších argumentů přichází s odpovědí, která favorizuje vojenskou oblast a teritoriální kontrolu státu. Tallinnský manuál v sobě také má tuto teorii zabudovanou, a to v pravidlech 1 a 2. Tato pravidla stanovují, nad kým může stát vykonávat svou moc, co se týče kyberprostoru. Je tedy stanoven okruh účastníků, nad kterými může stát vykonávat svou moc, i když se účastníci vyskytují kdekoli např. na palubách lodí pod statní vlajkou, nebo jejich kyber aktivita přes území státu pouze prochází.

Zastánci teorie o kyberprostoru jako SDL vidí podobnost mezi existujícími doménami a kyberprostorem. Jedná se o teorie spíše prezentované ve vojenském prostředí, a tedy argumenty podporující vojenskou angažovanost a zapojení v kyberprostoru. Z tohoto pohledu lze přijít s kritikou následující teorie propojenosti kyberprostoru s ostatními sférami. Dalším argumentem je pouhá podobnost kyberprostoru k ostatním prostorům. Jedná se však o nepřesnou analogii, z důvodu již patrného, že kyberprostor je uměle vytvořen a nelze jej plně ovládat a limitovat.

Ačkoliv se již v dnešní době dá hovořit o tom, že Severoatlantická aliance (dále jen „NATO"),[69] Organizace spojených národů[70] (dále jen „OSN") souhlasí, že kyberprostor není zemí nikoho a mezinárodní právo se zde aplikuje, existuje stále mnoho nejasností. Například z komuniké ze summitu ve Varšavě[71] zjistíme, že kyberprostor je také považován za vojenskou oblast, tedy prostor, kde lze s limitací vykonávat vojenské akce.[72] Dle názoru autora je jedním z hlavních problémů, a dá se říct nedostatků, neexistence jednotné definice kyberprostoru v mezinárodním právu. Toto můžeme spatřovat v definicích jednotlivých mezinárodních

[68] Johnson, David R., and David Post. "Law and Borders: The Rise of Law in Cyberspace." Stanford Law Review 48, no. 5 (1996): 1380.
[69] „Cyber defence"., jako speciální úloha NATO při kolektivní obraně.
[70] Cyrus Jabbari, „The Application of International Law in Cyberspace: State of Play", United Nations, 10 2018, https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/.
[71] „Warsaw Summit Communiqué: issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016" (Press Release (2016) 100, 9. červenec 2016).
[72] Miroslav Potočný, *Mezinárodní právo veřejné : zvláštní část.*, 6., doplněné a rozšířené vydání, Právnické učebnice (Praha: C.H. Beck, 2011), str. 441.

organizací,[73] vojenských manuálů[74] a národních právních řádů.[75] I přes neexistenci jednotné definice ICRC tvrdí, že ať finální pojetí kyberprostoru bude jakékoliv, pořád platí omezení stanovená Chartou OSN a *ius in bello,*[76] s odkazem na to, že mezinárodní humanitární právo, se může aplikovat na kyberprostor, a to skrze ustanovení o nových typech a způsobech vedení války.[77]

Při definování kyberprostoru je stále hlavní otázkou jeho povaha. Dle mnohých názorů se může buďto jednat o „prostor", nebo „vojenskou oblast" ve smyslu mezinárodního práva, anebo médium, tedy nosič informací, a /nebo se jedná o *sui generis* oblast, kterou tak musí právo reflektovat. Jak bylo zmíněno, kyberprostor je převážně spojován s vojenskou činností, ale také se státní bezpečností a suverenitou.[78]

Tyto teoretické přístupy k regulaci kyberprostoru dle názoru autora značně ovlivňují jeho definování. Na jedné straně může být kyberprostor něco, co podléhá, ačkoliv nepřímo, jurisdikci jednotlivých států, tedy jakýsi nosič, nebo způsob komunikace. Může se také jednat o definování nového prostoru jako oblasti, kde suverenita a jurisdikce jednotlivých států neplatí, a tudíž by byla potřeba nové smluvní úpravy, státy by byly oprávněny pouze aplikovat svou moc nad osobami, které jednají v kyberprostoru. Stanovení definice tak, aby uspokojila zastánce teorie o novém prostoru, může vést k značné militarizaci kyberprostoru. Na druhou stranu stanovení definice kyberprostoru na základě efektivity může vést k politické diskusi a dalšímu odložení řešení palčivé otázky úpravy kyberprostoru na úrovni mezinárodního společenství.

Například v Tallinnském manuálu v pravidle č. 1, může mít čtenář pocit, že autoři jsou toho názoru, že suverenitu nad kyberprostorem není možné vykonávat. Jediné, nad čím stát může vykonávat suverenitu, jsou koncová zařízení a aktivity na území státu. Jedná se tedy spíše o Effects principle, který byl zmíněn výše. Kyberprostor není vnímán jako SDL.

Ani jedna z představených teorií však není dostatečná k pochopení toho, co vlastně kyberprostor je, co jsou jeho hlavní aspekty a jak je možné v něm určit konkrétní pravidla chování. Přístup do kyberprostoru je dán každému člověku, kterému jeho stát, či agentura přiřadí

[73] ICRC, „International Humanitarian Law and Cyber Operations during Armed Conflicts, position paper submitted to OEWG", 2019.
[74] Department of the Army, „FM 3-12, Cyberspace and Electronic Warfare Operations".
[75] Např. zákon o kybernetické bezpečnosti zmíněný výše.
[76] ICRC, „International Humanitarian Law and Cyber Operations during Armed Conflicts, position paper submitted to OEWG". str. 4.
[77] „Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)", 6 1977, 1125 U.N.T.S. 3.
[78] Pojem suverenita je v této práci chápán tak, jak byl stanoven v rozsudku Stálého rozhodčího soudu ze dne 4. dubna 1928, Las Palmas, USA v. Nizozemsko: „Suverenita ve vztahu mezi státy značí nezávislost. Nezávislost ve vztahu k části Země je právo zde vykonávat výlučné aktivity státu." Permanent Court of Arbitration, Island of Palmas Case (or Miangas), United States v Netherlands, Award, (1928) II RIAA 829, ICGJ 392 (PCA 1928), 4th April 1928.

IP adresu, a kdo má přístup k počítači či mobilnímu telefonu.[79] IP adresa je v množství případů dostatečným identifikátor pro vystopování jednotlivého zařízení, ale jedná se pouze o pseudo identifikaci. Tato identifikace tedy neslouží k určení pachatele, například pro použití v trestních věcech. IP adresa jednoduše označuje původ a destinaci dat, ve spolupráci s poskytovatelem internetu, přes jehož systém je zařízení připojeno k internetu. Takto může být identifikován jedinec, skupina, nebo alespoň stát původu.[80] Dnes již existuje řada způsobů, jak svou aktivitu maskovat.[81] Kyberprostor není něco, na co je možné automaticky vztáhnout stávající speciální úmluvy. Kyberprostor je kombinací hmotných prvků, které si může jednotlivec přivlastnit, ale hlavně prvků nehmotných, které nelze k nikomu přiřadit, pokud ten dotyčný nechce být vystopován. Pro užití v ozbrojených konfliktech je důležité si ujasnit, že obyčejové právo[82] se uplatní vždy, a pro signatáře Dodatkového protokolu 1 se uplatní i jeho článek 36 o použití nových zbraní, způsobů vedení války.

1.1.2. Technická definice

Z faktického hlediska je možné definovat kyberprostor jako „*virtuální počítačový svět, přesněji elektronické médium, které slouží k online komunikaci*“.[83] Již z této definice jsou pozorovatelné tři aspekty i) jedná se propojení počítačů/zařízení (fyzický prvek) ii) je potřeba lidský prvek (personální prvek)[84] a iii) jedná se o jeho používání v čase (logický prvek). Tato definice slouží pouze k představení skutečnosti, že kyberprostor není pouze internet.

[79] Jan-Frederik Kremer a Benedikt Müller, ed., *Cyberspace and international relations : theory, prospects and challenges.* (Berlin: Springer, 2014). str. 45.

[80] Ibid. 33.

[81] Například služby, které jsou poskytování tzv. VPN = virtuální privátní síť

[82] Jean-Marie Henckaerts, „Study on customary international humanitarian law: A contribution to the understanding and respect for the rule of law in armed confl ict", *International Review of the Red Cross* 87, č. 857 (březen 2005): 175–212. str. 176-179.

[83] „What Is Cyberspace? - Definition from Techopedia", Techopedia.com, viděno 28. duben 2021, http://www.techopedia.com/definition/2493/cyberspace.

[84] Nelze pominout fakt, že již existují autonomní zbraňové systémy. Tyto systémy se poněkud liší od konvenčních zbraní a autonomních zařízení hlavně v tom, že autonomní zbraňové systémy jsou vytvořeny, aby se sami rozhodovaly (přístup založený na pravidlu vs. Přístup založený na pravděpodobnosti). Striktně vzato, tyto zbraňové systémy nepotřebují k funkčnosti žádný lidský prvek (v daný okamžik). Fungují tedy nezávisle na tom, zda je někdo ovládá. Příkladem může být Izraelský „Iron Dome“ (viz „The Iron Dome Missile Defense System", viděno 14. duben 2021, https://www.jewishvirtuallibrary.org/the-iron-dome.“). Jedná se o mobilní, protiraketový obranný systém, který má za úkol zaměřit všechny rakety, které by měly za cíl obydlené oblasti Izraele. Z pohledu autora by tato technická definice byla pořád schopná obstát i v porovnání s těmito autonomními zbraněmi. Jedná se totiž v důsledku o počítačový program, který je sice schopný vlastního rozhodování, ale toto rozhodování je stanoveno lidským prvkem. Tyto autonomní zbraně se tedy budou řadit spíše do první skupiny zařízení. Autonomní zbraňové systémy budou častěji cílem kybernetických útoků, například by se mohlo jednat o nový vir typu Stuxnet, který by dokázal přeprogramovat tento systém. Druhou možností je vytvoření autonomního systému na ochranu kyberprostoru. V tomto případě, kdyby se jednalo o program, který by se šířil po kyberprostoru a dokázal by identifikovat hrozby, muselo by dojít k přehodnocení potřeby lidského prvku v definici. Tento scénář však spíš již připomíná umělou inteligenci a od autonomních zbraní by se značně odlišoval. (Expert Meeting, *Autonomous weapon systems: Technical, military, legal and humanitarian aspects* (Geneva: ICRC, 2014).

Kyberprostor existuje mezi zařízeními a jeho příkladem je i telefonní spojení, kdy se hovor ve skutečnosti neodehrává v daných zařízeních ale v „prostoru“, který zařízení spojuje a ve kterém se tyto osoby opravdu setkávají.[85] Pokud tak vycházíme z této definice, nemůžeme označit kyberprostor za něco úplně nového. Je však na místě zmínit, že problematika kyberprostoru je otázkou posledních pár desítek let z toho důvodu, že jej lze využívat novými způsoby.[86]

V dnešní době dochází k častým diskusím o umělé inteligenci a potenciálním problémům, které mohou nastat v případě porušení norem práva. Výše zmíněný Iron Dome (viz poznámka č. 80) může být v některých aspektech považován za umělou inteligenci, a to v rozeznávání, zda útok míří na civilní oblasti.[87] Dle některých autorů se za umělou inteligenci dají považovat zařízení, která se dokážou strojově učit.[88] V případě postupného vývoje a aplikace nových strojů, které se budou moci rozhodovat a učit a činit jednoduché úkony nezávisle na lidském prvku je velice pravděpodobné, že dosavadní teorie se stanou obsoletními. Diskuse bude na místě také v případech, kdy z tohoto celého cyklu vypadne lidský prvek, který nebude schopen ani na rozhodování stroje dohlížet, protože takovéto rozhodování bude v rozmezí několika mikrosekund. Pro účely této práce bude používán aktuální vývoj technologií s ohledem na to, že opravdová umělá inteligence ve všech ohledech ještě neexistuje.[89] Zároveň se jedná pouze o zmínku možného dalšího rozšíření tématu, které je však v současnosti nad rámec daný názvem této diplomové práce.

Kyberprostor je prostor, který se skládá ze všech počítačových sítí a všech elektronických zařízení, které jsou k těmto sítím připojeny. Tato definice znamená, že pokud se jedná i o flash disk, mobil, jakékoliv jiné zařízení, které se stane součástí této sítě, lze se skrze něj dostat k jiným zařízením, tedy do kyberprostoru. Kyberprostor je definován složitými procesy mezi výše zmíněnými třemi aspekty a skládá se z vrstev.

---

[85] Poznámka autora: ačkoliv se nejedná o akademickou publikaci, ale spíše o poskytnutí reálné situace o kyberkriminalitě na konci 20. století, tato kniha, v podobě „electronic commons“ poskytuje pro laickou veřejnost jednoduše pochopitelnou definici kyberprostoru :Bruce Sterling, *The Hacker Crackdown : Law and Disorder on the Electronic Frontier*, Project Gutenberg Etext (Champaign, Ill: Project Gutenberg, b.r.). http://www.gutenberg.org/files/101/101-h/101-h.htm.

[86] P. J. Blunt, „How Cyberspace Changes International Conflict", in *Reprogramming the World: Cyberspace and the Geography of Global Order*, Creative commons (E-International Relations, b.r.), https://www.e-ir.info/pdf/80610. str. 1.

[87] Jim Garamone, „Esper Sees Iron Dome Missile Defense System in Tel Aviv", US. Dept. of Defense, b.r., https://www.defense.gov/Explore/News/Article/Article/2400629/esper-sees-iron-dome-missile-defense-system-in-tel-aviv/.

[88] Mark Coeckelbergh, „Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability", *Science and Engineering Ethics* 26, č. 4 (1. srpen 2020): 2051–68, https://doi.org/10.1007/s11948-019-00146-8.

[89] Max Simkoff a Andy Mahdavi, „AI Doesn’t Actually Exist Yet", Scientific American, 11 2019, https://blogs.scientificamerican.com/observations/ai-doesnt-actually-exist-yet/.

Technická definice nám navazuje na dříve stanovený problém vlastní identifikace kyberprostoru a jeho vlastností. Jak je patrno z textu výše, tyto tři charakteristiky jsou často základem pro ostatní definice a vesměs se jimi prolínají.

1.4. Shrnutí

V této části byla nastíněna problematika kyberprostoru z právního hlediska a teoretické přístupy, které jsou dnes viditelné v akademickém diskursu. Pro účely této práce tak bude používaná definice, kterou stanovil Tallinnský manuál spolu s vypůjčením části pojmů z práce UNIDIR a teoretický přístup Effects principle. Argumentace vychází právě z této definice a tohoto teoretického přístupu.

Kyberprostor je tedy pro účely práce považován ve stejné definici, kterou užívá UNIDIR, za medium, nosič dat, jehož vrstvy se skládají z fyzické, syntaktické, sémantické a pragmatické složky, kdy fyzická a pragmatická podléhá jurisdikci a kontrole některých svrchovaných států. Součástí kyberprostoru jsou i data, vytvořená, nebo měněná počítačem. Komunikací mezi jednotlivými fyzickými prvky lze dosáhnout k jinému zařízení, kdy fyzická a personální složka spolu musejí komunikovat a může tak dojít k změně, nebo výměně dat mezi jednotlivými zařízeními.

Součástí kyberprostoru je i fyzická složka, jedná se o zařízení různého typu, která mohou být součástí kritické infrastruktury státu, jako jsou nemocnice, elektrárny. Může se také jednat o vojenské cíle pro účely práva ozbrojených konfliktů. Je třeba, aby právě tato součást kyberprostoru zůstala chráněna. Proto je žádoucí, aby byla otázka kyberprostoru vyřešena co nejdříve a byl představen jednotný postup mezinárodního společenství. S postupným nárůstem kyberútoků je potřeba, aby státy měly stanoveny alespoň právní rámec, ve kterém se mohou pohybovat.

2. Odpovědnost a přičitatelnost

Jak již bylo stanoveno v první části této práce, je nesporné, že mezinárodní právo se v jistém ohledu aplikuje i na kyberprostor. Toto je patrné jak z práce expertů, tak i z dalších okolností. Kromě Tallinnského manuálu došlo letos (2021) ke zveřejnění finální zprávy Open-ended Working Group, která vznikla na základě rozhodnutí valného shromáždění OSN 73/27[90] a která se zabývala bezpečnostním používáním informačních a komunikačních technologií. V této finální zprávě z 12. března 2021 státy ujišťují, že mezinárodní právo je možné použít a že je také základem pro zachování míru a stability a podpory otevřeného, bezpečného, přístupného a mírového prostředí informačních a komunikačních technologií.[91]

Klasické (vnitrostátní) chápání odpovědnosti určují dvě povinnosti, právně závazné pravidlo chování (primární povinnost) a nedodržení/porušení této povinnosti, které přináší negativní následek (sekundární povinnost).[92] V mezinárodním právu se však tento postup liší od běžných vnitrostátních přístupů, kdy odpovědnost je navázána buďto na občanskoprávní odpovědnost, nebo trestněprávní odpovědnost, které mohou vyústit v peněžitý trest, trestní stíhání a jiné.

V dnešní době je odpovědnost států stabilizovaná obyčejová norma. Odpovědnost (ve smyslu odpovědnosti za mezinárodně protiprávní jednání, angl. *responsibility*) nastává, když se stát dopustí jednání, konáním či opomenutím, které není v souladu s jeho právními závazky s tzv. primárními normami, je tedy protiprávní. Písemnou úpravu najdeme v dokumentu Články o odpovědnost státu za mezinárodně protiprávní jednání[93] (ARSIWA), které vypracovala Komise OSN pro mezinárodní právo.[94] Vývoj této normy byl dlouholetý a plánovaný již od 30. let minulého století. Své kodifikace se mezinárodněprávní odpovědnost dočkala až v roce 2001. Ačkoliv se nejedná o primární pramen práva byly ARSIWA vydány jako rezoluce OSN.[95]

[90] UN, General Assembly, „Resolution adopted by the General Assembly: Developments in the field of information and telecommunications in the context of international security A/RES/73/27", 11. prosinec 2018.

[91] General Assembly, „Open-ended working group on developments in the field of information telecommunications in the context of international security" (A/AC.290/2021/CRP.2, 10. březen 2021). odst. 34.

[92] Kimberley N. Trapp, „Terrorism and the international law of state responsibility", in *Research Handbook on International Law and Terrorism* (Cheltenham, UK: Edward Elgar Publishing, 2020), https://www.elgaronline.com/view/edcoll/9781788972215/9781788972215.00010.xml. str. 32.

[93] Komise pro mezinárodní právo, „Odpovědnost státu za mezinárodně protiprávní jednání" (Příloha k rezoluci Valného shromáždění 56/83 ve znění opravného dokumentu A/56/49(Vol. I)/Corr.4, 12. prosinec 2001).

[94] The International Law Commission was established by the General Assembly, in 1947, to undertake the mandate of the Assembly, under article 13 (1) (*a*) of the Charter of the United Nations to "initiate studies and make recommendations for the purpose of ... encouraging the progressive development of international law and its codification".

[95] UN, General Assembly, „Resolution adopted by the General Assembly: Responsibility of States for internationally wrongful acts A/RES/56/83", 28. leden 2002., UN, General Assembly, „Resolution adopted by the General Assembly: Responsibility of States for internationally wrongful acts A/RES/71/133", 19. prosinec 2016.

Důležitým aspektem této úpravy však je, že Mezinárodní soudní dvůr a jiné soudní instituce nahlížejí a citují[96] právě ARSIWA, kterým takto dodávají váhu. ARSIWA mají z velké části kodifikační povahu, tedy jedná se povětšinou o odraz mezinárodních obyčejových norem ucelených do jednoho dokumentu. Odpovědnost státu se pak skládá ze dvou důležitých aspektů, porušení normy jako takové a přičitatelnosti. Dále by se do této oblasti dala přiložit i část povinné prevence (due diligence) v mezinárodním právu.

Stěžejní princip je uveden hned v čl. 1: „*Každé mezinárodně protiprávní jednání státu zakládá mezinárodněprávní odpovědnost daného státu*“.[97]

2.1. Přičitatelnost

Dle čl. 2 ARSIWA se jedná o mezinárodně protiprávní jednání, pokud a) je toto jednání přičitatelné státu; b) toto jednání zakládá porušení mezinárodněprávní povinnosti státu.[98] Přičitatelnost jednání státu, jako subjektu mezinárodního práva je založeno na kritériích stanovených mezinárodním právem, a nikoliv na pouhé příčinné souvislosti a faktické kauzalitě.[99] To, že se určí jeden aspekt neznamená, že je daný stát odpovědný, proto musí být obě podmínky naplněny současně. S ohledem na to, že stát, jako organizovaná jednotka, má blíže v právu k právnickým osobám než k těm fyzickým, musí za stát vždy někdo jednat. Může se jednat o orgány státu, např. vlády, ale i jiné orgány, stejně tak i o jednotlivce, kterým stát svěřuje nějaké pravomoci atd. Státu tak může být nejen přičteno jednání jeho orgánu při výkonu vládní moci, ale také se může jednat o jednání, nad kterými má stát jako suverén dohled. Jedná se o případy, kdy o tomto jednání stát měl nebo musel vědět, ale nijak nereagoval.[100] Stěžejní principy přičitatelnosti státu jsou určeny v čl. 4–11. Tyto části postupně hovoří o orgánech státu *de iure*, *de facto* a o zvláštních případech přičitatelnosti.

2.1.1. Obecné principy přičitatelnosti – články 4-9

Orgány de iure

Pravidla přičitatelnosti najdeme v části druhé ARSIWA, dle čl. 4[101] je takové jednání státu přičitatelné, pokud orgán[102] vykonává legislativní, exekutivní, soudní nebo jinou činnost.

[96] Obligations Concerning Negotiations Relating To Cessation Of The Nuclear Arms Race And To Nuclear Disarmament (Marshall Islands V. United Kingdom) Preliminary Objections Judgment Of 5 October 2016.
[97] Komise pro mezinárodní právo, „Odpovědnost státu za mezinárodně protiprávní jednání". čl. 1.
[98] Komise pro mezinárodní právo. čl. 2.
[99] Komise pro mezinárodní právo, „Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries". str. 38.
[100] Viz Corfu Channel ICJ, „Corfu Channel Case (United Kingdom v. Albania); Assesment of Compensation" (15 XII 49, 15. prosinec 1949).
[101] Komise pro mezinárodní právo, „Odpovědnost státu za mezinárodně protiprávní jednání".
[102] V této části se orgánem rozumí organizační složka státu, úřad, ministerstvo a podobné organizace.

Může se jednat o jednání daného úřadu, nebo osoby, která zastává činnost v tomto úřadu nehledě na její zařazení v hierarchii moci. Stejně tak nezáleží, jestli se jedná o státní správu anebo jinou regionální správu (tedy i obecní, federální, konfederační a jinou).[103] Tyto orgány se dají nazvat jako orgány *de iure*. Tento článek bere v potaz všechny možné varianty, jak tradičních státních úprav, i těch netradičních, kde rozdělení státní moci není tripartitní. Je nutné podotknout, že jednání orgánu státu je v tomto případě státu přičitatelné, v případě, kdy tento orgán jedná v rámci své působnosti. O případech překročení pravomoci bude pojednáno níže. Nepůjde o případy, kdy úředník mimo službu na dovolené spáchá přestupek. Může se však jednat o nepřímou přičitatelnost státu, jak bylo naznačeno výše, jako v případu Korfského průlivu.[104] V některých rozhodnutích rozhodčího orgánu Světové obchodní organizace můžeme najít, to, že za nedodržení povinnosti soukromé entity může být odpovědný stát. Např. za neohlídání toho, aby daná entita danou povinnost neporušila.[105]

Orgány *de iure* se primárně rozdělují na legislativu, exekutivu a justici. Pokud začneme u exekutivy, jedná se o klasický příklad armády, ozbrojených vojsk. Jejich počínání je státu přičitatelné, i když nad nimi ztratí kontrolu, tím je myšleno, když se například některé jednotky ztratí.[106] V takových to případech je možné, aby stát byl odpovědný za jednání orgánů představující např. orgány, které bojují proti kyberkriminalitě a kyberzločinům. Legislativu představují akty, zákony a jiné právní normy. Může se jednat i o nepřijetí normy, která měla být podle mezinárodní smlouvy přijata. Rozhodnutí orgánů justice pak také mohou být přičitatelné státu. Může se jednat např. o špatný výklad smluv, neposkytnutí přeshraniční pomoci aj.

Mezi takováto jednání orgánů se mohou počítat zásahy státu, orgánů, které vydají rozhodnutí, které může uzavřít přístup k internetové stránce, nebo trestat porušení lidských práv na internetu. Může jít i o přijetí diskriminačních zákonů, nebo soudních rozhodnutí. O tomto více v kapitole 3.2.

Přičitatelnost za jednání entity, která není orgánem státu, a orgánu, kterému nebyla formálně svěřena nebo delegována pravomoc státu, je řešena v čl. 5 (pro entity) a v čl. 8 (pro *de facto* orgány). Čl. 5 stanoví, že: „*Chování osoby nebo entity, která není orgánem státu podle čl.*

[103] James Crawford, *State Responsibility : The General Part*, Cambridge Studies in International and Comparative Law (New York: Cambridge University Press, 2013).

[104] V tomto případu najely dvě britské lodě v albánských vodách Korfského průlivu na miny. Po prozkoumání okolí zde nalezly miny další. Albánie byla nařčena z rozmisťování min nebo, že alespoň o minách věděla. Mezinárodní soudní dvůr došel k závěru, že Albánie neoznámila existenci min ve vodách, které byly střeženy a ani nikoho nevarovala. Albánie byla odpovědná za explozi min a škody, na základě toho, že o existenci min měla a mohla vědět. Pavel Šturma, *Casebook : výběr případů z mezinárodního práva veřejného.*, 4. upravené vydání, Scripta iuridica: No. 8 (Praha: Univerzita Karlova v Praze, Právnická fakulta, 2019). str. 25.

[105] Crawford, *State Responsibility : The General Part*. str. 118.

[106] Lze například polemizovat nad povahou československých legionářů po konci 1. sv. války, zda by toto jejich jednání bylo přičitatelné státu, a jakému.

4, ale která je zplnomocněna zákonem tohoto státu, aby vykonávala určitou činnost vládní autority, je považováno za jednání státu podle mezinárodního práva, pokud daná osoba nebo entita jedná v daném rozsahu v dané situaci“.[107] Tento článek představuje „faktický test“ oproti testu představenému výše v čl. 4 (strukturální test). Tento článek získává na relevantnosti s ohledem na moderní praxi států outsourcovat své vládní funkce na nestátní entity. Do této kategorie se staví podle komentáře k ARSIWA veřejné korporace, poloveřejné společnosti a v některých zvláštních případech i soukromé právnické osoby. Hlavním problémem identifikace jsou tzv. „soukromé vojenské organizace“. Tyto organizace byly nasazeny Spojenými státy v Afghánistánu a Iráku.[108] Nejedná se však o jediné organizace, některé státy dávají soukromím organizacím na práci vedení věznic.[109] Podle ARSIWA je potřeba „jednání vládní moci“, ohledně které není zatím žádný konsensus, s ohledem na sociální a historické rozdílnosti států. Podle komentáře se jedná o organizace zabývající se detencí, migrací a quasi soudními záležitostmi. Teoreticky se ale může jednat i o organizace, které zabezpečují chod státních webových stránek nebo například zajišťují chod určitých serverů. Jedná se tedy o funkce, které historicky byly vykonávány státem, ale v současnosti jsou k tomuto jednání zmocněny zákonem. Dalšími kritérii může být důvod převodu těchto pravomocí, obsah, způsob a cesta, jak může být tato organizace veřejně odpovědná. Jednání *ultra vires* je jednání, kdy orgán překročí své pravomoci. Tohoto se mohou dopustit orgány specifikované v čl. 4 ARSIWA. Dále je to pak upraveno v čl. 7.

Také se jedná o orgány, které byly jednomu státu propůjčeny jiným státem, jak stanoveno v čl. 6. Jedná se o situaci, kdy jeden stát poskytne k dispozici jinému státu svůj orgán, který tento druhý stát může efektivně ovládat. Jednání tohoto orgánu jsou tak exkluzivně, za podmínek uvedených v čl. 6, přičítána státu, který je dostal k dispozici. Může se jednat o různé orgány, například propůjčený zdravotnický personál.[110] Nemůže se však jednat o fyzické osoby nenapojené na státní správu, teď osoby a orgány musejí odpovídat definic čl. 4.[111] Nejedná se také o orgány státu, které vysílá jeden stát do druhého, např. diplomatické mise, politická jednání. Příklad takového jednání můžeme vidět v rozsudku Evropského soudu pro lidská práva ve věci souzení v Andoře a zadržení ve Francii. U Andorského soudu byli přítomni jak soudci ze

[107] Komise pro mezinárodní právo, „Odpovědnost státu za mezinárodně protiprávní jednání". čl. 5.
[108] Crawford, *State Responsibility : The General Part*. str. 127.; Alex Kmeroff, „War for money. Leading private military companies of the world.", viděno 12. červen 2021, https://medium.com/smartaim-tech/war-for-money-leading-private-military-companies-of-the-world-eab9f9fe2de8.
[109] Austrálie John Alizzi, „Private prisons in Australia: our 20 year trial", viděno 12. červen 2021, https://rightnow.org.au/opinion-3/private-prisons-in-australia-our-20-year-trial/.
[110] Komise pro mezinárodní právo, „Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries". str. 44.
[111] Crawford, *State Responsibility : The General Part*. str. 135.

Španělska, tak z Francie, protože Andora nemá vlastní soudce. Byli tedy dáni k dispozici. Jakmile soudili v Andoře, nebylo jejich jednání považováno za jednání ani Francie, ani Španělska.[112]

Jednání *ultra vires* je upraveno v čl. 7. Vytvoření orgánu pomocí zákona mu vkládá určité pravomoci, které jsou striktně vyjmenovány[113] a např. v českém právu se tento institut nazývá enumerativnost veřejnoprávních pretenzí.[114] Každé překročení pravomoci může založit přičitatelnost danému státu.[115] O odpovědnost státu nepůjde, pokud daná entita, nebo orgán bude jednat v svém čistě soukromém zájmu.[116]

Orgány de facto

Orgány de facto jsou, nehledě na organizaci státu, všechny orgány, které mají svěřené nějaké pravomoci, nebo vykonávají činnost státní správy a nejsou vyjmenovány dle čl. 4 a 5 ARSIWA. Toto pravidlo je uvedeno v čl. 8 „*Chování osoby nebo skupiny osob je považováno jako jednání státu podle mezinárodního práva, jestliže tato osoba nebo skupina osob ve skutečnosti jedná na základě pokynů nebo pod vedením nebo kontrolou státu*“.[117] Základní pravidlo je však v právu opačné, jednání soukromých osob nemůže být státu obecně přičitatelné, mohou však nastat situace, kdy vztah mezi danou osobou a státem je specifický a fakticky dochází k chování osoby jako zmocněnce státu.[118] Bezesporu může nastat situace, kdy stát svěří nějaký úkol soukromé osobě, například si ji najme. I v tomto případě by se jednalo o přičitatelné jednání státu. Dále se jedná o orgány, kterým národní právo nepřiznává povahu orgánu, nebo úřadu. Náznak dalších definic můžeme najít v rozsudku Nicaragua,[119] kde se soud zabýval přičitatelnosti chování „pod vedením nebo kontrolou státu“, kdy došlo k představení „testu efektivní kontroly“. Stupeň kontroly musí být podle tohoto rozhodnutí úplná závislost, aby mohlo dojít postavení soukromé osoby do stejné pozice jako orgán státu. V případě, že se chování soukromé osoby řídí rozkazy a pokyny státu, které by sama jinak neučinila, bude se jednat o účinnou kontrolu. Poskytnutí výbavy a financování jednotek nezakládá celkovou

[112] Evropský soud pro lidská práva, Drozd and Janousek v. France and Spain, 12747/87, rozsudek ze dne 26. 06. 1992, ECLI:CE:ECHR:1992:0626JUD001274787.
[113] Komise pro mezinárodní právo, „Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries". str. 45.
[114] Aleš Gerloch, *Teorie práva.*, 8. aktualizované vydání, Právnické učebnice (Vydavatelství a nakladatelství Aleš Čeněk, 2021). str. 34. Ústava ČR, ústavní zákon č. 1/1993 Sb. čl. 2 odst. 3.
[115] Thomas Payne, „Teaching old law new tricks: Applying and adapting state responsibility to cyber operations", *Lewis & Clark Law Review* 20, č. 2 (2016): 683–715. str. 702.
[116] Crawford, *State Responsibility : The General Part*. str.137.
[117] Komise pro mezinárodní právo, „Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries". str. 47.
[118] Crawford, *State Responsibility : The General Part*. str. 130.
[119] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. Unite States of America). Merits, Judgement. I.C.J. Reports 1986.

kontrolu (complete dependance) Odvolací komora Soudního tribunálu pro bývalou Jugoslávii v případu Tadić[120] rozhodla, že stupeň kontroly musí být podle „testu celkové kontroly“ (*overall control*). ICTY došel k závěru, při studiu typu ozbrojeného konfliktu, neřešila se tedy odpovědnost a přičitatelnost státu. Odvolací soud rozvedl tuto myšlenku ještě dále: „*Požadavek mezinárodního práva přičitatelnosti státu za jednání učiněné soukromými osobami je, že stát musí vykonávat nad těmito osobami kontrolu. Stupeň kontroly se může měnit s ohledem na faktické okolnosti případu. Odvolací komora nevidí důvod, proč by mezinárodní právo mělo v každém z takových případů požadovat úplnou kontrolu*“.[121] Soud dále pokračuje a identifikuje dva druhy kontroly státu. První, kterou tvoří jednotlivci, kteří byli osloveni státem, aby provedli určité nelegální činy na území jiného státu.[122] Tito jednotlivci by museli mít přesné rozkazy k jednotlivým činům, aby mohlo dojít k přičitatelnosti. Toto můžeme podřadit pod tzv. „test efektivní kontroly“. Druhou skupinou jsou pak organizované a hierarchizované skupiny. V tomto případě by postačila „celková kontrola“, tzn. nemusí dostávat přímé instrukce či rozkazy. Další vývoj můžeme sledovat v rozsudku Mezinárodního soudního dvora ve věci Bosenská genocida.[123] V tomto rozsudku se MSD vrací k použitým argumentům v rozsudku Nicaragua, a to převážně z důvodu toho, že v případu Tadić nešlo o řešení odpovědnosti státu.[124] Hlavním argumentem, proč se MSD vrátil k testu efektivní kontroly je, že v případě použití testu „celkové kontroly“ dojde k rozšíření subjektů a chování, které by se státu mohly přičítat.[125] Čl. 8 tedy přebírá závěry přijaté těmito soudy a praxí státu, ale nestaví se přímo k jednomu závěru. Dle tohoto článku je možno použít jak test efektivní kontroly, tak test celkové kontroly, ale musí se přihlížet k jednolitým okolnostem a odlišnostem. Chování orgánů *de facto* nebude proto často spojeno se státem, s ohledem na složitost testů přednesených výše.

Pro aktivity v kyberprostoru bude právě čl. 8 často citovaný v rámci přičitatelnosti jednání státu. Příkladem mohou být různé organizace nebo polostátní orgány. V roce 2007 byla

[120] Obžalovaný Tadić byl bosenský Srb, který byl uznán vinných účastí při konfliktu po rozpadu Jugoslávie. Byl vinen z porušení Ženevských úmluv (1949) a zločinů proti lidskosti. V rámci předběžných otázek byla rozhodována i přičitatelnost státu v rámci určení povahy ozbrojeného konfliktu. ICTY neměl jurisdikci rozhodovat o odpovědnosti státu, ale pouze jednotlivců. Prosecutor v. Dusko Tadić. ICTY Case No. IT-94-1-T, Trial Chamber, 7 May 1997.

[121] Prosecutor v. Duško Tadić, International Tribunal for the Former Yugoslavia, Case IT-94-1-A (1999), ILM, vol. 38, No. 6 (November 1999), p. 1518, at p. 1541, para. 117.

[122] Payne, „Teaching old law new tricks: Applying and adapting state responsibility to cyber operations". str. 703.

[123] Case concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Yugoslavia); ICJ Reports 2007.

[124] Antonie Cassese, „The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia", *The European Journal of International Law*, č. 18 (b.r.). str. 653.

[125] Cassese. str. 657.

z kyberútoku na Estonsko podezřívána skupina jednotlivců Nashi,[126] poté co došlo k jejich přihlášení se k tomuto útoku.[127] Jednalo se o sponzorovanou skupinu jednotlivců, kteří byli navázání na Kreml. Nebylo však prokázáno dostatečné navázaní. V tomto případě lze spatřovat podobnost s případem Nicaragua.[128] Jejich jednání, které se protestních akcí by však se vší pravděpodobností nebylo možné, přičíst Rusku. Jejich jednání nebylo ovládáno nebo se neřídilo přímými pokyny z Ruska a tato organizace by nesplňovala podmínky testu efektivní kontroly.

2.1.2. Zvláštní případy přičitatelnosti – články 9-11

Články 9-11 ARSIWA se zaobírají zvláštními typy přičitatelnosti státu. Článek 9 upravuje případy, které se nestávají tak často, může k nim dojít v případě revolucí, ozbrojených konfliktů nebo okupace.[129] Jedná se o případy, kdy osoba nebo skupina osob fakticky vykonává státní moc při absenci státních orgánů. Komise pro mezinárodní právo se rozhodla v komentáři k tomuto článku uvést tři podmínky.[130] Zaprvé, chování osoby, nebo skupiny osob se musí efektivně podobat výkonu prvků státní moci. Toto pravidlo se odchyluje od podmínky navázání na stát, nelze tedy hovořit o orgánech státu *de facto*. Pokud však revolucionáři převezmou vládní orgány jako takové, bude pak toto chování přičitatelné podle čl. 4 a nikoliv čl. 9. Zadruhé, toto chování musí být uskutečněno v době, kdy státní orgány neexistují (*absent or default*). Tato podmínka se snaží podchytit veškeré případy, kdy může dojít, i k částečnému úpadku státu. Může se jednat i o nevykonávání státní moci na části území. Zatřetí, situace musí být taková, aby si vyžádala výkon těchto prvků státní moci. Jinými slovy, okolnosti výkonu prvků státní moci soukromými osobami by muselo obhájit pokus výkonu funkce policie nebo jiné funkce státu v případě jeho absence. Toto chování pak může být přičitatelné onomu státu. Tento princip možná naráží na obyčejové právo *levée en masse,*[131] tedy spontánní povstání obyvatelstva, které je upravené v právu ozbrojených konfliktů. V takovýchto případech, kdy revolucionáři převezmou vládu, je pochopitelné, že státní aparát již není funkční a nahradili jej jednotlivci revolucionářů, kteří pak mohou být odpovědni.

Článek 10 hovoří o odpovědnosti státu za jednání spáchané povstalci. Základem principu tohoto článku je, že stát nemůže být odpovědný za jednání povstalců. Tento článek však

[126] Молодёжное демократическое антифашистское движение "Наши" – Mladé demokratické antifašistické hnutí „Naši“.
[127] Christian Lowe, „Kremlin loyalist says launched Estonia cyber-attack", Reuters, viděno 15. červen 2021, https://www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090313.
[128] Payne, „Teaching old law new tricks: Applying and adapting state responsibility to cyber operations". str. 707.
[129] Crawford, *State Responsibility : The General Part*. str. 167.
[130] Komise pro mezinárodní právo, „Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries". str. 49.
[131] Crawford, *State Responsibility : The General Part*. 171; Geneva Convention 4A(6).

stanovuje výjimky z tohoto pravidla. Je rozdělen do tří odstavců. První odstavec stanoví, že pokud bude povstalecké hnutí úspěšné, a vytvoří novou vládu, bude chování povstalců přičitatelné státu. Podobnou situaci řeší odstavec druhý. V případě úspěšného povstaleckého hnutí, kdy dojde k vytvoření nového státního zřízení na území již existujícího státu, bude toto jednání přičteno nově vzniklému státu podle mezinárodního práva. Třetí odstavec pak stanoví, že se toto netýká situace, kdyby toto jednání mělo být určeno podle čl. 4 až 9.[132]

Posledním zvláštním případem, kdy stát jednání, které nelze přičítat státu podle čl. 9 a 10, potvrdil a přijal toto jednání za své. Jedná se o případy např. pozdějšího potvrzení. Toto pravidlo zakotvuje čl. 11. Příklad můžeme najít například v zajetí Adolfa Eichmanna, jednoho z vedoucích představitelů SS, ten byl zajat v roce 1960 skupinou Izraelců v Buenos Aires, poté odvezen zpět do Izraele. Argentina poté obvinila izraelskou vládu ze spoluúčasti na tomto únosu. Toto nařčení nebylo vyvráceno, ale však ani potvrzeno izraelským ministrem zahraničí. Byla otázka, zda Izrael o této situaci věděl, či vědět měl a mohl a bylo by mu přičítáno jednání podle čl. 8. V tomto případě vznikly pochybnosti, protože Izrael se o této skupině, která zajala Eichmanna, vyjadřoval jako o „skupině dobrovolníků“. Rezolucí Rady bezpečnosti bylo rozhodnuto, že Izrael o tomto jednání věděl a dal k němu souhlas. Bylo velice nepravděpodobné, že se jednalo o skupinu dobrovolníků, navíc fakt, že Izrael přijal zajatého Eichmanna a následně se pokusil o jeho popravu může být považován jako přijetí tohoto únosu, který může být podle tohoto článku postižen.[133]

Teoreticky lze uplatnit toto pravidlo i na útoky provedené v kyberprostoru, ale to pouze z důvodu, že jej lze uplatit na všechny situace.

2.1.3. Okolnosti vylučující protiprávnost

Ve vnitrostátním právu existují situace, kdy by bylo došlo k odpovědnosti státu, ale určitá okolnost vyloučí složku protiprávnosti. Jedná se primárně o situace souhlasu, sebeobrany, protiopatření, vyšší moci, tísně a nouze. V takovém případě, kdy stát se chce dovolat okolnosti vylučující protiprávnost, je obrácené důkazní břemeno.

2.1.4. Protiprávnost

Výše byl představen jeden z konstitutivních komponentů odpovědnosti, a to přičitatelnosti. Nyní dojde k představení druhého komponentu: protiprávnosti.[134] Protiprávnost je požadována již podle ARSIWA a to v čl. 2 odst. 1 písm. b). „*Jedná se o porušení závazku*

[132] Komise pro mezinárodní právo, „Odpovědnost státu za mezinárodně protiprávní jednání". čl. 10.
[133] Crawford, *State Responsibility : The General Part*. str. 183.
[134] Čestmír Čepelka, *Mezinárodní právo veřejné.*, Vyd. 1., Právnické učebnice (Praha: Beck, 2008). str. 584.

plynoucího z jakéhokoli platného pravidla mezinárodního práva, a to jak obyčejového, tak i smluvního“.[135] Protiprávní jednání může být způsobeno jednáním či opomenutím. Může být také způsobeno omezením, např. tím, že výkon povinnosti nesmí být provázeno úmyslem poškodit jiného nebo zasáhnout do sféry jiného. Povinnost může být založena také rozhodnutím soudu nebo mezinárodní organizace. Zde. lze uvést, že závaznost rezoluce Rady bezpečnosti OSN se opírá o čl. 25 Charty OSN, dle kterého mají tyto závazky před jinými závazky přednost.[136]

Protiprávní jednání a jeho identifikace bude záviset striktně na určitosti právní normy, která byla porušena.[137] Jedná se o situace, kdy daná norma v sobě například obsahuje ustanovení, že musí dojít ke vzniku škody, nebo jinému následku. V tomto okamžiku, porušením dané normy, ale i v případě, kdy norma žádnou takovouto specifikaci neobsahuje, dojde k protiprávnímu jednání. Pro účely odpovědnosti je pak důležitá protiprávnost jako celek, neboť způsobená škoda je již obsažená v protiprávnosti, tedy porušení dané normy.

V mezinárodním právu může dojít k situaci, kdy dané chování regulované žádnou psanou normou upraveno není. V takovém případě se může pak jednat o porušení obyčejového práva.

K protiprávnosti je též potřeba aby byla norma v platnosti a závazná. Inspirací zde může být rozhodnutí ve věci Gabčíkovo-Nagymaros.[138] V tomto rozhodnutí bylo dosaženo závěru, že věc platnosti a odpovědnosti jsou rozdílné věci a musí se k nim i tak přistupovat. Platnost závazku se tak posoudí podle mezinárodního smluvního práva, ale porušení závazku, nebo jeho chybné vypovězení, se posoudí podle pravidel odpovědnosti.[139]

Protiprávním jednáním se zabývají i některé články ARSIWA, a to v své třetí části.

2.2. Shrnutí

Odpovědnost v obecném měřítku lze aplikovat na celou oblast mezinárodního práva veřejného. Tyto principy jsou již uznávanými obyčejovými normami, které řídí odpovědnost států, nehledě na to, kde se porušení vyskytne. Lze tedy uzavřít, že odpovědnost státu jako taková může být v kyberprostoru aplikovatelná za podmínky aplikovatelnosti hmotného mezinárodního práva v této oblasti, čemuž se věnuje, se zaměřením na dvě oblasti, následující kapitola. Pokud však dojde k nějakému porušení, je potřeba podle této části dostatečně toto jednání podřadit jednání státu. K tomu tak dojde, pokud se bude jednat o jednání státního orgánu, nebo státem ovládané skupiny jednotlivců.

[135] Čepelka. str. 584.
[136] Čepelka. str. 585
[137] Crawford, *State Responsibility : The General Part*. str. 216.
[138] Gabčíkovo-Nagymaros Project (Hungary v. Slovakia); ICJ Reports 1997, str. 7.
[139] Crawford, *State Responsibility : The General Part*. str. 217.

Mezi hlavní způsoby přičtení jednání státu bude v oblasti kyberprostoru buďto jednání, které bude provedeno orgánem de facto, nebo de iure. Nejčastěji se můžeme setkávat s útoky v době míru, které jsou provedeny např. rozvědkami nebo vojskem. Útoky na cíle kritické infrastruktury jsou pak páchány jednotlivci, u kterých se odpovědnost státu vyšetřuje poměrně složitě.

Problematika u konkrétního jednání v kyberprostoru však nastává v kroku přičitatelnosti. Z povahy kyberprostoru a nedostatečně vyvinuté obrany států vůči útokům a zásahům z kyberprostoru dochází, jak již bylo zmíněno výše, k častým útokům, u kterých se nedokáže identifikovat viník. Bez ohledu na tento fakt, z hlediska aplikovatelnosti jsou odpovědnostní principy způsobilé být plně aplikovány na kyberprostor.

3. Aplikovatelnost práva kolektivní bezpečnosti a vybraných lidských práv v kyberprostoru.

Protiprávní jednání státu, tedy porušení jeho primární povinnosti, může vycházet z různých zdrojů mezinárodního práva.[140] V dnešní době je možné v kyberprostoru vykonávat různou činnost a tím pádem tato činnost spadá pod jiná odvětví mezinárodního práva. V tomto případě se může jednat např. o porušení Charty OSN, práva ozbrojených konfliktů nebo lidských práv. Mimo to je v kyberprostoru velice časté páchání trestné činnosti, kterou se pak zabývají orgány činné v trestním řízení národních států, nebo mezinárodní tribunály a soudy. Toto chování souvisí s kyberkriminalitou a jejím potíráním jak v oblasti transnacionálního práva, tak mezinárodního práva veřejného. Jednoduchost a přístup k nástrojům, kterými se dá páchat protiprávní jednání v kyberprostoru může vést k vzniku odpovědnosti státu dle předchozí kapitoly. Kyberútoky mohou svou povahou vystoupat až do míry, při které dojde k vysoké materiální škodě, nebo újmě na zdraví. Zatím lze konstatovat, že k žádnému kyberútoku s obdobnými následky nedošlo.[141,142]

Jednotlivých případů může být více a způsobů provedení taktéž. Je třeba mít na paměti, že i útokem DDoS, nebo Wormem se dají napáchat škody, které by byly na roveň kinetickým útokům, jak bude představeno dále. Tato část se zaměřuje na obecnou povahu odpovědnosti státu v kyberprostoru k vybraným oblastem mezinárodního práva. Tyto oblasti byly vybrány z důvodu možnosti využití stávající judikatury k provedení analýzy aplikovatelnosti mezinárodního práva veřejného. Dále se jedná o důvod již existující judikatury, kterou lze vztáhnout i na kyberprostor.

3.1. Kolektivní bezpečnost

3.1.1. Použití síly

Ať se jedná o kyberútoky nebo o kyberoperace, Charta OSN a její základní, obyčejová pravidla se uplatní na oba případy stejně. Jak již bylo zmíněno výše, obecně se mezinárodní právo uplatní i na kyberprostor. Čl. 2 odst. 4 Charty OSN stanoví, že: „*Všichni členové se vystříhají ve svých mezinárodních stycích hrozby silou nebo použití síly jak proti územní celistvosti nebo politické nezávislosti kteréhokoli státu, tak jakýmkoli jiným způsobem*

[140] Čepelka, *Mezinárodní právo veřejné.* str. 383.
[141] Roscini, *Cyber Operations and the Use of Force in International Law*. str. 2.
[142] Daniel Lohrmann, „Cyber Attacks: Is the 'Big One' Coming Soon?", viděno 15. červen 2021, https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cyber-attacks-is-the-big-one-coming-soon.html.

neslučitelným s cíli Organizace spojených národů“.[143] Toto pravidlo se vztahuje na období míru, nikoliv na *ius in bello.*[144]

Ačkoliv se jedná o stěžejní princip mezinárodního práva, pojem „síla“ není v Chartě definován.[145] V praxi určení, zda se jedná o použití síly, a nikoliv o jiné porušení mezinárodního práva, nebo o žádné, činí značné potíže.[146] Použití síly je podle některých autorů možné v případě použití ozbrojené síly. Výkladem čl. 2 odst. 4 nedojdeme k jasnému argumentu, že tomu tak opravdu je. V již zmíněném rozsudku Nicaragua došel soud k závěru, že použití síly může mít i jiné povahy, nemusí se jednat jen o přímé použití zbraní (i když v tomto případě došel soud závěru, že toto chování nedosáhlo hranice použití síly). Ozbrojený útok naopak bude vždy porušením tohoto článku. Ačkoliv již v rozsudku Nicaragua došel soud k závěru, že se jedná o obyčejové pravidlo a také o „*základní kámen celé Charty OSN*“,[147] není stále stanovena přesná definice. Odpověď na otázku, zda se tato pravidla aplikují i na kyberprostor, můžeme podpořit poradním posudkem Mezinárodního soudního dvora nazvaném Oprávněnost hrozby nebo použití jaderných zbraní,[148] v tomto posudku soud dochází k závěru, že ustanovení regulující použití síly, včetně sebeobrany, se vztahují na jakékoliv použití síly, nehledě na použitou zbraň. Lze tedy argumentovat, že do určité míry se mezinárodní právo bude vztahovat na kyberprostor.[149]

Zde dochází k určitému hodnocení, které působí oběma směry. Pokud závažnost kyberútoku bude nižší než použití síly, bude se jednat o vměšování se do záležitostí státu, pokud bude úroveň závažnosti vyšší, bude se jednat o ozbrojený útok.

Pokud bychom chtěli dojít k závěru, že kyberoperace může dosáhnout úrovně použití ozbrojené síly, je třeba použití síly rozebrat z různých analytických přístupů.[150]

Prvním takovým je přístup založený na typu zbraně[151] (instrumentu).[152] Tento přístup je tradičním přístupem odlišení mezi ozbrojenou silou nebo ekonomickými sankcemi. Základem je

---

[143] „Charter of the United Nations", 1 UNTS XVI.

[144] Michael N. Schmitt, *The Use of Cyber Force and International Law*, *The Oxford Handbook of the Use of Force in International Law:* (Oxford: Oxford University Press, 2015), https://doi.org/10.1093/law/9780199673049.003.0053. str. 1.

[145] Schmitt. str. 3.

[146] Roscini, *Cyber Operations and the Use of Force in International Law*. str. 45.

[147] Schmitt, *The Use of Cyber Force and International Law*. str. 2.

[148] Tento poradní posudek byl vyžádán na základě rezoluce Valného shromáždění 49/75 K. Otázka, která byla položena zněla: „Za jakých podmínek je dle mezinárodního práva hrozba nebo použití jaderných zbraní povolena?“ V tomto poradním posudku došel soud k závěru, který lze obecně aplikovat na všechny případy použití síly. Jednalo se o princip proporcionality, který sám o sobě nemůže vyloučit použití jaderných zbraní ve všech případech sebeobrany. Též bylo řečeno, že pokud je použití síly protiprávní, je poté i hrozba síly protiprávní. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226, International Court of Justice (ICJ), 8 July 1996.

[149] Roscini, *Cyber Operations and the Use of Force in International Law*. str. 45.

[150] Roscini. str. 46.

[151] Ačkoliv „zbraň“ není v mezinárodním právu taktéž definována, v tomto kontextu je chápána jako věc, která je určená, aby někomu ublížila, nebo aby někoho zabila. (Black’s Law Dictionary). ICRC termín „zbraň“

tedy zbraň. Tento přístup byl kritizován z důvodu, že zbraně jsou hodnoceny pouze na základě jejich fyzických charakteristik. Tedy nemůže jít o použití síly, pokud použijeme něco, co nemůže mít běžným používáním takový následek. Použitím tohoto přístupu bychom tak došli k závěru, že kyberútok nemůže být nikdy považován za použití síly, protože jeho charakteristiky nejsou stejné v porovnání se zbraní (např. tankem). Při použití prostého útoku DDoS nemůže dojít k použití síly, i když např. dojde v jeho důsledku k odstavení nebo přetížení letištních věží, což má za následek mnohem větší škodu, než by mohla způsobit konvenční zbraň. Stejně tak by útok na Estonsko nemohl být považován za kyberútok, protože programy nejsou určené primárně k páchání škod, nebo hrožení silou, protože nejsou primárně stvořeny k usmrcení. Tento přístup však neobstojí, protože jak je již v této práci na několika místech zmíněno, následky použití škodlivých programů a jiných způsobů útoků v kyberprostoru můžou dosáhnout následku srovnatelného s konvenčními zbraněmi. Domnívám se, že malware může způsobit škody srovnatelné s konvenční zbraní.

Další přístup je založený na typu cíle (target).[153] Tento přístup, na rozdíl od prvního, neřeší, jakým nástrojem byl čin spáchán, ale rozhodující je cíl tohoto útoku. V tomto případě se jedná o prvky kritické infrastruktury.[154] Prahu použití síly, případně ozbrojeného útoku, je tedy dosaženo, pokud je veden proti národní kritické infrastruktuře nehledě na její povahu.[155] V tomto případě by se jakýkoliv kyberútok považoval za použití síly, to znamená, že i pouhé nahrání určitého malwaru do systému prvku kritické infrastruktury, např. za účelem špionáže, by vedlo k porušení čl. 2 odst. 4. Tento přístup není žádoucí a užití jej společně s kyberútoky by vedlo k rozšíření zamýšleného rozsahu tohoto článku. V takovémto případě lze také za určitých okolností, v případě očekávaného útoku na kritickou infrastrukturu, uvažovat o případné „anticipatory self-defence“.[156] Použití tohoto typu sebeobrany by vyžadovalo splnění dalších podmínek, např. dosažení intenzity ozbrojeného útoku, tento druh sebeobrany nelze použít jen v případě nahrání malwaru do zařízení.

---

popisuje jako „prostředky ke krutému jednání vůči lidem nebo majetku nepřátelských sil“. (Jean-Marie Henckaerts a Louise Doswald-Beck, *Customary International Humanitarian Law* (Cambridge: Cambridge University Press, 2005). str. 23).

[152] Roscini str. 47.

[153] Roscini. str. 47.

[154] „*kritickou infrastrukturou [se rozumí] prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušením jejichž funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu*“ (zákon č. 240/2000 Sb. Krizový zákon, ze dne 9.8.2001, § 2 odst. 1 písm. g).

[155] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013) str. 45.

[156] Walter Gary Sharp, *Cyberspace and the Use of Force* (United States of America: Aegis Research Corporation, 1999). str. 130.

Posledním přístupem je přístup založený na následku (effect)[157] daného jednání. Na rozdíl od jiných přístupů k použití síly je zde rozhodný následek. Může se jednat o škodu na majetku nebo újmě na zdraví osob. Dochází zde k přirovnání, které připodobňuje kyberútoky s kinetickými zbraněmi. Kyberútoky jsou tak považovány za jakousi zbraň. Na základě tohoto přístupu by se o použití síly jednalo i v případě Stuxnetu,[158] nebo kyberútoku na plynovod v Turecku.[159] Pokud dojde k zničení celé sítě, nebo zastavení továrny, je možné toto považovat za použití síly, popřípadě ozbrojený útok. „*Zdá se být rozumné, považovat kyberútoky, které způsobí dostatečnou škodu, za ozbrojené útoky*".[160] Tento přístup limituje použití čl. 2 odst. 4 jen na ty útoky, které mohou způsobit stejný následek jako zbraně konvenční (kinetické). Dle Tallinnského manuálu tento přístup nereflektuje dnešní dobu. Kyberútoky lze v dnešní době spáchat i větší škody, než by způsobila kinetická zbraň. Je to z toho důvodu, že v dnešní informační sféře lze způsobit značné škody, a to fyzicky neničivými způsoby.

Jak je ale patrné z povahy provedení kyberútoků, ty mohou mít i jiné určení než zbraně, typu cíle nebo následku. Je možné, aby útok vedený věcí, která nemá svoje běžné užití jako zbraň, mohl napáchat škody srovnatelné s konvenčními zbraněmi. Je tedy možné argumentovat, že nezáleží na povaze předmětu, zbraně, ale spíše na jeho následcích, které se připodobňují následkům kinetických zbraní.

3.1.2. Ozbrojený útok vs. Použití síly

Hlavní rozdíl mezi použitím síly obecně a ozbrojeným útokem je, že při ozbrojeného útoku mohou státy aplikovat čl. 51 Charty OSN, sebeobranu. Platí, že vždy když bude učiněn ozbrojený útok, bude se také jednat o použití síly, ale ne vždy tomu bude naopak.[161] Určení, zda se jedná o použití síly, nebo specificky ozbrojený útok, je důležité pro určení následných reakcí států na tento čin. Ozbrojený útok je považován za nejzávažnější formu porušení míru.

---

[157]Roscini, *Cyber Operations and the Use of Force in International Law*. str. 45.

[158] Viz výše.

[159] V roce 2008 došlo k explozi na tureckém území. Tato exploze byla z počátku přičítána Kurdským extrémistům, kteří údajně měli spáchat kinetický útok na tento plynovod. Po delším vyšetřování důkazy ukazovaly na jiného aktéra, a to Rusko. Rusko mělo údajně být odpovědné za kyberútok na tento plynovod. Z následků a vyšetřování je patrné, že intenzita tohoto kyberútoku dosáhla následku, který byl podobný použití výbušniny. https://www.sans.org/blog/closing-the-case-on-the-reported-2008-russian-cyber-attack-on-the-btc-pipeline/

[160] Christopher C. Joyner a Catherine Lotrionte, „Information Warfare as International Coercion: Elements of a Legal Framework", *European Journal of International Law* 12, č. 5 (1. prosinec 2001): 825–65, https://doi.org/10.1093/ejil/12.5.825.str. 855.

[161] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. Unite States of America). Merits, Judgement. I.C.J. Reports 1986. para. 191.

Ozbrojený útok byl probírán v rozsudku Nicaragua (viz výše). V tomto rozsudku soud konstatuje, že mezi státy již existuje všeobecná shoda o tom, co zakládá ozbrojený útok.[162] Dále dodává, že definice ozbrojeného útoku nemá být součástí smluvního práva, ale spíše obyčejového.[163] Ozbrojený útok je tedy nejvážnějším porušením zákazu použití síly. Dle tohoto rozsudku je hlavním faktorem rozlišení ozbrojeného útoku od použití síly rozsah a následek (scale and effect).

Koncept ozbrojeného útoku byl taktéž řešen v rozsudku Ropné plošiny.[164] Tento rozsudek nepřímo stanovuje určité podmínky, které musí stát splnit, aby mohl využít své právo na sebeobranu. Jedná se o existenci útoku, odpovědnost státu a charakter útoku, tedy zda jeho účinky a rozsah jsou dostatečně závažné.

Všeobecná shoda panuje v některých aspektech ozbrojeného útoku. Primárně musí dojít k protiprávnímu použití síly. Dále se může jednat o podmínky, které mají určitou úroveň závažnosti. Závažnost můžeme spatřovat v následcích útoku, teritoriálním přesahu nebo škodách na životech a majetku.[165] Dále lze mluvit o faktoru přeshraničního útoku, použití ozbrojených sil státu a odpovědnosti státu.

Dle poradního posudku „*Otázka legality hrozby nebo použití jaderných zbraní"* bylo stanoveno, že k provedení ozbrojeného útoku není důležité, zda dojde k následku pomocí zbraně, či nikoliv.[166] Tento závěr tak minimálně vyvrací výše zmíněný přístup s ohledem na použití zbraně. S ohledem na tato zjištění lze argumentovat, že kyberútok lze za určitých podmínek kvalifikovat jako ozbrojený útok.

Je možné, že pro definování ozbrojeného útoku jsou důležité faktory narušení teritoriální integrity, vážné následky, užití ozbrojených sil, ztráty na lidských životech a na majetku.[167]

Pro účely této práce se ozbrojeným útokem rozumí útok, který se od „běžného" použití síly odlišuje ve svých následcích a rozsahu a který může být přičten státu. Nejedná se o přeshraniční potyčky, následek musí být dostatečně vážný a škoda, která tímto útokem vznikne, nesmí být nepatrná. Použití ozbrojeného útoku pak povede k možnosti aplikace článku 51 Charty OSN.

---

[162] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. Unite States of America). Merits, Judgement. I.C.J. Reports 1986. para. 195.

[163] Ibidem.

[164] Oil Platforms, Iran v United States, Judgment, merits, ICJ GL No 90, [2003].

[165] Tom Ruys, *„Armed Attack" and Article 51 of the UN Charter : Evolutions in Customary Law and Practice*, Cambridge Studies in International and Comparative Law (New York: Cambridge University Press, 2010), https://search.ebscohost.com/login.aspx?authtype=shib&custid=s1240919&profile=eds. str. 150.

[166] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226, International Court of Justice (ICJ), 8 July 1996. para. 40.

[167]Yoram Dinstein, *War, aggression, and self-defence.*, 5th ed. (Cambridge University Press, 2012), https://search.ebscohost.com/login.aspx?authtype=shib&custid=s1240919&profile=eds. str. 193.

Autoři Tallinnského manuálu vědomi si těchto problémů identifikace ozbrojeného útoku a použití síly přišli s demonstrativním výčtem faktorů, které, s ohledem na okolnosti, určí, zda mezinárodní společenství bude považovat kyberútok za použití síly, nebo ozbrojený útok, a zda tento útok naplní podmínky aplikace čl. 4 nebo čl. 51 Charty OSN,[168] které jsou zmíněny dále.

3.1.3. Pozice států

Některé státy v průběhu posledních let vydaly své „postition papers" týkající se postavení k problematice kyberprostoru, včetně použití síly. Německo například v svém position paper uvádí, že se ztotožňuje se závěry Tallinnského manuálu 2.0., tj. některé kyberoperace mohou dosáhnout intenzity použití síly, ale za splnění striktních pravidel. Německo se přiklání k porušení použití síly v případě, kdy kyberoperace dosáhne následku srovnatelného s následkem tradičním kinetickým použitím síly.[169] Posuzování by mělo probíhat případ od případu a mezi zkoumané aspekty by se měly *inter alia* řadit závažnost, bezprostřednost, úroveň narušení do cizí kybernetické infrastruktury nebo úroveň organizace a koordinace škodlivých kyberoperací.[170]

Spojené království se k těmto situacím staví poněkud neurčitě. Uznává, že se mezinárodní právo aplikuje na kyberprostor. Použití síly se pak aplikuje v určitých mezích, což je uvedeno na příkladu zničení jaderného reaktoru kyberútokem. Stejně tak se jedná o protiprávní použití síly v případě, kdy dojde k vyřazení letištních věží a dojde ke škodě na lidských životech. Tyto situace bude Spojené království považovat za použití síly, nebo ozbrojený útok.[171]

Francie se přihlásila k aplikaci mezinárodního práva v kyberprostoru a k použití síly a prohlašuje, že parametry stanovené v Tallinnském manuálu 2.0 jsou jen demonstrativní a nesouhlasí s požadavkem způsobení škody. K faktorům, dle kterých by se měl stát rozhodovat, přidává původ nepřátelského útoku a dopad, který útok zamýšlel.[172]

Spojené státy americké se shodují, že kyberoperace mohou zakládat porušení zákazu použití síly. Souhlasí, že určité faktory by měly být vzaty v potaz, těmi jsou například kontext, dopad, záměr. V určitých případech stanoví, že se jedná o použití síly automaticky, jedná se o

---

[168] Schmitt, *The Use of Cyber Force and International Law* str. 4.

[169] Michael Schmitt, „Germany's Positions on International Law in Cyberspace Part I", Just Security, podzim 2021, https://www.justsecurity.org/75242/germanys-positions-on-international-law-in-cyberspace/.

[170] Germany, „On the Application of International Law in Cyberspace, position paper", podzim 2021, https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf.

[171] Jeremy Wright, „Cyber and International Law in the 21st Century", 23. květen 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

[172] Ministére des Armées, „DROIT INTERNATIONAL APPLIQUÉ AUX OPÉRATIONS DANS LE CYBERESPACE", 12. listopad 2018, https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf.

narušení jaderné elektrárny, otevření přehrad nad obydlenými oblastmi a kyberoperace, které vyřadí letištní věže.[173]

Nizozemsko také považuje aplikaci mezinárodního práva v kyberprostoru za fakt. Pro Nizozemsko není za kyberoperaci považován pouze útok, který je svým dopadem a následky totožný s kinetickými útokem. Podle Nizozemska záleží na různých aspektech, kterými jsou povaha, závažnost, rozsah a cíl kyberútoku.[174]

Rusko a Čína daly ve svých vyjádřeních v position papers k OEWG najevo své pozice ke kyberprostoru. Z podání Ruska je patrné, že se staví k aplikaci mezinárodního práva v kyberprostoru s jistými výhradami. Jedná se převážně o vyloučení, že informační technologie nepovažuje za zbraně. Dále považuje za podstatné, aby nedocházelo k „politické přičitatelnosti" státům, ale aby tato přičitatelnost byla založena na pevném základě důkazů.[175] Čína na druhou stranu považuje aplikaci Charty OSN na kyberprostor za vitální.[176] Čína považuje za příznivé použití stávajících norem, ale i vznik nových norem.

Dalo by se shrnout, že tyto zmíněné státy zastávají teorii následku daného jednání, protože přirovnávají dopad kybernetických útoku, nebo operací, k těm konvenčním.

3.1.4. Určení intenzity kyberútoku

Jak bylo stanoveno výše, tým expertů a řada autorů je toho názoru, že státy by měly považovat kyberútoky za použití síly za splnění určitých podmínek.[177] Tyto podmínky jsou stanoveny demonstrativním výčtem. Mezi podmínky stanovené Tallinnským manuálem, kdy by mělo dojít ke kvalifikaci kyberútoků jako použití síly, patří následující faktory. Je nutné podotknout, že tyto faktory se do určité míry budou aplikovat i na stanovení limitů ozbrojeného útoku.

Závažnost (severity). Tento faktor je někdy uváděn jako samostatný. Jednání, které napáchá fyzické škody, bude častěji považováno za použití síly.[178] Jednání, které nepůsobí fyzické škody,[179] např. v případě poskytnutí tréninku kyberaktivistů, dodáváním peněz,[180,181]

---

[173] Harold Hongju Koh, „International Law in Cyberspace", 18. září 2012, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.

[174] Ank Bijleveld, „Keynote address by the Minister of Defence, Ms. Ank Bijleveld, marking the first anniversary of the Tallinn Manual 2.0.", 06 2018, https://english.defensie.nl/downloads/speeches/2018/06/21/keynote-address-by-the-minister-of-defence-ms.-ank-bijleveld-marking-the-first-anniversary-of-the-tallinn-manual-2.0-on-the-20th-of-june-2018.

[175] https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-the-russian-federation-15-june-2020.pdf.

[176] https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf

[177] Payne, „Teaching old law new tricks: Applying and adapting state responsibility to cyber operations". str. 694.

[178] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*. str. 48.

[179] Payne, „Teaching old law new tricks: Applying and adapting state responsibility to cyber operations". str. 695.

[180] Schmitt, *The Use of Cyber Force and International Law*. str. 4.

bude považováno za použití síly pouze s ohledem na rozsah, trvání a intenzitu společně s faktory, které jsou uvedeny dále. Tento faktor bude hrát velkou roli v identifikaci útoku jako ozbrojeného útoku, v případě, kdy kyberútok bude schopen způsobit škody na majetku nebo zdraví.[182]

Bezprostřednost (immediacy). Čím rychleji se následek projeví, tím mají státy méně možností řešit situaci mírovými cestami. Státy bude více zajímat rychlejší následek útoku než ten, který se postupně buduje.[183] Útok tedy musí mít zamyšlený efekt téměř okamžitě, aby došlo k jeho klasifikaci jako použití síly.[184] Pro klasifikaci jako ozbrojený útok nebude bezprostřednost hrát tak značnou roli.

Přímost (directness). Na rozdíl od bezprostřednosti tento aspekt pracuje s kauzálním řetězcem,[185] mezi konáním a následkem. V případě, že kybernetický útok nebude přímý, ve smyslu že nebude přímo veden na svůj cíl, nedojde k jasné klasifikaci tohoto chování jako použití síly.[186] Pokud tedy dojde k napadení systému, který zajišťuje například zabezpečení elektrické sítě, a dojde i k výpadku elektrické sítě, tento útok nebude mít přímou kauzu. Přímost lze ilustrovat i na konvenčních zbraních. Bomba exploduje a způsobí škodu, kyberútok, který se tomuto připodobní, bude velmi často považován za použití síly.[187] Malwarové útoky jsou typické právě ve své nepřímosti. Ne vždy, když se nahraje vir do počítače, nebo se provede DDoS útok na cílové zařízení, dojde k následku přímo u tohoto zařízení.

Invazivnost (invasiveness). Ta odkazuje na míru proniknutí kyberútoku nebo kyberoperace do systémů státu, nebo na území státu. Čím více je systém zabezpečený, tím větší je míra proniknutí do tohoto systému, a tím je větší možnost, že mezinárodní společenství jej bude považovat za použití síly. Stejné je to s tím, pokud dojde k útoku DDoS na stránky vlády, nebo ministerstva obrany. Tyto útoky budou často považovány za použití síly. Je však nutné je odlišovat od špionáže. Ke kvalifikaci kyberútoku jako použití síly tedy nebude stačit špionáž jako taková, ale například umožnění špionáže.[188] V případě, že dojde k porušení teritoriální suverenity, nebo napadení kritických systémů do značné míry nad úroveň špionáže, lze diskutovat o možnosti klasifikace jako ozbrojený útok.

Měřitelnost následku (measurability of effects). V běžném konvenčním prostředí je často jednoduchá, protože následek je často identifikovatelný a vyčíslitelný. V kybernetickém prostředí je vyčíslení a kvantifikace škody s ohledem na povahu cílů nemožná. Pokud budeme

[181] Viz také případ skutkové okolnosti případu Nicaragua.
[182] Ruys, *„Armed Attack" and Article 51 of the UN Charter : Evolutions in Customary Law and Practice*. str. 176.
[183] Schmitt, *The Use of Cyber Force and International Law*. str. 5.
[184] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*. str. 49.
[185] Schmitt, *The Use of Cyber Force and International Law*. str. 4.
[186] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*. str. 49.
[187] Schmitt. str. 50.
[188] Schmitt.str. 51.

situaci ilustrovat například na zrušení přístupu k internetové stránce, majetková škoda nepůjde vyčíslit. Situace, kdy toto nebude činit takové obtíže, budou útoky např. na letištní věže, které povedou k pádu letadel.

Vojenská povaha (military character). Ta je splněna, pokud je navázána na armádu nebo na vojenské operace spáchané vojenským personálem.[189] Může se také jednat o charakter daného cíle.[190]

Zapojení státu (state involvement).[191] To znamená, že se bude na kyberoperaci častěji pohlížet jako na použití síly, pokud bude spáchána tak, že jednání bude přičteno státu, nebo bude přímo státem činěno. Bude se tak jednat o činy spáchané rozvědkou, tajnými službami, nebo armádou.[192]

Presumovaná legálnost (presumptive legality).[193] Mezinárodní právo pracuje s přístupem „co není zakázáno je dovoleno“, jedná se například o již zmíněnou špionáž, ekonomický nátlak, propagandu.[194] Toto jednání bude považováno za legální a méně často dojde ke klasifikaci jako použití síly.

Některé z těchto faktorů uvedených v Tallinnském manuálu lze vztahovat i na ozbrojené útoky. Bude záviset na jejich míře a následku, který kyberútok napáchá. V případě míry, která bude převyšovat určitou hranici, lze usuzovat, že místo použití síly dojde ke kvalifikaci ozbrojeného útoku. Tyto faktory budou hrát roli při identifikaci, nejedná se však o závaznou metodiku. Domnívám se, že v případě dostatečné majetkové škody, která přesahuje úroveň přeshraniční potyček a dosahuje určité intenzity, lze dojít k závěru, že je možné přičíst státu porušení zákazu použití síly, ale i ozbrojeného útoku, a to v případě dosažení větší míry intenzity pomocí kyberútoku. To následně povede k použití čl. 51 a práva na sebeobranu.

3.1.5. Použití síly, odpovědnost a přičitatelnost v kyberprostoru

Dle výše řečeného lze dojít k závěru, že někteří autoři a experti zastávají názor, že kyberútoky lze považovat za použití síly s výhradou toho, že musejí být zkoumány případ od případu.[195]

[189] Schmitt. str. 52.
[190] Payne, „Teaching old law new tricks: Applying and adapting state responsibility to cyber operations". str. 696.
[191] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*. str. 52.
[192] Schmitt, *The Use of Cyber Force and International Law*. str. 5
[193] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*. str. 53.
[194] Schmitt, *The Use of Cyber Force and International Law*. str. 6
[195] Schmitt, *The Use of Cyber Force and International Law* str. 6.

Pro ilustraci svých dílčích závěrů bych stanovil reálný příklad. S ohledem na definice a teorii v této práci bych se pokusil dojít k závěru, zda lze kyberútoky považovat za použití síly, popřípadě i za ozbrojené útoky.

Stuxnet byl vyvinut s cílem zneškodnit vybavení Iránského zařízení na obohacování uranu. Stuxnet byl nejdříve vyvinut, a poté nahrán na flash disk. Tento virus byl upraven tak, aby vyhledával v zařízeních jistý program. Do té doby jinak neohrožoval zařízení. Jakmile nalezl správný program (Siemens step 7 software) začal tento vir nahrávat a měnit kódování tohoto programu. Program pracoval stále správně, protože vykazoval již změněné procesy. Po nějaké době změněného fungování tohoto programu selhalo vybavení, chlazení a jiné, čímž došlo k zničení tohoto vybavení.[196]

Pokud vycházíme z teorie Effects principle a z definice, že za kyberprostor se považují i zařízení a abstraktní nehmotná síť (viz kapitola 1), můžeme dojít k závěru, že tento útok se v kyberprostoru odehrál a mezinárodní právo se v tomto případě uplatní. Propojením z flash disku a následkem, který se projevil na zařízení, došlo k útoku pomocí kyberprostoru, cílem byl totiž počítačový systém, který spravoval chod zařízení.

Závažnost tohoto jednání lze spatřovat v tom, že se jednalo na útok na území cizího státu, tedy došlo k porušení suverenity státu, na kterém v konečném důsledku vznikla škoda, která svou výší a cílem byla závažná. Bezprostřednost však již není tolik patrná, po nahrání viru do prvního zařízení mohla uplynout delší doba, není jednoznačné, zda došlo k nahrání viru do systému a poté k bezprostřednímu „útoku“, tento fakt nelze prokázat s ohledem na nejisté informace. Přímost je naplněna, útok byl proveden přímo na zařízení, přes jeho počítače, nikoliv přes internet a kauzální nexus je zde patrný. V případě, že by útok nebyl veden přímo na cílové zařízení a procházel by přes řadu zdrojů, tak by útok působil nahodile. V tomto případě ale v důsledku nahrání viru došlo k selhání zařízení. Invazivnost je splněna, protože se jedná o citlivé zařízení a zásahu do Íránské suverenity. Následkem byla majetková škoda, která se dá změřit. Vojenský charakter nelze zhodnotit, protože není jasné, kdo čin spáchal. Zapojení státu také není jasné, i když panují dohady, které s ohledem na jejich nepodloženost v práci neuvádím. Čin nemohl být považován za legální, i kdyby se z počátku jednalo o špionáž, ve finálním důsledku došlo ke škodě a čin by to tak byl v každém ohledu nelegální.

S využitím výše uvedené analýzy Stuxnetu lze tyto faktory použít a pokusit se argumentovat, že Stuxnet nebyl pouze použitím síly, ale že tento útok dosáhl úrovně

[196] Tento odstavec představuje hypotetický příklad, který je inspirovaný skutečnými událostmi. Pro ilustraci nejsou uvedeny všechny tyto okolnosti, ale jen část, která tak slouží k právnímu rozboru, který jej následuje. „What is Stuxnet?", Mcafee, viděno 12. květen 2021, https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html.

ozbrojeného útoku. Cílem Stuxnetu bylo zničit zařízení. Následkem byly obrovské škody. Jednalo se o útok, který nejspíše cílil přes hranice jiného státu. Problémem však zůstává jeho nepřímost, kdy k útoku docházelo, ale následek se neprojevil. Pokud vynecháme aspekt přičitatelnosti státu a spáchání tohoto činu ozbrojenými silami, Stuxnet by se dal považovat za ozbrojený útok. V tomto případě je také potřeba určit, zda se v této době již neaplikovalo právo ozbrojených konfliktů. V případě, že se viník nedopátral, není možné tento faktor zkoumat. Dalším faktorem je to, že Írán žádným způsobem tento útok nehodnotil jako ozbrojený útok.[197]

Dle názoru autora je logické, aby útok na Iránské zařízení pomocí Stuxnet byl považován za použití síly v mezinárodním prostředí. Stuxnet by tedy mohl být považován některými státy za použití síly.[198] Tyto závěry však nelze generalizovat a bude potřeba zkoumat každý jednotlivý kyberútok zvlášť. Přičitatelnost státu je však v tomto případě nejistá. Jak již bylo zmíněno výše, nesnadné zjištění toho, kdo kyberútok spáchal, bude nadále značným limitem pro jednotlivou odpovědnost státu v kyberprostoru.

Stuxnet však zůstává jedním z mála případů, které slouží k ilustraci použití síly, jelikož následkem tohoto kybernetického útoku došlo k materiální škodě. Intenzita je klíčová pro vůli států označit útok za porušení zákazu použití síly. Jednotlivé zkoumání případů, kdy došlo k porušení suverenity, dostatečné intenzitě útoku, a naplnění limitů, bude záviset na možnosti mezinárodního vyšetřování. Pokud jednotlivé státy dovolí vyšetření a čin bude přičten státu podle pravidel určených v kapitole 2, je velice pravděpodobné, že stát bude za tento čin odpovědný. Dále bude pravděpodobné, že v případě, kdy dojde k plynutí času od provedení útoku, nebude již sebeobrana ze strany oběti legitimní.

3.1.6. Agrese v kyberprostoru

Definice agrese se objevuje již v rezoluci Valného shromáždění OSN č. 3314 (XXIX) ze dne 14. prosince 1974.[199] Agresí podle definice z roku 1974 se rozumí použití ozbrojené síly státem proti suverenitě, územní celistvosti nebo politické svobodě jiného státu, nebo jakýkoliv způsob, který je neslučitelný s Chartou OSN.[200] Skutkové podstaty agrese jsou invaze nebo útok ozbrojených sil nebo okupace, bombardování, blokáda. Hlavním definičním prvkem je použití síly, které se soustředí na nějakém území. K tomuto závěru můžeme dojít analýzou zmíněných způsobu v demonstrativním výčtu.

[197] Andrew C. Foltz, „Stuxnet, Schmitt Analysis, and the Cyber ‚Use-of-Force´ Debate", *JFQ* 67, č. 4 (2012). str. 46.
[198] Foltz. str. 42.
[199] UN General Assembly, „Resolution 3314 (XXIX). Definition of Aggression, with annex", 12 1974, https://undocs.org/en/A/RES/3314(XXIX).
[200] General Assembly.

Pro účely této práce bude zločin agrese zkoumán z pohledu kolektivní bezpečnosti, a to části VII Charty OSN, na základě rozhodnutí Rady bezpečnosti OSN.[201]

Pokud jde o spáchání agrese v kyberprostoru, nejprve je nutné rozhodnout, zda lze naplnit definici agrese i přes útok vedený přes kyberprostor, nebo proveden v kyberprostoru. Zásadní v tomto případě bude určení Rady bezpečnosti OSN, že došlo ke spáchání zločinu agrese.[202] I v případě agrese platí rozlišení mezi použitím síly a ozbrojeným útokem, ne vždy může agrese dosáhnout dostatečné intenzity, kdy bude možné použití sebeobrany.

Definice agrese je použitelná na konvenční ozbrojené útoky. Rezoluce, která zavádí definici agrese z roku 1974, uvádí, že k některým útokům může dojít na moři, ve vzduchu a jiných „doménách". Dále je zde uvedeno, že zmíněné útoky, jako je invaze, námořní blokáda a jiné, jsou jen demonstrativním výčtem možných způsobů spáchání zločinu agrese. Někteří autoři docházejí k závěru, že ozbrojený útok může nastat i tehdy, pokud jsou jeho následky srovnatelné s takovýmto tradičním chápáním.[203] Pro zločin agrese je důležitá teritorialita. Může se jednat o případ, kdy půjde o útok na území státu, nebo dojde k útoku na kyberprostor, který např. hostí určité cloudové servery daného státu. V dnešní době, kdy jsou dodávky vody, elektřiny, a i potravin řízeny pomocí počítačů, lze argumentovat, že naplnění těchto podmínek v kyberprostoru nebo skrze něj je možné.[204]

Rezoluce Rady bezpečnosti, které v historii hodnotily zločiny proti míru, se vždy zaobíraly událostmi, které měly konvenční charakter, nikdy nebylo rozhodnuto o zločinu proti míru v rámci kyberprostoru.[205] Kyberkriminalita byla považována za novou rostoucí hrozbu v letech 2010-2011,[206] ale od té doby probíhala pouze neformální setkání v rámci řešení kyberprostoru.

Rada bezpečnosti nevydala žádné formální vyjádření, ani v této oblasti formálně nejednala. K jednáním docházelo vždy pouze mezi jednotlivými státy, nebo na úrovni ministrů jednotlivých států. Jedním z takovýchto jednání bylo neformální setkání (Arria-formula) konané

[201] Niels Blokker, „The Crime of Aggression and the United Nations Security Council ESSAYS IN HONOUR OF JOHN DUGARD: THE PROTECTION OF THE INDIVIDUAL IN INTERNATIONAL LAW", *Leiden Journal of International Law* 20, č. 4 (2007): 867–94. str. 880.

[202] Blokker. str. 803.

[203] Sharp, *Cyberspace and the Use of Force*. str. 115.

[204] Kristýna Urbanová, „The Kampala Agreement on Crime of Aggression and Responsibility for Cyber-Attacks", *Czech yearbook of public & private international law = Česká ročenka mezinárodního práva veřejného a soukromého/ Česká společnost pro mezinárodní právo*, č. 6 (2015): 103–14. str. 110.

[205] Security Council, „Actions with respect to threats to the peace, breaches of peace, and acts of aggression", in *Repertoire of the Practice of the Security Council: 22nd Supplement* (New York: Department of Political and Peacebuilding Affairs, 2019).

[206] Security Council, „Actions with respect to threats to the peace, breaches of peace, and acts of aggression", in *Repertoire of the Practice of the Security Council* (New York: Department of Political and Peacebuilding Affairs, 2011). str. 463.

28. listopadu 2016, které bylo organizované Španělskem a Senegalem. Na tomto setkání se došlo k závěrům, že určité kyberútoky mohou ohrozit mír a bezpečnost. S ohledem na problémy přičitatelnosti a dopátrání se skutečného viníka bylo výsledkem tohoto setkání pouhé doporučení, aby se státy soustředily na prevenci a sdílení postupů. Další setkání proběhlo v roce 2017, toto jednání se soustředilo na nové metody hybridních válek a jiných instrumentů, které se pokouší prosadit politické zájmy.

Estonsko si v rámci svého předsednictví v Radě bezpečnosti ve svém programu zařadilo kyberbezpečnost mezi své priority.

3.1.7. Agrese a Tallinnský manuál

Tallinnský manuál představuje pravidlo[207] obdobné čl. 39 Charty OSN. Rozhodnutí ohledně agrese dle tohoto článku závisí na Radě bezpečnosti. Rozhodnutí, zda některý z kyberútoků dosáhne míry, při které dojde k jeho identifikaci agrese, se však nevyjadřuje. Vodítkem k aplikaci těchto ustanovení na kyberprostor může být čl. 41 Charty OSN. Ten určí, jaká možná opatření nezahrnující použití síly mohou být přijata. Mezi ně patří také přerušení telegrafních, rádiových a jiných spojení.

Při výkladu definice agrese nesmí dojít rozšíření, ani zúžení rozsahu ustanovení Charty OSN, které by měly být porušeny.[208] S ohledem na výše uvedené, a pokud státy uznají použití síly v kyberprostoru za možné, lze argumentovat, že by mohlo být uznáno i spáchání agrese v kyberprostoru. Analogie by v tomto případě mohla být nápomocná. Může se jednat o přirovnání kyberútoku k ozbrojenému útoku (jak je diskutováno výše), nebo přirovnání jednotlivých útoků k vyjmenovanému demonstrativnímu výčtu.

Definice agrese z roku 1974 však obsahuje některá ustanovení, která mohou použití v kyberprostoru bránit. Jedná se především o soustředění ozbrojených útoků na území státu a ochrana územní celistvosti. Jak je patrné z první kapitoly této práce, kyberprostor nelze jako celek vlastnit, můžeme pouze vlastnit zařízení, která jsou připojena ke kyberprostoru. Dalším aspektem je narušení politické svobody a suverenity.[209] Oproti teritorialitě je možné najít oporu pro provedení útoku proti suverenitě, a to ve vyjádření Spojeného království při kyberútoku na Gruzii.[210] Je nutné podotknout, že tento útok cílil přímo na poskytovatele internetového hostingu a důsledkem byl výpadek národních stránek. I přes to, že by nebylo možné, nebo by bylo velice

[207] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*. str. 65.
[208] Potočný, *Mezinárodní právo veřejné : zvláštní část.* str. 433.
[209] rezoluci Valného shromáždění OSN č. 3314 (XXIX) ze dne 14. prosince 1974.
[210] Dominic Raab, „UK condems Russia's GRU over Georgia cyber-attacks", Government UK, 02 2020, https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.

nepravděpodobné provést kyberútok v rozsahu agrese proti územní celistvosti státu, bude velice pravděpodobně možné provést takový útok proti suverenitě, nebo politické svobodě.

Mezinárodní soudní dvůr se agresi věnoval krátce ve svém rozsudku Nicaragua.[211] K tomuto se vyjádřil, že agrese může být považována za obyčejové právo, a dále, že se jedná o akci, která svým rozsahem a následkem je připodobněna ozbrojenému útoku.[212] Dále pak také zdůvodnil, že některá jednání však nedosáhnou dané intenzity a mohou být klasifikovány jinak.

Tyto možnosti však nezaručí, že Rada bezpečnosti podle čl. 42 Charty OSN, MSD, nebo jiný orgán rozhodne, že došlo agresi. Z tohoto důvodu je nutné prozkoumat postavení států, judikaturu anebo přístup jednotlivých organizací k aplikaci mezinárodního práva na kyberprostor. Rada bezpečnosti má pět stálých členů, dále se zaměřím právě na ně, z důvodu práva vetovat rozhodnutí.[213] Jedná se tedy o Rusko, Čínu, USA, Spojené království a Francii. K postavení jednotlivých států viz kapitolu 3.1.3.

S ohledem na výše zmíněné bude pravděpodobně záležet případ od případu, kdy dojde k přiznání porušení zákazu agrese.

3.1.8. Shrnutí

Použití síly v kyberprostoru je některými státy považováno za možné při splnění určitých kritérií. Hlavním spojovacím argumentem je, že se kyberútok ve svých následcích vyrovná konvenčnímu útoku co do vzniklé škody, tak i například typu cíle, na který je útok veden. Dojde-li k vyřazení prvků kritické infrastruktury, např. vyřazením zařízení pro výrobu elektřiny, nebo o obsluhu letiště nebo navigaci, tak v těchto případech je nejspíš možné, že dojde k identifikaci kyberútoku jako použití síly.

Tallinnský manuál přichází s možným vodítkem pro státy, jak hodnotit různé útoky co se týče jejich závažnosti, invazivnosti, vojenského charakteru aj.[214] Z některých prohlášení států je patrné, že tyto faktory berou v potaz v rámci identifikace jednotlivých útoků.

Někteří „větší“ aktéři prozatím nevydali prohlášení, zda a v jaké míře považují použití síly v kyberprostoru za možné (Rusko, Čína). Ti, kteří prohlášení vydali, využívají k použití síly teorii Effects principle, jak je uvedena v první kapitole. Je tedy otázkou času, kdy dojde k podobnému útoku na prvky kritické infrastruktury, nebo většího rozsahu, které budou považovány za použití síly.

---

[211] Viz výše.
[212] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. Unite States of America). Merits, Judgement. I.C.J. Reports 1986. str. 93.
[213] „Voting System", UN Security Council, b.r., https://www.un.org/securitycouncil/content/voting-system.
[214] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*. str. 51.

Stále však platí výše zmíněné, to, že přičitatelnost v takovýchto případech použití síly je značně obtížná a odpovědnost státu jako takovému těžko prokazatelná.

S ohledem na skutečnosti, že použití síly, ozbrojený útok a agrese na sebe striktně navazují, je potřeba se k tomuto rozdělení vymezit. Použití síly, které dosáhne určité intenzity, může být analogicky použito na agresi. S ohledem však na specifičnost agrese v demonstrativním výčtu v rezoluci č. 3314 není jednoznačně možné určit, zda praxe států bude shodná při určování použití síly stejně jako hodnocení zločinu jako agrese.

Agrese může mít různé povahy, tradičně se objevuje v případě, kdy dochází k porušení míru, nebo jeho ohrožení. Logicky by se tak dalo uvažovat o tom, že pokud dojde k vyřazení zařízení kritické infrastruktury, následky budou podobné, jako kdyby došlo například k potyčkám, nebo ozbrojeným útokům.

Některé státy jsou toho názoru, že lze kyberútokem lze narušit suverenitu státu, která je jednou z podmínek určených v původní rezoluci. V tomto případě lze argumentovat, že agrese může být spáchána s ohledem na intenzitu a další aspekty, které budou hodnoceny případ od případu.

Nelze v tomto případě spoléhat na postavení států, které se k této záležitosti ve svých prohlášení nevyjadřují.

Lze také argumentovat, že lze spáchat i ozbrojený útok v kyberprostoru, je ale potřeba naplnit striktnější limity, které mohou spočívat převážně v rozsahu a následcích (scale and effect), ale taky jiných, jako jsou použití ozbrojených sil, porušení suverenity státu ad.

3.2. Porušení lidských práv v kyberprostoru

Odpovědnost státu za protiprávní jednání v kyberprostoru není ve své podstatě pouze spojené s materiální škodou nebo ztrátou lidských životů. Jak bylo zmíněno výše, stát může být odpovědný i za to, že nekonal. Pro lidská práva platí to stejné, co pro ostatní oblasti; mezinárodní právo se na ně v určitém rozsahu aplikuje.[215] Povinnost států v oblasti lidských práv však nezůstává jen u toho, aby stát tato ujednání dodržoval. Stát má povinnost respektovat, chránit a naplňovat lidská práva a musí za použití soudních, správních, vzdělávacích a jiných prostředků dosáhnout svých povinností.[216] Stát má tedy povinnost zajistit i právní prostředí pro respektování lidských práv.

K mezinárodněprávnímu zakotvení ochrany moderních lidských práv coby cíle OSN ve světovém měřítku došlo v Chartě OSN (1945). Tato úprava byla však příliš obecná[217] a státy se snažily její nedostatky postupně odstraňovat tím, že obecné ustanovení o cíli ochraně lidských práv rozšiřovaly a konkretizovaly. Nejdůležitějším předpisem ve formě soft law je Všeobecná deklarace lidských práv[218] a dvě úmluvy z roku 1966, Mezinárodní pakt o hospodářských sociálních a kulturních právech a Mezinárodní pakt o občanských a politických právech. V mezinárodním právu najdeme mnohem více předpisů různých forem, které se zabývají ochranou lidských práv. Postupem času se objevují i regionální úmluvy, například v rámci Rady Evropy, nebo Evropské Unie.

Mezi nejvíce vyvinuté regionální úpravy se řadí práce Rady Evropy a zejména Úmluva o ochraně lidských práv a svobod („Úmluva“),[219] touto úmluvou byl také zřízen Evropský soud pro lidská práva (ESLP). Za svou dlouhou existenci dokázal vytvořit stabilní judikaturu a výklad jednotlivých ustanovení Úmluvy. Pro účely této práce je pracováno právě s rozhodnutími tohoto soudu, a to z důvodu množství použitelné judikatury a jejich aktuálnosti.

ESLP i ve svých rozhodnutí pracuje s myšlenkou, že se lidská práva, mimo jiné právo v čl. 10, aplikují i na internet[220] (rozsah aplikace lidských práv v kyberprostoru však není neomezený a univerzální, může se jednat o práva na internetu, jako složky kyberprostoru, ve které lze aplikovat svobodu projevu, protože lidský prvek jej může používat jako platformu pro

[215] Gabor Rona a Lauren Aarons, „State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace", *Journal of National Security Law and Policy* 8, č. 3 (2015): 503–30. str. 503.
[216] Rona a Aarons. str. 503.
[217] Rona a Aarons. str. 505.
[218] UN General Assembly, „Universal Declaration of Human Rights", 12 1948, 217 A (III).
[219] Rada Evropy, ETS 5, European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 listopad 1950, uložena u Generálního sekretariátu Rady Evropy.
[220] „Freedom of Expression and Information", Freedom of Expression, viděno 2. květen 2021, https://www.coe.int/en/web/freedom-expression/freedom-of-expression-and-information-explanatory-memo.

své vyjadřování, jedná se tak o „veřejné fórum“,[221] dále může jít v kyberprostoru jako takovém o ochranu soukromí a dat uložených v kyberprostoru (čl. 8), ale i některá další, jako je např. právo na život (čl. 2).

3.2.1. Právo na soukromí

Právo na soukromí je upraveno v čl. 8 Úmluvy o ochraně lidských práv a svobod, který je nazvaný „Právo na respektování soukromého a rodinného života“.[222] Ve své rozhodovací činnosti došel Velký senát k závěru, že i informace a komunikace na internetu je předmětem ochrany soukromí. Komunikací se rozumí telefonní hovory, emailová komunikace, ať již učiněna soukromě nebo v rámci zaměstnání.[223] Porušení práva na soukromí je v kyberprostoru velice časté a jedná se o často zmiňované téma.[224]

V kyberprostoru jde nejčastěji o zásah do soukromí, které je představováno zásahem do „osobní“ sféry na internetu. Ta může představovat to, jaké webové stránky navštěvujeme, s kým a co si píšeme, kdy se přihlašujeme. Aktivita pak může být přímo přičtena jednotlivci s ohledem na jeho IP adresu.

Stát může zasáhnout do této sféry jen pokud je toto jednání upraveno zákonem a odůvodněno dostatečným důvodem. Důvody jsou poté doplňovány judikaturou nebo mezinárodním právem, např. Úmluva o počítačové kriminalitě.[225] Mezi možné důvody se řadí například potírání trestné činnosti.[226]

Prolomení práva na soukromí může být provedeno státem, v případech trestního vyšetřování a jen pro tyto účely. V rozsudku ve věci Benedik v. Slovinsko[227] bylo konstatováno, že právní úprava těchto zákroků ze strany státu musí být dostatečně určitá a opodstatněná. V tomto případě se jednalo o sdílení dětské pornografie. Pachatel byl dopadnut na základě zjištění jeho dynamické IP adresy (IP adresa která je proměnná oproti statické) od poskytovatele internetového připojení. V rozsudku ve věci Bărbulescu proti Rumunsku došlo k porovnání, zda a do jaké míry lze očekávat, že soukromí jednotlivce bude respektováno a chráněno a zda

[221] Nils Muižnieks, „“How to ensure that the Internet remains an open and public forum for exercising freedom of opinion and expression and facilitating other human rights and fundamental freedoms" (Dublin Conference on Internet Freedom, Dublin: Commissioner for Human Rights, 2012). str. 1.

[222] Rada Evropy, ETS 5, European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 listopad 1950, uložena u Generálního sekretariátu Rady Evropy čl. 8.

[223] Copland v. the United Kingdon, 62617/00, rozsudek ESLP čtvrté sekce, ze dne 3.7.2007.; Bărbulescu v. Rumunsko, 61496/08, rozsudek ESLP velkého senátu, ze dne 5.9.2015.

[224] Viz kausa Cambridge Analytica - Carole Cadwalladr a Emma Graham-Harrison, „Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", The Guardian, viděno 16. květen 2021, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[225] Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě, Sdělení č. 104/2013 Sb. m. s., ze dne 23.12.2013.

[226] Benedik v. Slovinsko, 62357/14, rozsudek ESLP ze dne 24.4.2018. para. 137.

[227] Benedik v. Slovinsko, 62357/14, rozsudek ESLP ze dne 24.4.2018.

takovéto očekávání může mít rozhodující vliv na porušení čl. 8. V tomto případě se jednalo o případ zasílání soukromé korespondence ze zaměstnání. Stěžovatel byl seznámen s tím, že nesmí používat pracovní zařízení k zasílání soukromích zpráv, nebyl však vyrozuměn o tom, že tyto zprávy budou také monitorovány. V tomto případě soud shledal, že zaměstnavatel nemá právo monitorovat soukromé zprávy svých zaměstnanců. V Evropě v tomto ohledu nepanuje shoda a právní úprava je pouze sporadická. Tímto autor nechce vyloučit případy, kdy se obě strany domluvily a monitorování je například doplněno i v zákoně. Soud sám argumentoval tím, že ve skutkových okolnostech tohoto případu nedošlo k naplnění odůvodněného monitorování korespondence, jako by tomu bylo například v případě vyzrazování obchodních tajemství, nebo nežádoucích kyberaktivit.

Dále se může jednat o únik dat, které se týkají například GPS polohy, tyto informace jsou získávány ze zařízení, které obsahují polohový čip.[228] V těchto případech ESLP řešilo přípustnost využití těchto dat.[229] Dále se může jednat o použití odposlechů telefonických hovorů.[230] S ohledem na použití těchto dat pro účely trestních řízení nebo vyšetřování, kdy to národní legislativa dovoluje, je tento zásah do těchto lidských práv opodstatněn. Je však patrné, že jakmile se zásah odchýlí svým skutkovým dějem od okolností, které by zakládaly opodstatněný zásah do lidských práv, je poté stát za tento přístup odpovědný.[231]

3.2.2. Hromadné sledování

V návaznosti na ochranu soukromí je problémem moderního světa také hromadné sledování. Tato praktika vnikla na povrch světa po whistleblowingu Edwarda Snowdena. Hromadné sledování je často spojováno s porušením práva na soukromí. Hromadnému sledování se, mimo jiné ESLP věnoval ve svém nedávném rozsudku velkého senátu ESLP ve věci Big Brother Watch v. UK.[232] Tento rozsudek, mimo to že se vyjadřuje k legálnosti hromadných sledování, vysvětluje, jak k takovému sledování může docházet.

Pro pochopení tohoto rozsudku je podstatné, že chování dat na internetu není přímočaré. Povaha internetu a přenosu packetů nejde přímou cestou jako jiné telekomunikační metody. Data

[228] Raed. S. A. Faqir, „The use of Technology of Global Positioning System (GPS) in Criminal Investigation & Right to Privacy under the Constitution and Criminal Legislations in Jordan : Legal Analysis Study", *Revue internationale de droit pénal* 84, č. 3–4 (2013): 433–62, https://doi.org/10.3917/ridp.843.0433. str. 1.
[229] Press unit, „Personal data protection - Factsheet" (European Court of Human Rights, 2021). str. 2.
[230] Press unit. str. 3.
[231] Press unit. str. 3.
[232] Big Brother Watch and others v. the United Kingdom, 58170/13, 62322/14 a 24960/15 rozsudek ESLP velkého senátu, ze dne 25.5.2021.

si hledají nejlevnější a nejrychlejší cestu.[233] S ohledem na to, že většina internetu je poskytována a v držení největších firem jako jsou Google a Yahoo a jiné, se stává, že data odeslaná z Evropy budou určitý okamžik procházet přes území USA. Právní úprava USA dovoluje sledování dat na internetu v rámci ochrany veřejnosti před teroristickými útoky.[234] USA mohla při své činnosti dostat do svého držení údaje o uživatelích, kteří se ani na území nemuseli nacházet. Upozornění na různé programy americké vlády přišlo právě od Edwarda Snowdena. Tyto programy fungují na bázi vyhledávání klíčových emailových adres a v těchto adresách poté vyhledávají klíčová slova. Tato data mohou, ale nemusí být v konečné fázi přezkoumávaná člověkem, na ostatních úrovních přezkum probíhá pouze na základě algoritmů.

Závěrem soudu je, že hromadné sledování není obecně zakázané a apriori neporušuje právo na soukromí (tzv. Weber kritéria).[235] Nedostatečná právní úprava a nedostatečný dohled nad správou osobních údajů, které se mohou v této zadržené a sledované komunikaci vyskytovat, mohou toto porušení založit.

Problémem hromadného sledování je však to, že jednání na území jednoho státu může procházet teritorii jiných států, a to bez úmyslu konajícího jednotlivce. To může přinášet problémy s určením teritoriality a v případě, kdy například stát mimo EU poruší práva jednotlivce na svém území, například zadržením jeho komunikace, mohou nastat problémy s určením rozhodného práva.

3.2.3. Pozitivní závazek státu

Spolu s tím, že se stát má něčeho zdržet dochází soudní praxe i k případům, kdy státu stanoví pozitivní závazek.[236] V případě K.U. proti Finsko došlo v roce 1999 k zveřejnění reklamy (inzerátu) na webových stránkách, na kterých bylo jméno 12letého chlapce bez jeho souhlasu.[237] Tato reklama lákala na seznámení s tímto chlapcem a naznačovala sexuální tématiku. O této reklamě se žalobci dozvěděli až v okamžiku, kdy se na tuto reklamu ozval zájemce. Policie požádala soud, aby vydal rozhodnutí, aby vlastník webové stránky poskytl údaje o inzerentovi reklamy.[238] Soud však tento návrh zamítl s tím, že neexistuje právní úprava, která by soudu toto rozhodnutí dovolila vydat. Úprava v národním právu povolovala policii

[233] Big Brother Watch and others v. the United Kingdom, 58170/13, 62322/14 a 24960/15 rozsudek ESLP velkého senátu, ze dne 25.5.2021. para. 14.
[234] Big Brother Watch and others v. the United Kingdom, 58170/13, 62322/14 a 24960/15 rozsudek ESLP velkého senátu, ze dne 25.5.2021. para. 23.
[235] Big Brother Watch and others v. the United Kingdom, 58170/13, 62322/14 a 24960/15 rozsudek ESLP velkého senátu, ze dne 25.5.2021. para. 341.
[236] „K.U. v. FINLAND", 2872/02, rozsudek ESLP, čtvrtá sekce, ze dne 2.12.2008..para. 46.
[237] „K.U. v. FINLAND", 2872/02, rozsudek ESLP, čtvrtá sekce, ze dne 2.12.2008. para 7.
[238] „K.U. v. FINLAND", 2872/02, rozsudek ESLP, čtvrtá sekce, ze dne 2.12.2008. para. 10.

použít informace od poskytovatelů těchto služeb jen v případě určitých přestupků, nebo trestných činů. Po podání stížnosti k ESLP soud vyhodnotil, že ačkoliv čl. 8 (ochrana soukromí) slouží k ochraně jednotlivců proti zásahu státu, toto ale nestačí k tomu, aby stát přinutil k zdržení se takového jednání. Navíc k tomuto primárnímu závazku zdržet se jednání zde může být také pozitivní závazek státu vlastní efektivnímu respektování rodinného a soukromého života. Tento pozitivní závazek může spočívat v přijetí nástrojů, které by byly upraveny k zajištění respektu osobního života. Stát tedy může být odpovědný za nepřijetí národní legální úpravy. Tento judikát nám prezentuje situaci, že nejenom pouhé konání, ale i nekonání může být porušením práva. Svou povahou se dá uplatnit i na kyberprostor, i když aplikace je univerzální, bez ohledu na médium.

3.2.4. Svoboda projevu

V kyberprostoru dochází nejčastěji k porušování práva na soukromí a práva svobody projevu. S ohledem na jednoduchost a přístup k internetu mohou být některé projevy omezeny a tento přístup je i celosvětově vítán. Oblasti, kde se regulace státu předpokládá a vítá, jsou dětská pornografie, hate speech, pomluva, pobuřování, nepřátelské chování nebo násilí.[239] Stát poté přistupuje k přijetí legislativy, která by toto nebezpečné chování měla odstranit.

ESLP ve své judikatuře již rozhodoval v řadě případů, kdy byl stát shledán odpovědným za své chování na internetu. Jedná se spolu s výše zmíněnými i o ochranu osobních údajů, právo duševního vlastnictví, přístup k informacím a zablokování přístupu k internetu.

Svoboda projevu byla řešena v případu Magyar Tartalomszolgáltatók Egyesülete a Index.hu Zrt v. Maďarsko.[240] V tomto případu se jednalo o vydávání vulgárních a útočných komentářů na webových stránkách. Stěžovatelé byli internetovými poskytovateli a také zpravodajským webem. Maďarský soud je nejdříve shledal vinnými za to, že na svých stránkách tyto komentáři ponechali. Výsledkem bylo shledání, že stěžovatelé nejsou odpovědní za obsah, který je vkládán uživateli. V tomto případě by se jednalo o porušení čl. 10 také v případě, kdy by došlo k odstranění nevhodných komentářů. Opačné je v případě např. schvalování genocidy, při kterém může dojít k individuální trestní odpovědnosti.

V případě, že proběhne DDoS útok na webovou stránku, která například informuje o průběhu voleb[241,242] (v případě ČR by to byly stránky Českého statistického úřadu), toto jednání

[239] Research Division, „Internet: case-law of the European Court of Human Rights" (European Court of Human Rights, 2011), http://www.echr.coe.int/. str. 54.
[240] Magyar Tartalomszolgáltatók Egyesülete a Index.hu Zrt v. Maďarsko, 22947/13, rozsudek ESLP čtvrté sekce, ze dne 2.5.2016.
[241] Research Division, „Internet: case-law of the European Court of Human Rights". str. 32.

bude přičteno podle kapitoly 2. cizímu státu, tento stát může být *inter alia* odpovědný za porušení čl. 10 Úmluvy. Jednalo by se o znemožnění přístupu k informacím, které je také čl. 10 chráněno.

3.2.5. Zásah státu

Zásah státu, jehož následkem dojde k omezení lidských práv, musí být vždy odůvodnění a opodstatněný. Obecně by stát měl co nejméně zasahovat do omezování svobody projevu na internetu.[243] Ve 21. století je mnohem důležitější zaručit ochranu i v různých nových oblastech, jako je např. kyberprostor. Internet se stal novým fórem pro mnoho lidí, kteří tak využívají své právo na svobodu projevu právě tam. Ať již se jedná o sociální média, nebo různé diskusní stránky nebo novinové stránky, na všech by měla být zaručena stejná úroveň lidských práv.

Dle judikatury ESLP se zkoumají tři faktory. Zásah musí být stanoven zákonem, musí být sledován legitimní cíl, a musí se jednat o zásah nezbytný v demokratické společnosti.[244] Jedná se o již běžnou praxi ESLP. Ve věci legitimního omezení určitých práv se např. vyjádřil v rozsudku ve věci Yildirim v. Turecko,[245] kde došel k závěru, že určitá omezení lze aplikovat, ale nelze je pojmou obecně, nýbrž zaměřené na obsah. V tomto případě se jednalo o pana Yildrima, který si založil webovou stránku pomocí Googlesites. Soud poté došel k závěru, že tato stránka porušuje určitý turecký zákon a rozhodl, že stránku zruší. Nebylo však možné zrušit přístup z Turecka jen na tuto specifickou stránku. Došlo tedy k rozhodnutí, že bude přerušen přístup na všechny stránky tohoto typu na stejném hostingu. Turecko pak bylo označeno za odpovědné za porušení přístupu k informacím.

3.2.6. Právo na život

Dalším z lidských práv, o kterém lze uvažovat, že musí být chráněno univerzálně, je právo na život, jak je uvedeno v čl. 2 Úmluvy. Na úvod lze shrnout, že ESLP ve své rozhodovací praxi zatím nedošlo k závěru, že se právo na život může uplatit i v kyberprostoru, jinými slovy, že pomocí kyberprostoru může být stát odpovědný za usmrcení osoby.

V tomto případě lze analogicky postupovat a argumentovat např. rozhodnutím Isayeva, Yusupova a Bazayeva v. Rusko.[246] V tomto případě šlo o bombový útok na civilní konvoj. Při

[242] Rona a Aarons, „State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace". str. 10.
[243] Research Division, „Internet: case-law of the European Court of Human Rights". Str. 7.
[244] Viz čl. 10 Úmluvy.
[245] Ahmet Yildirim v. Turkey, 3111/10, rozhodnutí ESLP, 18.12.2012.
[246] Isayeva, Yusupova a Bazayeva v. Rusko, 57947/00, 57948/00 a 57949/00, rozsudek ESLP bývalá první sekce, ze dne 6.7.2005.

tomto útoku došlo k usmrcení několika osob.[247] Útok byl proveden pomocí letadlového náletu na konvoj vozidel civilistů, kteří se pokoušeli dostat k humanitární pomoci. Ochrana života je jednou z hlavních povinností státu dle tohoto článku. Jednalo se o útok spáchaný armádou, a tedy přičitatelný státu.

Stát tedy může být odpovědný za usmrcení jednotlivců, pokud se jedná vojenský útok. V tomto duchu lze argumentovat, že v případě usmrcení nehraje roli použitý prostředek, nebo zbraň. Lze se tedy domnívat, že v případě situací, kdy kyberútok povede k usmrcení osoby, např. vyřazením z provozu elektrické sítě, která zásobuje nemocnice, bude možné považovat tento čin i za porušující čl. 2 Úmluvy.

3.2.7. Ochrana lidských práv v Tallinnském manuálu

Talinský manuál 2.0 obsahuje téměř totožná pravidla jako která jsou v mezinárodních paktech týkající se ochrany lidských práv, a to v části 6 články 34-38.[248] Tato pravidla se shodují s přístupem zmíněným výše. V pravidlu č. 34 stanoví, že se lidská práva aplikují a osoby požívají tato práva ve stejné míře jak v kyberprostoru,[249] tak v off-line světě. Přičitatelným jednáním ve výše zmíněných případech je také porušení práva na soukromí na příkaz státu soukromou entitou, a to v případě, kdy například stát nemá infrastrukturu ke spáchání tohoto protiprávního jednání sám. Tallinnský manuál poté pracuje s teoretickými příklady, kdy se například jedná o automatizované zkoumání toku dat pro účely plynulého provozu sítí, tento monitoring je pak považován buďto jako že není porušením soukromí, anebo že je považován za obhájitelný. Tallinnský manuál 2.0. uvádí tyto principy i pro státy, které nejsou součástí Rady Evropy a neaplikují se na ně regionální evropské úmluvy o ochraně lidských práv.

Tallinnský manuál pak ilustruje porušení pomocí příkladů. Dle expertů může docházet k porušení lidských práv ze strany státu například blokování přístupu jednotlivých IP adres k obsahu specifických webových stránek,[250] blokování odchozích emailů, filtrování obsahu na internetu. Tyto aktivity by pak dosáhly na porušení přístupu k informacím, které obsahuje svoboda projevu.[251]

[247] Isayeva, Yusupova a Bazayeva v. Rusko, 57947/00, 57948/00 a 57949/00, rozsudek ESLP bývalá první sekce, ze dne 6.7.2005. para. 23.
[248] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2. vyd. (Cambridge: Cambridge University Press, 2017), https://doi.org/10.1017/9781316822524.
[249] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. str. 188.
[250] Může se jednat také o tvz. Geoblocking.
[251] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. str. 188.

3.2.8. Shrnutí

Ochrana lidských práv v judikatuře ESLP, která by se aplikovala i na kyberprostor v případě ochrany určitých lidských práv, již existuje a lze tedy shrnout, že stát může být odpovědný za své protiprávní jednání spočívající v porušování některých lidských práv i v kyberprostoru.

Právo na soukromí je řešeno s ohledem na aktivitu jednotlivců na internetu a jejich důvodný předpoklad, že jejich soukromí je zde také zachováno. K tomuto došel ESLP v případu Bărbulescu proti Rumunsku,[252] kde došlo k určení, že i zásah do soukromích zpráv, i přes to, že jsou zasílány z pracovního počítače, podléhají ochraně soukromí. V případu Benedik v. Slovinsko[253] došel soud k závěru, že i v případech trestního vyšetřování musí být sledování a identifikace pachatele na internetu opřena o právní úpravu, která naplňuje opodstatněnost v demokratické společnosti. V případu hromadného sledování občanů pomocí elektronického sledování, Big Brother Watch v. UK,[254] došel soud k závěru, že takovéto sledování bylo porušením čl. 8 ze strany Velké Británie, s ohledem na neurčitou právní úpravu a také nedostačenou ochranu (safeguards) s nakládáním se získanými daty.

Státu je v této souvislosti přičítána odpovědnost za porušení jeho pozitivního závazku v kyberprostoru, tento závazek může spočívat v pasivitě státu se stíháním zločinů. V případu K.U. v. Finsko došlo k shledání, že i na internetu má stát povinnost zajistit právní úpravu tak, aby mohlo dojít k trestání určitých zločinů, v tomto případě šlo o přijetí právní úpravy, aby mohlo dojít k identifikaci pachatele.

Svoboda projevu je pak rozšířena i v ochraně vyjadřování se na internetových fórech, hate speech, odmítnutí přístupu k informacím aj. V případě Magyar Tartalomszolgáltatók Egyesülete a Index.hu Zrt v. Maďarsko[255] se soud zabýval odpovědností provozovatelů internetových stránek a zpravodajského webu, zda odpovídají za vulgární komentáře na svých platformách. Soud došel k závěru, že provozovatel nemůže být odpovědný za ponechání těchto komentářů (to nevylučuje individuální odpovědnost). V případu Yildirim v. Turecko[256] soud došel k závěru, že určité omezení na základě zákona a přístupu k informacím je možné, nikoliv však omezení plošně a nerozlišující. V tomto případě bylo Turecko shledáno odpovědným za zablokování přístupu k všem stránkám na podpoře Googlesites. Dle některých autorů je také

[252] Bărbulescu v. Rumunsko, 61496/08, rozsudek ESLP velkého senátu, ze dne 5.9.2015.
[253] Benedik v. Slovinsko, 62357/14, rozsudek ESLP ze dne 24.4.2018.
[254] Big Brother Watch and others v. the United Kingdom, 58170/13, 62322/14 a 24960/15 rozsudek ESLP velkého senátu, ze dne 25.5.2021.
[255] Magyar Tartalomszolgáltatók Egyesülete a Index.hu Zrt v. Maďarsko, 22947/13, rozsudek ESLP čtvrté sekce, ze dne 2.5.2016.
[256] Ahmet Yildirim v. Turkey, 3111/10, rozhodnutí ESLP, 18.12.2012.

možné, že k porušení čl. 10 Úmluvy povede např. vyřazení přístupu k stránkám poskytujícím informace o průběhu voleb.

Právo na život nebylo doposud v rozhodovací praxi ESLP řešeno s přihlédnutím na kyberprostor. Lze ale argumentovat, že pokud by došlo k prokazatelnému porušení čl. 2 Úmluvy skrze kyberprostor, dal by se analogicky použít rozsudek ve věci Yusupova a Bazayeva v. Rusko,[257] kdy došlo k útoku na civilní konvoj a ztrátám na civilních životech.

Tallinnský manuál na druhou stranu vychází z univerzálního pojetí lidských práv a jejich ochrany i v kyberprostoru. Tallinnský manuál přiznává ochranu v kyberprostoru všem, a to ve všech lidských právech.

Lze tedy shrnout, že v případech zmíněných výše může dojít k přičitatelnosti státu za jeho jednání, konáním či opomenutím, v kyberprostoru. Může se jednat, nikoliv však výlučně o případy zamítnutí přístupu k jednotlivým webovým stránkám nebo o případy nepřijetí nutných právních norem. Jednalo by se tedy o čl. 1 ve spojení s čl. 4 ARSIWA.

[257] Isayeva, Yusupova a Bazayeva v. Rusko, 57947/00, 57948/00 a 57949/00, rozsudek ESLP bývalá první sekce, ze dne 6.7.2005.

Závěr

Kyberprostor je již součástí každodenního života velké části obyvatel naší planety. Téměř každý používá internet, který je jen pouhou částí širokého kyberprostoru. Setkáváme se s ním denně, když zapneme televizi, někomu zavoláme, připojíme se k bezdrátové síti internetu přes své mobilní zařízení. Každý den jsme svědky kybernetických útoků po celém světě, o kterých se také dozvídáme z kyberprostoru. Kyberprostor však není jen to, co je hned na první pohled patrné. Do kyberprostoru můžeme zařadit i to, že nám proudí elektrický proud do domácností, že máme dostatek tepla a že nám správně pracují sítě, které řídí provoz kritické infrastruktury. Kyberprostor nás obklopuje, jen těžko můžeme na světě najít místo, kde bychom od něj byli úplně odtrženi.

Technologický vývoj jde kupředu a s ním i možnosti, se kterými můžeme do kyberprostoru vstupovat, měnit jej anebo na něj útočit. Ačkoliv nástup informačních technologií můžeme pozorovat již dlouhodobě, mezinárodní právo na něj reaguje opožděně v době, kdy již mohou být cílem útoků téměř všichni uživatelé internetu a téměř všechny státy. V dnešní době tak můžeme pozorovat vznik různých počinů akademiků, mezinárodních organizací i jednotlivých států, které se snaží podchytit problémy spojené s kyberprostorem alespoň přijetím závazných norem chování. Jedná se tak zejména o dva Tallinnské manuály, konference OEWG, směrnice EU a národní zákony o elektronické komunikaci a ochraně kritické infrastruktury. Stále ale nepanuje všeobecná shoda v tom, zda se všechny aspekty a dosavadní normy mezinárodního práva aplikují na kyberprostor, či nikoliv. V jednom může být ale jasno, obyčejové principy mezinárodního práva jsou obecně přijímány jako platné i v kyberprostoru.

Cílem této práce bylo potvrdit, nebo vyvrátit hypotézu, že mezinárodní právo lze aplikovat v kyberprostoru, a to v oblasti kolektivní bezpečnosti a lidských práv. Tato práce nedošla k jednoznačnému prokázání, nebo vyvrácení této teze, ale došla k dílčím výsledkům, které stanovují, že mezinárodní právo je mezinárodním společenstvím považované v určitém rozměru za platné i v kyberprostoru. V rámci rešerše byly v této práci představeny i nové poznatky v rámci právní úpravy kyberprostoru. Primárně ale došlo ke zkoumání, zda se v těchto zmíněných oblastech mezinárodní právo již aplikuje, nebo by se aplikovat mohlo, s ohledem na dané normy, které tyto problematiky upravují.

Prvním dílčím závěrem je možnost porušení zákazu použití síly v kyberprostoru. Tato práce jednoznačně prokázala, že existuje konsensus mezi některými státy mezinárodního společenství, který vychází z práce Tallinnského manuálu. Použití síly bude považováno za porušení čl. 4 odst. 2 Charty OSN pouze v případě, kdy dojde k naplnění určitých aspektů tohoto daného kyberútoku. Jedná se převážně o bezprostřednost, zapojení vojska, závažnost a

invazivnost. Státy jako Francie, Spojené království a Nizozemsko jsou toho názoru, že zde neexistuje omezení, které by nedovolovalo vztáhnout tyto normy i na použití síly. V kapitole 3.1.4. došlo k představení všech uvedených faktorů. Autor této práce je toho názoru, že v rámci teorie Effects principle je namístě, aby státy, alespoň prozatím, aplikovaly tato ustanovení i na kyberprostor. O použití síly by se mohlo jednat i v případech podpory organizovaných skupin, kdy stát dodává finance k provozování kyberútoků, nebo tyto skupiny řídí.

Dále došlo k rozdělení a určení rozdílu mezi ozbrojeným útokem, agresí a použití síly. Ozbrojený útok je možné hodnotit podobně, jako je tomu v případě použití síly. Je však sporné, zda mezinárodní společenství přijme určitý kyberútok za ozbrojený útok. V rozhodovací praxi soudů jsme se zatím nesetkali s rozsudkem, který by jednotlivé porušení v kyberprostoru řešil. Limity ozbrojeného útoky jsou stanoveny nejen rozsudkem ve věci Nicaragua, ale také rozsudkem Ropné plošiny a dále v teoretických přístupech Tallinnského manuálu. Naplnění těchto limitů může být považováno taktéž podle kapitoly 3.1.4, s tím, že tento následek musí dosahovat vyšší úrovně, nežli je tomu u pouhého použití síly. V rozhodovací praxi MSD však nebyla otázka použití síly, ani ozbrojeného útoku v kyberprostoru řešena. Práce tedy nedochází v tomto případě k jednoznačnému závěru, zda lze shledat stát odpovědným za ozbrojený útok v kyberprostoru. Identifikace ozbrojeného útoku je vitální převážně s možností použití sebeobrany.

Agrese v mezinárodním právu kolektivní bezpečnosti je stejně tak řešena v kapitole 3.1.6. Dochází zde k polemice o tom, zda lze dojít k závěru, že v jakékoliv intenzitě (v intenzitě ozbrojeného útoku nebo použití síly) lze shledat stát odpovědný za spáchání agrese v kyberprostoru, nebo skrze něj. Nedostatek jednotlivých názorů nebo praxe států vedl k závěru, že nelze hypotézu v tomto bodě potvrdit, ani vyvrátit. Vždy bude převážně záležet na konkrétním případu kyberútoku. Demonstrativní výčet v rezoluci valného shromáždění a jeho rozbor nevede k dostatečnému přesvědčení, že by byl takový kyberútok považován za zločin agrese.

Dalším dílčím závěrem je možnost porušení lidských práv v kyberprostoru. Kapitola 3.2 již jednoznačně potvrdila praxi ESLP, který dává státům pozitivní i negativní závazek ochrany lidských práv, které vztahuje v tomto případě i na internet. Jednotlivé mezinárodní smlouvy, které chrání lidská práva, vycházejí z obdobných principů a nejsou ve svém textu omezené na prostředky, kterými by mělo dojít k takovému porušení. Jedná se převážně o porušení svobody slova, ochrany soukromí a práva na život. Právo na soukromí je řešeno nejen s přihlédnutím ke kyberprostoru jako takovému, ale také s přihlédnutím k problematice hromadného sledování. Ochrana soukromí byla vyslovena v řadě rozhodnutí, která zabezpečují, že jednotlivci jsou před

zásahy státu chráněni i v kyberprostoru. Hromadné sledování nelze provádět bez dostatečného důvodu a zmocnění. Právo na soukromí obsahuje převážně ochranu komunikace, ale i ochranu soukromí v rámci užití svého obrazu nebo údajů.

Svoboda slova je chráněna taktéž i s ohledem na kyberprostor, a to v různých sférách. Jedná se o stíhání jednotlivců za překročení únosné úrovně vyjadřování na internetu, hate speech, anebo také o zamítnutí přístupu k informacím. ESLP například shledal, že stát může být odpovědný za nedostatečnou ochranu svobody projevu, nebo také, že nemůže trestat poskytovatele webových stránek za příspěvky na těchto stránkách. Autor tedy považuje aplikaci lidských práv v těchto dvou oblastech za nespornou.

Právo na život v kyberprostoru nebylo doposud v rozhodovací praxi ESLP řešeno, jedná se o povinnost chránit lidský život. V této práci došlo k polemice nad možností užití analogie s konvenčním útokem. S ohledem na to, že práce pracuje s myšlenkou, že použití síly je v kyberprostoru možné, bude tedy možné odebrat někomu právo na život i v kyberprostoru. Může se tak jednat o případy, kdy v nemocnici dojde k vyřazení elektřiny, které povede k úmrtí osob, a to následkem kyberútoku přičitatelného státu. Může se tak jednat i o menší intenzitu útoku, v smyslu úmrtí jedné osoby. Tento dílčí výrok však autor nepovažuje za dostatečně prokázaný s ohledem na nedostatek rozhodovací praxe a pozice jednotlivých aktérů mezinárodního společenství.

Dle názoru autora však není možné pohlížet na platné právo jako na něco, co dostatečně pokryje právo kyberprostoru. Jedná se však o možnost vyplnění vakua, které přesně zapadá do teorie Effects principle. Tento postup však nebude dále udržitelný, jak se autor této práce pokusil na řadě míst poukázat, s ohledem na vývoj technologií. Stávající stav tedy považuji za stav přechodný, který by měl vést k tomu, že se přijme nová právní úprava, která zabezpečí aplikaci práva bezpodmínečně. S četnějším výskytem kyberútoků dojde k odhalení slabin aplikace stávajících norem, např. v oblasti umělé inteligence, a ta se tak stane nedostatečnou.

Je potřeba rozlišovat, zda k protiprávnímu jednání došlo v kyberprostoru (kdy jeho počátek i následek je v kyberprostoru), nebo bylo použito kyberprostoru jako nosiče (útok z kyberprostoru s následkem v reálném světě), nebo možné kombinace obou. Dle názoru autora je takovéto dělení jedním z možných postupů, kam by měla mezinárodní úprava směřovat, neboť takovéto rozdělení pomůže na jednu stranu lépe identifikovat již platnou normu, kterou je možné aplikovat, nebo povede k identifikace právního vakua, které bude potřeba zaplnit.

Co se týče přičitatelnosti jednotlivých protiprávních jednání, tak v tomto případě se autor domnívá, že se bude jednat o otázku striktně technickou, neboť nelze zlehčovat míru důkazů na úkor dosažení identifikace pachatele. Státy se musí nejprve soustředit na vývoji kybernetických

bezpečnostních systémů, aby bylo možné předcházet jednotlivým útokům, nebo je alespoň rychleji likvidovat.

V rámci rešerše došlo k identifikaci možných problémů, které vyvstávají z úpravy kyberprostoru. Jedná se převážně o problematiku teritoriality, protože jak bylo poukázáno v kapitole 3.2.2, jednání v kyberprostoru se může dostávat, i nevědomky, do teritoria jiného státu. Dále pak může jít o již zmíněnou problematiku aplikace jednotlivých mezinárodních norem na kyberprostor. Posledním problémem, který je zmíněn v kapitole 1.2 je fakt, že neexistuje jednotná definice kyberprostoru. To může přinášet značné potíže s postupným vývojem právní úpravy na mezinárodní úrovni.

Závěrem je nutné podotknout, že přes všechny snahy mezinárodních organizací a různých států, nejsou zbylé státy ochotny investovat značné peníze do vývoje nových instrumentů na ochranu kyberprostoru. Jedná se také z části o problematiku vyšších nároků a due diligence. Státy se rovněž mohou obávat odpovědnosti vůči vlastnímu obyvatelstvu. Nevole států k implementaci nových ochranných prostředků v kyberprostoru je však neudržitelná, protože, jak v současné době vidíme, kybernetických útoků stále přibývá.

Seznam použitých zdrojů

Seznam použité literatury

Odborné knihy

- Bílková, Veronika. *Mezinárodní humanitární právo.* Vyd. 1. Beckova edice právní instituty. Praha: C.H. Beck, 2010.
- ———. *Mezinárodní humanitární právo : vznik, vývoj a nové výzvy.* Studie z lidských práv Studies in human rights: č. 9 = vol. 9. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2015.
- ———. *Úprava vnitrostátních ozbrojených konfliktů v mezinárodním humanitárním právu.* 1. vyd. Prameny a nové proudy právní vědy: No. 37. Praha: Eva Rozkotová - IFEC, 2007.
- Blunt, P. J. „How Cyberspace Changes International Conflict". In *Reprogramming the World: Cyberspace and the Geography of Global Order*, Creative commons. E-International Relations, b.r. https://www.e-ir.info/pdf/80610.
- Crawford, James. *State Responsibility : The General Part*. Cambridge Studies in International and Comparative Law. New York: Cambridge University Press, 2013.
- Čepelka, Čestmír. *Mezinárodní právo veřejné.* Vyd. 1. Právnické učebnice. Praha: Beck, 2008.
- Dinstein, Yoram. *War, aggression, and self-defence.* 5th ed. Cambridge University Press, 2012.
- Dinstein, Yoram, a Arne Willy Dahl. *Oslo Manual on Select Topics of the Law of Armed Conflict : Rules and Commentary*. Springer Nature, 2020. https://doi.org/10.1007/978-3-030-39169-0.
- Erbschloe, Michael. *Trojans, Worms, and Spyware : A Computer Security Professional's Guide to Malicious Code*. Amsterdam: Butterworth-Heinemann, 2005.
- Expert Meeting. Autonomous weapon systems: Technical, military, legal and humanitarian aspects. Geneva: ICRC, 2014.
- Gibson, William. *Neuromancer.* 28th print. New York: Ace Books, 1984.
- Henckaerts, Jean-Marie, a Louise Doswald-Beck. *Customary International Humanitarian Law*. Cambridge: Cambridge University Press, 2005.
- Chen, Thomas M. *Cyberterrorism after Stuxnet*. US Army War College: Strategic Studies Institute, 2014.

- Kremer, Jan-Frederik, a Benedikt Müller, ed. *Cyberspace and international relations : theory, prospects and challenges.* Berlin: Springer, 2014.
- Lindsay, Jon R., Tai Ming Cheung, a Derek S. Reveron, ed. *China and cybersecurity : espionage, strategy, and politics in the digital domain.* [First edition]. Oxford: Oxford University Press, 2015.
- Nandal, Priyanka. *Malware Detection*. Hamburg: Anchor Academic Publishing, 2018.
- National Research Council. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington, DC: The National Academies Press, 2010. https://doi.org/10.17226/12997.
- Ondřej, Jan. *Právní režimy mořských oblastí : srovnání s kosmem a Antarktidou.* Monografie. Praha: Vydavatelství a nakladatelství Aleš Čeněk, 2017.
- Potočný, Miroslav. *Mezinárodní právo veřejné : zvláštní část.* 6., Doplněné a Rozšířené vydání. Právnické učebnice. Praha: C.H. Beck, 2011.
- Provost, René. State Responsibility in International Law. Library of Essays in International Law. Oxon, England: Routledge, 2016.
- Ragazzi, Maurizio. „The Examples of Obligations Erga Omnes Given by the International Court in Its Dictum: (B) The Outlawing of Genocide". In The Concept of International Obligations Erga Omnes. Oxford: Oxford University Press, 2000. https://doi.org/10.1093/acprof:oso/9780198298700.003.0005.
- Roscini, Marco. *Cyber Operations and the Use of Force in International Law*. Oxford: OUP Oxford, 2014.
- Ruys, Tom. *„Armed Attack" and Article 51 of the UN Charter : Evolutions in Customary Law and Practice*. Cambridge Studies in International and Comparative Law. New York: Cambridge University Press, 2010.
- Security Council. „Actions with respect to threats to the peace, breaches of peace, and acts of aggression". In *Repertoire of the Practice of the Security Council*. New York: Department of Political and Peacebuilding Affairs, 2011.
- ———. „Actions with respect to threats to the peace, breaches of peace, and acts of aggression". In *Repertoire of the Practice of the Security Council: 22nd Supplement*. New York: Department of Political and Peacebuilding Affairs, 2019.
- Shakarian, Paulo. *Introduction to cyber-warfare : a multidisciplinary approach.* Waltham: Morgan Kaufmann Publishers, an imprint of Elsevier, 2013. https://doi.org/10.1016/C2012-0-06618-5.

- Sharp, Walter Gary. *Cyberspace and the Use of Force*. United States of America: Aegis Research Corporation, 1999.
- Shipley, Todd G. *Investigating internet crimes : an introduction to solving crimes in cyberspace.* Waltham: Syngress, 2014.
- Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press, 2013.
- ———. *The Use of Cyber Force and International Law*. *The Oxford Handbook of the Use of Force in International Law:* Oxford: Oxford University Press, 2015. https://doi.org/10.1093/law/9780199673049.003.0053.
- Schmitt, Michael N., a Brian T. O'Donnell. *Computer network attack and international law [electronic resource] / Michael N. Schmitt & Brian T. O'Donnell, editors.* International law studies: v. 76. Newport, R.I.: Naval War College, 2002.
- Staniforth, Andrew. „Chapter 17 - Securing Cyberspace: Strategic Responses for a Digital Age". In *Strategic Intelligence Management*, editoval Babak Akhgar a Simeon Yates, 213–23. Butterworth-Heinemann, 2013. https://doi.org/10.1016/B978-0-12-407191-9.00017-X.
- Sterling, Bruce. *The Hacker Crackdown : Law and Disorder on the Electronic Frontier*. Project Gutenberg Etext. Champaign, Ill: Project Gutenberg, b.r.
- Šturma, Pavel. *Casebook : výběr případů z mezinárodního práva veřejného.* 4. upravené vydání. Scripta iuridica: No. 8. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2019.
- *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2. vyd. Cambridge: Cambridge University Press, 2017. https://doi.org/10.1017/9781316822524.
- Trapp, Kimberley N. „Terrorism and the international law of state responsibility". In *Research Handbook on International Law and Terrorism*. Cheltenham, UK: Edward Elgar Publishing, 2020. https://www.elgaronline.com/view/edcoll/9781788972215/9781788972215.00010.xml.
- Ventre, Daniel. *Cyber Conflict : Competing National Perspectives*. London: Wiley-ISTE, 2012.

Odborné články

- Bastl, Martin, a Zuzana Gruberová. „Kyberprostor jako „pátá doména'? / Cyberspace as a ‚Fifth Domain′?" Vojenské rozhledy / Czech Military Review 22, č. 4 (1. leden 2013): 10–21.

- Benjamin, Edwards, Furnas Alexander, Forrest Stephanie, a Axelrod Robert. „Strategic aspects of cyberattack, attribution, and blame". Proceedings of the National Academy of Sciences of the United States of America 114, č. 11 (14. březen 2017): 2825–30.
- Blokker, Niels. „The Crime of Aggression and the United Nations Security Council ESSAYS IN HONOUR OF JOHN DUGARD: THE PROTECTION OF THE INDIVIDUAL IN INTERNATIONAL LAW". Leiden Journal of International Law 20, č. 4 (2007): 867–94.
- Boer, Lianne J. M. „Echoes of Times Past: On the Paradoxical Nature of Article 2(4)". Journal of Conflict and Security Law 20, č. 1 (2015): 5–26.
- Buchan, Russell, a Nicholas Tsagourias. „Special Issue: Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence". Journal of Conflict and Security Law 21, č. 3 (2016): 377–82.
- Bussel, Jennifer. „Cyberspace". In Britannica, 2. květen 2021. https://www.britannica.com/topic/cyberspace.
- Buttigieg, Jean. „The Common Heritage of Mankind : From the Law of the Sea to the Human Genome and Cyberspace", 2012. https://www.um.edu.mt/library/oar/handle/123456789/6883.
- Cassese, Antonie. „The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia". The European Journal of International Law, č. 18 (b.r.).
- Coeckelbergh, Mark. „Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability". Science and Engineering Ethics 26, č. 4 (1. srpen 2020): 2051–68. https://doi.org/10.1007/s11948-019-00146-8.
- Corn, Gary, a Eric Jensen. „The Use of Force and Cyber Countermeasures". Temple International & Comparative Law Journal 32, č. 2 (2018): 127–34.
- Denning, Dorothy E. „Stuxnet: What Has Changed?" Future Internet 4, č. 3 (ervenec 2012): 672–87. https://doi.org/10.3390/fi4030672.
- Deshmukh, Rashmi V., a Kailas K. Devadkar. „Understanding DDoS Attack & its Effect in Cloud Environment". Procedia Computer Science 49 (1. leden 2015): 202–10.
- Diakun-Thibault, Nadia. „Defining Cybersecurity". Technology Innovation Management Review, 10 2014.

- Donner, Marc. „Cyberassault on Estonia". IEEE Security & Privacy, Security & Privacy, IEEE, IEEE Secur. Privacy 5, č. 4 (ervenec 2007): 4–4. https://doi.org/10.1109/MSP.2007.78.
- Faqir, Raed. S. A. „The use of Technology of Global Positioning System (GPS) in Criminal Investigation & Right to Privacy under the Constitution and Criminal Legislations in Jordan : Legal Analysis Study". Revue internationale de droit pénal 84, č. 3–4 (2013): 433–62. https://doi.org/10.3917/ridp.843.0433.
- Foltz, Andrew C. „Stuxnet, Schmitt Analysis, and the Cyber ‚Use-of-Force´ Debate". JFQ 67, č. 4 (2012).
- Gaeta, Paola. „On What Conditions Can a State Be Held Responsible for Genocide?" European Journal of International Law 18, č. 4 (1. září 2007): 631–48. https://doi.org/10.1093/ejil/chm037.
- Ghandhi, Sandy. „Human Rights and the International Court of Justice The Ahmadou Sadio Diallo Case". Human Rights Law Review 11, č. 3 (2011): 527–55.
- Henckaerts, Jean-Marie. „Study on customary international humanitarian law: A contribution to the understanding and respect for the rule of law in armed confl ict". International Review of the Red Cross 87, č. 857 (březen 2005): 175–212.
- Herzog, Stephen. „Revisiting the Estonian Cyber Attacks : Digital Threats and Multinational Responses". Journal of Strategic Security 4, č. 2 (ervenec 2011): 49–60.
- „Iron Dome". In Wikipedia, 10. duben 2021. https://en.wikipedia.org/w/index.php?title=Iron_Dome&oldid=1016978699.
- Joyner, Christopher C., a Catherine Lotrionte. „Information Warfare as International Coercion: Elements of a Legal Framework". European Journal of International Law 12, č. 5 (1. prosinec 2001): 825–65. https://doi.org/10.1093/ejil/12.5.825.
- Kersting, Kristian. „Machine Learning and Artificial Intelligence: Two Fellow Travelers on the Quest for Intelligent Behavior in Machines". Frontiers in Big Data 1 (2018): 6. https://doi.org/10.3389/fdata.2018.00006.
- Krausova, Alzbeta. „Identification in Cyberspace". Masaryk University Journal of Law and Technology 2, č. 1 (2008): 83–96.
- Liu, Ian Yuying. „The due diligence doctrine under Tallinn Manual 2.0". Computer Law & Security Review: The International Journal of Technology Law and Practice 33, č. 3 (1. červen 2017): 390–95.

- Lukasik, Stephen J. „Protecting the global information commons". Telecommunications Policy 24, č. 6 (1. leden 2000): 519–31.
- Mansfield-Devine, Steve. „DDoS goes mainstream: how headline-grabbing attacks could make this threat an organisation's biggest nightmare". Network Security, č. 11 (1. listopad 2016): 7–13.
- Manzo, Vincent A. „Deterrence and escalation in cross-domain operations : where do space and cyberspace fit?", Strategic forum, č. 272 (2011).
- McGuffin, Chris, a Paul Mitchell. „On Domains: Cyber and the Practice of Warfare". International Journal 69, č. 3 (2014): 394–412.
- Murphy, Sean D. „Peremptory Norms of General International Law (Jus Cogens) and Other Topics: The Seventy-First Session of the International Law Commission". American Journal of International Law 114, č. 1 (2020): 68–86. https://doi.org/10.1017/ajil.2019.74.
- Nevers, Renée de. „NATO's International Security Role in the Terrorist Era". International Security 31, č. 4 (2007): 34–66.
- Payne, Thomas. „Teaching old law new tricks: Applying and adapting state responsibility to cyber operations". Lewis & Clark Law Review 20, č. 2 (2016): 683–715.
- Rona, Gabor, a Lauren Aarons. „State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace". Journal of National Security Law and Policy 8, č. 3 (2015): 503–30.
- Shackelford, Scott J. „From Nuclear War to Net War: Analogizing Cyber Attacks in International Law". Berkeley Journal of International Law 27, č. 1 (2009): 192–252.
- ———. „The Law of Cyber Peace". Chicago Journal of International Law 18, č. 1 (2017): 1–47.
- Schmitt, Michael N. „The Use of Cyber Force and International Law", 2021, 22.
- Stahl, William M. „The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity". Georgia Journal of International and Comparative Law, č. 40 (2011): 247–74.
- Tanyildizi, M. Emrah. „STATE RESPONSIBILITY IN CYBERSPACE: THE PROBLEM OF ATTRIBUTION OF CYBERATTACKS CONDUCTED BY NON-STATE ACTORS." Siber Ortamda Devletlerin Sorumluluğu: Devlet Dışı Aktörlerce Gerçekleştirilen Siber Saldırıların Atfedilebilirliği Meselesi. 8, č. 14 (erven 2017): 119–76.

- Trautman, Lawrence J., a Peter C. Ormerod. „Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things". University of Miami Law Review 72, č. 3 (2017): 761–826.
- Urbanová, Kristýna. „The Kampala Agreement on Crime of Aggression and Responsibility for Cyber-Attacks". Czech yearbook of public & private international law = Česká ročenka mezinárodního práva veřejného a soukromého/ Česká společnost pro mezinárodní právo, č. 6 (2015): 103–14.
- Zeb, Khan, Owais Baig, a Muhammad Kamran Asif. „DDoS attacks and countermeasures in cyberspace." 2015 2nd World Symposium on Web Applications & Networking (WSWAN), leden 2015, 1–6.

Rozsudky soudů

a. Stály rozhodčí soud v Hague

- Island of Palmas Case (or Miangas), United States v Netherlands, Award, (1928) II RIAA 829, ICGJ 392 (PCA 1928), 4th April 1928.

b. Evropský soud pro lidská práva

- Ahmet Yildirim v. Turkey, 3111/10, rozhodnutí ESLP, 18.12.2012.
- Bărbulescu v. Rumunsko, 61496/08, rozsudek ESLP velkého senátu, ze dne 5.9.2015.
- Benedik v. Slovinsko, 62357/14, rozsudek ESLP ze dne 24.4.2018.
- Big Brother Watch and others v. the United Kingdom, 58170/13, 62322/14 a 24960/15 rozsudek ESLP velkého senátu, ze dne 25.5.2021.
- Copland v. the United Kingdon, 62617/00, rozsudek ESLP čtvrté sekce, ze dne 3.7.2007.;
- Drozd and Janousek v. France and Spain, 12747/87, rozsudek ze dne 26. 06. 1992.
- Isayeva, Yusupova a Bazayeva v. Rusko, 57947/00, 57948/00 a 57949/00, rozsudek ESLP bývalá první sekce, ze dne 6.7.2005.
- „K.U. v. FINLAND", 2872/02, rozsudek ESLP, čtvrtá sekce, ze dne 2.12.2008.
- Magyar Tartalomszolgáltatók Egyesülete a Index.hu Zrt v. Maďarsko, 22947/13, rozsudek ESLP čtvrté sekce, ze dne 2.5.2016.

c. 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 Reports 2007.
- Corfu Channel Case (United Kingdom v. Albania); Assesment of Compensation". ICJ Merits 15 XII 49, 15. prosinec 1949.

- Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. Unite States of America). Merits, Judgement. I.C.J. Reports 1986.
- Oil Platforms, Iran v United States, Judgment, merits, ICJ GL No 90, 2003

d. Soudní tribunál pro bývalou Jugoslávii

- Prosecutor v. Dusko Tadić. ICTY Case No. IT-94-1-T, Trial Chamber, 7 May 1997.

Právní předpisy

- Ústava České republiky č. 1/1993 Sb., Ústava.
- Zákon č. 240/2000 Sb., o krizovém řízení (Krizový zákon).
- Zákon č. 40/2009 Sb., trestní zákoník.
- Zákon č. 181/2014 Sb., o elektronických komunikacích

Elektronické publikace

- Bijleveld, Ank. „Keynote address by the Minister of Defence, Ms. Ank Bijleveld, marking the first anniversary of the Tallinn Manual 2.0.", 06 2018. https://english.defensie.nl/downloads/speeches/2018/06/21/keynote-address-by-the-minister-of-defence-ms.-ank-bijleveld-marking-the-first-anniversary-of-the-tallinn-manual-2.0-on-the-20th-of-june-2018.
- Department of the Army. „FM 3-12, Cyberspace and Electronic Warfare Operations". Army Publishin Directorate, 2017.
- General Assembly. „Open-ended working group on developments in the field of information telecommunications in the context of international security". A/AC.290/2021/CRP.2, 10. březen 2021.
- Germany. „On the Application of International Law in Cyberspace, position paper", podzim 2021. https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf.
- ICRC. „International Humanitarian Law and Cyber Operations during Armed Conflicts, position paper submitted to OEWG", 2019.
- Koh, Harold Hongju. „International Law in Cyberspace", 18. září 2012. https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.
- La Rue, Frank. „Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression". Human Rights Council, United Nations, 16. květen 2011.

- Ministére des Armées. „DROIT INTERNATIONAL APPLIQUÉ AUX OPÉRATIONS DANS LE CYBERESPACE", 12. listopad 2018. https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf.
- Press unit. „Personal data protection - Factsheet". European Court of Human Rights, 2021.
- Research Division. „Internet: case-law of the European Court of Human Rights". European Court of Human Rights, 2011. http://www.echr.coe.int/.
- Wright, Jeremy. „Cyber and International Law in the 21st Century", 23. květen 2018. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
- „Warsaw Summit Communiqué: issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016". Press Release (2016) 100, 9. červenec 2016.

Mezinárodně právní předpisy

- Council of Europe, ETS 185 Convention on Cybercrime, Budapest, 23.11.2001.
- General Assembly, UN. „Convention on the Prevention and Punishment of the Crime of Genocide, A/RES/3/260". Paris, France, 9. prosinec 1948.
- General Assembly, UN. „Rome Statute of the International Criminal Court". UN General Assembly, 7 1998.
- „Charter of the United Nations", 1945, 1 UNTS XVI.
- „Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)", 6 1977. 1125 U.N.T.S. 3.
- Rada Evropy, ETS 5, European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 listopad 1950, uložena u Generálního sekretariátu Rady Evropy.
- UN General Assembly,. „Universal Declaration of Human Rights", 12 1948. 217 A (III).

Rezoluce Valného shromáždění

- General Assembly, UN. „Resolution 3314 (XXIX). Definition of Aggression, with annex", 12 1974. https://undocs.org/en/A/RES/3314(XXIX).

- Komise pro mezinárodní právo. „Odpovědnost státu za mezinárodně protiprávní jednání". Příloha k rezoluci Valného shromáždění 56/83 ve znění opravného dokumentu A/56/49(Vol. I)/Corr.4, 12. prosinec 2001.
- Plenary meeting. „Resolution ICC-ASP/16/Res.5; Activation of the jurisdiction of the Court over the crime of aggression". ICC, 12 2017. https://asp.icc-cpi.int/iccdocs/asp_docs/Resolutions/ASP16/ICC-ASP-16-Res5-eng.pdf.
- Security Council. „Resolution 1973 (2011)", 17. březen 2011. https://undocs.org/S/RES/1973(2011).
- UN, General Assembly. „Resolution adopted by the General Assembly: Responsibility of States for internationally wrongful acts A/RES/56/83", 28. leden 2002.
- UN, General Assembly. „Resolution adopted by the General Assembly: Responsibility of States for internationally wrongful acts A/RES/71/133", 19. prosinec 2016.
- UN, General Assembly. „Resolution adopted by the General Assembly: Developments in the field of information and telecommunications in the context of international security A/RES/73/27", 11. prosinec 2018.

Konference

- Muižnieks, Nils. „"How to ensure that the Internet remains an open and public forum for exercising freedom of opinion and expression and facilitating other human rights and fundamental freedoms". Dublin: Commissioner for Human Rights, 2012.

Internetové stránky

- „50 U.S. Code § 1801 - Definitions ‚electronic surveillance´". Viděno 12. červen 2021. https://www.law.cornell.edu/uscode/text/50/1801.
- Cadwalladr, Carole, a Emma Graham-Harrison. „Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach". The Guardian. Viděno 16. květen 2021. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
- Cloudflare. „What is a packet? | Network packet definition". Viděno 7. červen 2021. https://www.cloudflare.com/learning/network-layer/what-is-a-packet/.
- Coalson, Robert. „Behind The Estonia Cyberattacks". RFERL, 6. březen 2009. https://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html.

- ČTK. „Kyberútok na nemocnici v Benešově způsobil škodu přes 59 milionů. Pachatele se vypátrat nepodařilo", 9. prosinec 2020. https://www.irozhlas.cz/zpravy-domov/kyberutok-kyberneticky-utok-nemocnice-v-benesove-skoda-pachatel-hacker_2008180912_ako.
- Deutsche Welle. „Coronavirus: Cyberattack blamed for delay in Germany's health data", 28. říjen 2020. https://p.dw.com/p/3kXzz.
- Dodson, Dan L. „Cybercrime on the rise: Plotting a way forward". Security Magazine, 5. únor 2021. https://www.securitymagazine.com/articles/94527-cybercrime-on-the-rise-plotting-a-way-forward.
- „Estonia's presidency in UN Security Council", 5 2021. https://vm.ee/en/activities-objectives/estonia-united-nations/estonias-presidency-un-security-council.
- Freedom of Expression. „Freedom of Expression and Information". Viděno 2. květen 2021. https://www.coe.int/en/web/freedom-expression/freedom-of-expression-and-information-explanatory-memo.
- GData. „Malware trends 2017", 4. říjen 2017. https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017.
- Garamone, Jim. „Esper Sees Iron Dome Missile Defense System in Tel Aviv". US. Dept. of Defense, b.r. https://www.defense.gov/Explore/News/Article/Article/2400629/esper-sees-iron-dome-missile-defense-system-in-tel-aviv/.
- Grassegger, Hannes, a Mikael Krogerus. „Fake news and botnets: how Russia weaponised the web". The Guardian, 2. prosinec 2017. https://www.theguardian.com/technology/2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia.
- Groll, Elias. „'Obama's General' Pleads Guilty to Leaking Stuxnet Operation". Foreign Policy, 17. říjen 2016. https://foreignpolicy.com/2016/10/17/obamas-general-pleads-guilty-to-leaking-stuxnet-operation/.
- Jabbari, Cyrus. „The Application of International Law in Cyberspace: State of Play". United Nations, 10 2018. https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/.
- Kemp, Simon. „DIGITAL 2020: 3.8 BILLION PEOPLE USE SOCIAL MEDIA", 30. leden 2020. https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media.

- Kmeroff, Alex. „War for money. Leading private military companies of the world." Viděno 12. červen 2021. https://medium.com/smartaim-tech/war-for-money-leading-private-military-companies-of-the-world-eab9f9fe2de8.
- „Man Receives Maximum Sentence for DDoS Attack on Legal News Aggregator", 11. červen 2020. https://www.justice.gov/usao-ndtx/pr/man-receives-maximum-sentence-ddos-attack-legal-news-aggregator.
- Markoff, John. „Before the Gunfire, Cyberattacks". The New York Times. Viděno 12. květen 2021. https://www.nytimes.com/2008/08/13/technology/13cyber.html.
- Mcafee. „What is Stuxnet?" Viděno 12. květen 2021. https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html.
- NATO. „Cyber defence", 12. duben 2021. https://www.nato.int/cps/en/natohq/topics_78170.htm.
- Pesce, Mark. „A brief history of cyberspace". Viděno 2. květen 2021. https://www2.cs.duke.edu/courses/spring01/cps049s/class/html/mp.history.html.
- Raab, Dominic. „UK condems Russia's GRU over Georgia cyber-attacks". Government UK, 02 2020. https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.
- Schmitt, Michael. „Germany's Positions on International Law in Cyberspace Part I". Just Security, podzim 2021. https://www.justsecurity.org/75242/germanys-positions-on-international-law-in-cyberspace/.
- Simkoff, Max, a Andy Mahdavi. „AI Doesn't Actually Exist Yet". Scientific American, 11 2019. https://blogs.scientificamerican.com/observations/ai-doesnt-actually-exist-yet/.
- Security Council Report. „January 2020 Monthly Forecast". Viděno 16. květen 2021. https://www.securitycouncilreport.org/monthly-forecast/2020-01/the-security-council-and-cyber-threats.php.
- Security InfoWatch. „The 10 most mysterious cyber crimes: Worms, hacks, satellites attacks, DNS spoofs and more unsolved computing crimes", 26. září 2008. https://www.securityinfowatch.com/cybersecurity/information-security/article/10545883/the-10-most-mysterious-cyber-crimes.
- Techopedia.com. „What Is Cyberspace? - Definition from Techopedia". Viděno 28. duben 2021. http://www.techopedia.com/definition/2493/cyberspace.

- „The Iron Dome Missile Defense System". Viděno 14. duben 2021. https://www.jewishvirtuallibrary.org/the-iron-dome.
- UN Security Council. „Voting System", b.r. https://www.un.org/securitycouncil/content/voting-system.
- WIKISOFIA. „IP adresa". Viděno 7. červen 2021. https://wikisofia.cz/wiki/IP_adresa#cite_note-3.

Odpovědnost státu za protiprávní jednání v kyberprostoru

Abstrakt

Tato diplomová práce se zabývá tématem odpovědnosti státu za protiprávní jednání v kyberprostoru. Předmětem výzkumu je aplikace norem a možnosti odpovědnosti státu v oblasti kolektivní bezpečnosti a lidských práv v kyberprostoru. Diskutována je zejména otázka použití síly, ozbrojeného útoku a agrese. V oblasti lidských práv pak právo na soukromí, svoboda projevu a právo na život. V práci také dochází k vymezení pravidel odpovědnosti státu podle Článků o odpovědnosti státu za protiprávní jednání.

Ve vybraných oblastech bylo shledáno, že se mezinárodní právo do určité míry na kyberprostor aplikuje. Dochází zde k častým útokům, které pak mohou porušovat specifické oblasti mezinárodního práva. K zodpovězení otázky odpovědnosti bylo nejdříve řešeno, zda je možné naplnit skutkové podstaty těchto porušení právě v kyberprostoru. V návaznosti na analýzu stávající judikatury a pozice vybraných států došlo k zjištění, že odpovědnost za porušení zákazu použití síly lze aplikovat v kyberprostoru.

Tato práce pracuje s povinnostmi souvisejícími s ozbrojeným útokem a agresí a možnosti státu být odpovědný za jejich porušení v kyberprostoru. V této oblasti práce nedochází k závěru, že lze použít agresi v kyberprostoru, ale dochází k závěru, že je zde možnost, aby stát byl shledán odpovědným za porušení zákazu použití síly a ozbrojeného útoku. Je to převážně z důvodu nedostatečného názoru států, ale také žádné rozhodovací praxe soudů.

V oblasti lidských práv bylo pracováno převážně s rozhodovací praxí Evropského soudu pro lidská práva. Tato práce došla k závěru, že svoboda projevu a právo na soukromí je v kyberprostoru chráněno, a to i s přihlédnutím k hromadnému sledování. Je zde také polemizováno nad ochranou práva na život, přičemž nebylo dosaženo jasného závěru, zda bude právo na život chráněno i v kyberprostoru.

Tato práce pak shrnuje dosavadní poznatky a dochází k závěru, že dosavadní právní stav úpravy kyberprostoru není dostačující, ale spíše přechodný. Nová právní úprava by měla být zaměřena více na specifika kyberprostoru, se kterými se v budoucnu bude mezinárodní společenství potýkat.

Klíčová slova: kyberprostor, odpovědnost státu, kolektivní bezpečnost, lidská práva

Responsibility of States for Unlawful Acts in Cyberspace

Abstract

This master's thesis addresses the topic of responsibility of state for the unlawful acts in cyberspace. The research subject is the application of the legal norms and the possibility of the state being held responsible in the field of collective security and human rights in cyberspace. It discusses mainly the question of use of force, armed attack, and aggression. Regarding the human rights, this master's thesis focuses on right to private life and family life, freedom of expression and right to life. This thesis delimitates the rules of responsibility of state under the Articles on Responsibility of State for Unlawful acts.

In the chosen fields it was found that the international public law applies in limited manner also to cyberspace. In cyberspace, many attacks take place, which may result in breach in different fields of international law. To answer the question of the state responsibility, it was firstly dealt with, whether the subject-matter of this breaches can be reached in cyberspace. Following the analysis of the contemporary case law and state positions, it was argued, that the responsibility for the breach of prohibition of use of force may be applied in cyberspace.

This thesis uses terms of armed attack and aggression and also the possibility of state to be held responsible for their commitment in cyberspace. In this field this thesis did not come to conclusion, that aggression may be committed in cyberspace. However, it argues that there exists possibility for a state to be held responsible for the breach of prohibition on use of force and armed attack. It is due to the lack of state positions and case law.

In the field of human rights this thesis analyses the case of the European Court of Human Rights. This thesis argues that the freedom of expression and right to privacy, including mass surveillance, is protected in cyberspace. The right to life is also discussed, however no clear conclusion is made on this topic, whether the human life will be protected even through cyberspace.

This thesis concludes the current new finds and comes to conclusion, that the contemporary law regarding cyberspace is not sufficient, more so temporary. New legislation should be more focused on the specifics of cyberspace, which the international community will have to face.

Keywords: Cyberspace, state responsibility, collective security, human rights