Univerzita Palackého v Olomouci

Právnická fakulta

Adam Friml

Kybernetické prostředky a metody vedení boje ve světle mezinárodního humanitárního práva

Diplomová práce

Olomouc 2018

Prohlašuji, že jsem diplomovou práci na téma „Kybernetické prostředky a metody vedení boje ve světle mezinárodního humanitárního práva“ vypracoval samostatně a citoval jsem všechny použité zdroje.

V Olomouci dne 23. února 2018 ……

Adam Friml

Na tomto místě bych velice rád poděkoval vedoucímu diplomové práce JUDr. Martinu Faixovi, Ph.D., MJI za jeho odborné vedení, rady, trpělivost a vstřícnost s níž tuto práci vedl. Chtěl bych také poděkovat rodičům za jejich podporu a Majdě za to, že je pro mě pevnou oporou.

Obsah

Seznam použitých zkratek

ICTY	Mezinárodní trestní tribunál pro bývalou Jugoslávii
MSD	Mezinárodní soudní dvůr
MVČK	Mezinárodní výbor Červeného kříže
OSN	Organizace spojených národů

Úvod

Jedním z leitmotivů lidských dějin je válka. Lidé mezi sebou válčí odnepaměti a vždy, i díky rozvoji vědy a techniky, dokázali vymyslet důmyslnější a účinnější prostředky vedoucí k porážce druhé strany. Mezinárodní společenství pochopilo, že nelze vymýtit válku jako takovou, a proto se alespoň snaží regulovat její průběh a následky pomocí pravidel mezinárodního práva veřejného. Soubor těchto pravidel je označován jako mezinárodní humanitární právo.

Rychlost mechanismu vzniku pravidel mezinárodního práva veřejného si ale nezadá s tempem rozvoje vědy a techniky. Právní úprava reagovala na technologický vývoj vždy až ex post. Toto tvrzení platí i pro kybernetické prostředky a metody vedení boje. Poslední kodifikační práce v oblasti mezinárodního humanitárního práva pochází z roku 1977, kdy byly na Diplomatické konferenci v Ženevě přijaty Dodatkové protokoly I a II k Ženevským úmluvám z 12. srpna 1949. V této době, kdy byly informační technologie ještě na počátku své existence, si málokdo uvědomoval jejich potenciál pro vedení bojových operací. Takové představy byly spíše obsahem vědeckofantastické literatury než vojenských manuálů. V současnosti jsou informační a komunikační technologie implementovány a užívány ve všech vojenských oblastech, a to včetně vedení bojové činnosti. Mezinárodní společenství nejenže nebylo dosud ochotné ani schopné zaujmout jednotné stanovisko k aplikaci mezinárodního humanitárního práva na nové vojenské technologie, ale nezaujalo ani žádnou oficiální pozici vůči aplikaci obecného mezinárodního práva v prostředí kyberprostoru.

Cílem diplomové práce je odpovědět na hlavní otázky – čím se kyberprostor odlišuje od ostatních oblastí vedení bojových operací a jaké z toho plynou konsekvence pro možnosti jeho mezinárodněprávní regulace. Dále, zda je mezinárodní humanitární právo aplikovatelné na kybernetické prostředky a metody vedení boje, případně jaké jsou problematické aspekty této aplikace. Při hledání odpovědí na výzkumné otázky bude použita v kapitole I převážně deskriptivní metoda a v následujících kapitolách metoda analýzy.

Těžištěm pro zodpovězení první otázky bude kapitola I, kde bude vymezeno prostředí kyberprostoru, včetně specifik jeho možné právní regulace. V kapitole budou dále nastíněny vybrané kybernetické incidenty nedávné historie spolu s právními výzvami, jež představují především pro úpravu mezinárodního humanitárního práva. Analýza působnosti mezinárodního humanitárního práva je obsahem kapitoly II a III. Na počátku kapitoly II bude pojednáno o Tallinnském manuálu, který představuje jediný komplexní dokument zabývající se problematikou vztahu mezinárodního práva a kybernetických operací. Jedná se o právně nezávazný dokument, který ale díky kvalitě své metodologie představuje ojedinělé akademické dílo. Následně bude v kapitole II analyzováno, zda právní úprava mezinárodního humanitárního práva obsahuje

nástroje pro překlenování mezer vzniklých v důsledku technologického vývoje a za jakých podmínek bude dána jeho působnost. Konkrétní podobou aplikace mezinárodního humanitárního práva se zabývá kapitola III., ve které budou rozebrány vybrané zásady mezinárodního humanitárního práva a jejich uplatnění při vedení kybernetických operací. Zásady byly zvoleny s ohledem na míru kontroverze, kterou vyvolávají v souvislosti s tématem práce.

Jako hypotéza práce bylo zvoleno tvrzení, že právní úprava mezinárodního humanitárního práva je aplikovatelná na kybernetické prostředky a metody vedení boje.

Tématu je v zahraniční akademické a vojenské literatuře věnována široká pozornost. Nejsilnější zastoupení v akademické sféře i vojenské praxi mají technologicky silné státy jako například Spojené státy americké nebo Izrael, disponující moderní a sofistikovanou vojenskou technikou i doktrínou. Není proto překvapivé, že v česky psané literatuře je zájem o téma zatím nižší. K tématu neexistuje žádná explicitní smluvní úprava ani obyčejová pravidla. Nebyla prozatím vydána žádná soudní rozhodnutí týkající se kyberprostoru. Většina prací proto vychází z platné právní úpravy a snaží se do určité míry na základě analogie aplikovat pravidla mezinárodního humanitárního práva včetně judikatorních závěrů na kybernetické prostředky a metody vedení boje. Některé práce se vůči tomuto postupu vymezují a snaží se navrhnout úpravu de lege ferenda s tím, že platná právní úprava je absolutně nedostatečná a nedokáže se vypořádat s výzvami představovanými kyberprostorem. Lze rozeznat odlišný přístup mezi pracemi teoretiků mezinárodního práva a publikujících vojenských právníků. Zatímco první skupina upřednostňuje přísnější požadavky a omezení na vedení vojenských kybernetických operací, druhá skupina se snaží o pragmatičtější přístup umožňující humánní, ale stále efektivní vedení kybernetických vojenských operací.

Při zpracování této práce bylo v převážné většině případů využito elektronicky přístupných článků ze zahraničních odborných časopisů přes databáze *HeinOnline* a *SSRN eLibrary,* doplněných několika dostupnými knižními publikacemi na téma kybernetických prostředků a metod vedení boje. Dále bylo pracováno s komentáři k Ženevským úmluvám z roku 1949 a komentáři k jejich Dodatkovým protokolům. Byla užita i některá soudní rozhodnutí Mezinárodního soudního dvora a Mezinárodního trestního tribunálu pro bývalou Jugoslávii, jejichž závěry jsou použitelné i v kontextu kybernetických operací. Hojně využívaným byl také Tallinnský manuál. Jak již bylo řečeno, jedná se o komplexní dokument z dílny mezinárodně uznávaných autorů, jehož rozsah zasluhuje podkapitolu ve vlastním textu práce a posloužil jako výchozí pramen při jejím zpracování. Četnost jeho využití jako hlavního pramene dále odůvodňuje fakt, že je v něm sumarizována diskuze vedená v jednotlivých odborných časopisech. Nutno poznamenat, že někteří autoři těchto prací působí zároveň v autorském kolektivu Tallinnského manuálu.

1 Mezinárodněprávní rámec kyberprostoru

Kybernetické prostředky a metody vedení boje jsou pouze dílčím aspektem komplexní mezinárodněprávní problematiky, jejímž objektem zájmu je kyberprostor jako takový. Tím, že v současném mezinárodním právu veřejném[1] neexistuje mezinárodní úmluva ani obyčejové pravidlo, které by se explicitně týkalo pravidel ovládajících kyberprostor, je nezbytné s pojmem zacházet v kontextu a rámci celé právní vědy mezinárodního práva.

Mezinárodní právo můžeme charakterizovat jako soubor právních pravidel, která upravují vzájemné vztahy mezi sobě rovnými subjekty. Tyto vztahy jsou vytvářeny na základě chování států v rámci mezinárodního společenství.[2] Státy, popřípadě jimi vytvořené mezinárodní organizace, určují pravidla vzájemného soužití pomocí mezinárodních smluv nebo právních obyčejů. Vymezují si svá „hřiště" a stanovují pravidla hry v rámci celé zeměkoule i mimo ni. Těmito hřišti byly tradičně voda, země a vzduch. Ve druhé polovině 20. století přibyl kosmický prostor. Díky technologickému pokroku se zatím poslední vrstvou reality stal kyberprostor. Jedná se o čistě lidský výtvor představující svým charakterem „hozenou rukavici" státům a ostatním aktérům mezinárodního společenství z pohledu tradičních mezinárodněprávních konceptů.

Až do vzniku kyberprostoru[3] pracovaly státy s objektivně vymezitelným prostorem a většina pravidel mezinárodního práva to v jistém ohledu odráží. Za příklad lze vzít koncept suverenity státu. Stát na svém vymezeném území vykonává svrchovaně veřejnou moc a ostatní státy mají povinnost do tohoto výkonu nezasahovat.[4] Státní území je vymezeno státní hranicí, kdy „*hranice tvoří pomyslné plochy, které vedou ze středu zeměkoule, protínají hraniční linii na zemském povrchu a s kuželovitým rozšiřováním pokračují až po hranici kosmu.*"[5] Podobně s vymezením suverenity ve vztahu k prostoru pracuje i Úmluva Organizace spojených národů o mořském právu, když v čl. 2 odst. 1 stanovuje: „*Svrchovanost pobřežního státu se rozšiřuje za jeho pevninské území a vnitřní vody, a v případě souostrovního státu za jeho souostrovní vody, na přilehlé mořské pásmo zvané pobřežní moře.*"[6] Konečně možnost, či spíše nemožnost uplatnění suverenity v kosmickém prostoru je obsahem ustanovení čl. 2 Kosmické smlouvy z roku 1967: „*Kosmický prostor včetně Měsíce a jiných nebeských těles si jednotlivé státy nemohou*

[1] V této práci dále pro zjednodušení jako „mezinárodní právo".
[2] DAVID, Vladislav a kol. *Mezinárodní právo veřejné s kazuistikou*. 2. aktualizované a přepracované vydání. Praha: Leges, 2011, s. 75.
[3] Počátky kyberprostoru jsou spojovány se vznikem sítí ARPANET a NSFNET v 80. letech 20. století. Blíže ANDRUŠKO, Alena. *Internet, informační společnost a autorské právo*. 1. vydání. Praha: Wolters Kluwer ČR, 2016, s. 6. – 9.
[4] K obsahu pojmu suverenity blíže Stálý rozhodčí soud: *Island of Palmas case* (Netherlands, USA), arbitral award, 4 April 1928, s. 838.
[5] DAVID: *Mezinárodní…,* s. 78. K výkonu suverenity nad vzdušným prostorem srov. čl. 1 Úmluvy o mezinárodním letectví ze dne 7. prosince 1944, vyhlášené pod č. 147/1947 Sb.
[6] Čl. 2 Úmluvy Organizace spojených národů o mořském právu, vyhlášené pod č. 240/1996 Sb. Dále jako „UNCLOS".

přivlastnit prohlášením suverenity, užíváním, okupací nebo jakýmkoli jiným způsobem.“[7] Není to ale pouze suverenita, která se váže na objektivně vymezitelný a ohraničený prostor. Stejnou vazbu na prostor obsahuje i koncept národní jurisdikce, místní působnost právních norem nebo pravidla neutrality.[8]

1.1 Kyberprostor – definiční vymezení a charakteristika

Kyberprostor je odlišný od tradičního chápání pojmu prostor. Neskládá se pouze z jedné fyzické složky jako například pevnina. Materiální podstatou kyberprostoru je internet, který lze popsat jako „*…celosvětovou distribuovanou počítačovou síť složenou z jednotlivých menších sítí, které jsou navzájem spojeny pomocí protokolů IP a tím je umožněna komunikace, přenos dat, informací a poskytování služeb mezi subjekty navzájem.*“[9] Jádro internetu, potažmo kyberprostoru, tvoří sítě, jejichž účelem je přenos elektromagnetického signálu skrze nosiče, jimiž mohou být vzduch, optické kabely nebo jiná přenosová média. Jednotlivé sítě mezi sebou komunikují pomocí specifických internetových protokolů, mezi kterými jsou nejdůležitější standardy TCP/IP (*Transmission Control Protocol/Internet Protocol*).

V kyberprostoru proto dochází na základě virtualizace sociálních vztahů k oddělení obsahu jednotlivých sítí od fyzické infrastruktury. Tento jev bývá označován jako delokalizace společenských vztahů na internetu.[10] Informace mohou být sdíleny mezi subjekty, aniž by tato komunikace byla omezována nebo limitována teritoriální bariérou.[11] K tomu lze shrnout, že „*Je-li místní působnost práva vztahem mezi fyzickou lokalitou a právním pravidlem, pak v situaci, kdy fyzická lokalita je irelevantním kritériem, pozbývá tento koncept význam.*“[12] Část odborníků argumentuje, že na základě nezávislosti kyberprostoru na fyzických hranicích existuje požadavek na vytvoření systému pravidel odlišného od toho, který reguluje prostor fyzický. Kyberprostor je totiž omezen spíše obrazovkami a hesly, než fyzickými ukazateli či hranicemi.[13]

Neuchopitelnost takového konceptu v rámci mezinárodního práva je zřejmá. Na fungování kyberprostoru nemají právní ani faktický vliv jednotlivé státy.[14] Státy si ani nemohou rozdělit

---

[7] Čl. 2 Smlouvy o zásadách činnosti států při výzkumu a využívání kosmického prostoru včetně Měsíce a jiných nebeských těles ze dne 7. února 1968, vyhlášené pod č. 40/1968 Sb.

[8] K pojmu jurisdikce srov. MENTHE, Darrel C. Jurisdiction in Cyberspace: A Theory of International Spaces. *Michigan Telecommunications and Technology Law Review*, 1998, roč. 4, č. 1, s. 71, a dále k pojmu neutralita např. MALANCZUK, Peter. *Akehurst's Modern Introduction to International Law*. 7. vydání. New York: Routledge, 1997, s. 350.

[9] KOLOUCH. Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, 2016, s. 43.

[10] POLČÁK. Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 102.

[11] POST, David G. Governing Cyberspace. *Wayne Law Review*, 1996, roč. 43, č. 1, s. 159.

[12] POLČÁK: *Internet a…*, s. 103.

[13] JOHNSON, David R., POST, David G. Law and Bordes – the Rise of Law in Cyberspace. *Stanford Law Review*, 1997, roč. 48, s. 1367.

[14] Jedním ze základních komponent fungování internetu je adresní a identifikační systém, jehož správa náleží soukromé společnosti ICANN, která podléhá právu státu Kalifornie. Podrobněji viz GÁBRIŠ, Tomáš. *Cyber Law: textbook*. 1. vydání. Bratislava: Univerzita Komenského v Bratislavě, 2014, s. 16 - 17. Dalším základním komponentem jsou standardy definující fungování internetu jako celku. Jejich vytvářením se zabývá mezinárodní organizace Internet Society.

kyberprostor podobně jako státní území, jelikož nelze jasně stanovit jeho hranice. Přesněji řečeno kyberprostor neoperuje s pojmy jako hranice, území, působnost nebo pravomoc. Podobně není dobře možné vymezit si práva a povinnosti v určité části kyberprostoru, jako je tomu v případě mořského práva.[15] To vyvolává otázku, jakým způsobem se státy, jakožto primární tvůrci norem mezinárodního práva, mají vypořádat s prostředím, nad kterým nemají přímý vliv.

Je patrné, že v důsledku sepětí kyberprostoru s technickou infrastrukturou, která jej fakticky vytváří, jsou státy při snaze o vytvoření pravidel regulujících kyberprostor nuceny spolupracovat ve vyšší míře i s nestátními aktéry. Je tomu tak proto, že právě nestátní aktéři reálně zajišťují fungování celého systému, jsou tzv. definičními autoritami.[16] Jsou jimi provozovatelé síťové komunikační infrastruktury, softwarové společnosti nebo provozovatelé logických služeb informačních technologií.[17]

V minulosti proběhly pokusy o vytvoření jisté formy globální správy kyberprostoru. Evropská unie i OSN se snažily prosadit, aby správa internetu přešla na mezivládní organizaci v rámci OSN, s čímž ale zásadně nesouhlasily Spojené státy americké. Jistým kompromisem bylo vytvoření mezinárodního Fóra pro správu internetu (*Internet Governance Forum*) v červenci 2006, ve kterém mohou debatovat představitelé vlád jednotlivých států a vytvářet doporučení ohledně správy internetu. Tato doporučení ovšem nemají žádný přímý vliv na samotnou správu internetu.[18] Fórum pro správu internetu proto nedosahuje důležitosti jiných mezinárodních organizací zabývajících se správou určité výseče prostoru.[19]

Dalším z problematických aspektů diskuze o právní regulovatelnosti kyberprostoru je absence jeho definičního vymezení. Doktrína mezinárodního práva prozatím nepřišla s ustálenou definicí kyberprostoru. Pokusy o jeho vymezení ve většině případů vycházejí z vojenských příruček. Jedním z prvních států, který zahrnul kyberprostor do své vojenské doktríny, byly Spojené státy americké v roce 2006. Podle Národní vojenské strategie pro operace v kyberprostoru je kyberprostor „*Doména charakterizovaná užitím elektroniky a elektromagnetického spektra k uchovávání, modifikaci a výměně dat skrze síťové systémy a přidruženou fyzickou infrastrukturu.*“[20]

---

[15] Tak čl. 3 UNCLOS stanovuje, že „*Každý stát má právo stanovit šíři svého pobřežního moře až po hranici nepřesahující dvanáct námořních mil měřených od základních linií určených v souladu s touto Úmluvou.*“

[16] POLČÁK: *Internet* a…, s. 107.

[17] Tito aktéři mohou mít odlišné zájmy a cíle na poli kyberprostoru, což se v minulosti projevilo vzájemnou konkurencí a pouze omezenou spoluprací se státy. Srov. KLEINWACHTER, Wolfgang. From Self – Governance to Public-Private Partnership: The changing Rule of governments in the Management of the Internet's Core Resources. *Loyola of Los Angeles Law Review*, 2003, roč. 36, č. 3, s. 1103 - 1126.

[18] Blíže GOLDSMITH, Jack, WU, Tim. *Who Controls the Internet? Illusions of Borderless World*. New York: Oxford University Press, 2006, s. 168 - 171.

[19] Například pro oblast mořského dna a jeho podzemí za hranicemi pravomoci států byla vytvořena Mezinárodní správa mořského dna. Srov. čl. 156 an. UNCLOS.

[20] National Military Strategy for Cyberspace Operations (NMS-CO), Chairman of the Joint Chiefs of Staff, Department of Defence, vydáno 11 prosince 2006, Washington D. C., USA.

Tato definice byla později dvakrát upravena v roce 2008.[21] Mezi odborníky byla shledána nedostatečnou, jelikož nevystihuje unikátní povahu kyberprostoru. Lépe a komplexněji lze kyberprostor vymezit takto: „*kyberprostor je globální doména v rámci informačního prostředí, jejíž rozlišující a unikátní charakter je zarámován užitím elektroniky a elektromagnetického spektra k vytváření, uchovávání, modifikování, výměně a využívání informací skrze nezávislé a propojené sítě využívající informační a komunikační technologie.*“[22]

Je tedy složité stanovit jednotnou definici kyberprostoru.[23] Obtížnost jeho objektivního vymezení znesnadňuje jednání o podobě pravidel, která by jej měla ovládat. Pro účely této práce lze kyberprostor vnímat jako uměle vytvořenou sféru, která se stala složkou životního prostředí a významným způsobem ovlivňuje chod globálního a ekonomického systému.[24] Závažnost, s jakou lze pomocí kyberprostoru působit na klíčové prvky státní infrastruktury, lze demonstrovat na kybernetických incidentech nedávné historie.

1.2 Moderní kybernetické incidenty

1.2.1 Kybernetický incident v Estonsku

Na přelomu dubna a května 2007 se Estonko stalo dějištěm jednoho z prvních rozsáhlých kybernetických incidentů v moderních dějinách. Spouštěcím momentem, který se stal příčinou následných událostí, bylo rozhodnutí estonské vlády přemístit bronzovou sochu sovětského vojáka z centra Tallinnu. Tato socha byla připomínkou vítězství Sovětské armády nad okupačními silami Nacistické říše za druhé světové války. Společně s přemístěním sochy měla být provedena i exhumace a přemístění těl neznámých padlých vojáků, jejichž hroby se zde nacházely.[25] Rozhodnutí estonské vlády zpočátku provázely civilní nepokoje a posléze se objevily i nepokoje v estonském kyberprostoru.[26]

Kybernetické operace[27] začaly 27. dubna 2007, kdy se jejich cílem staly vládní instituce a jejich informační infrastruktura. V různé intenzitě trvaly až do konce května 2007, kdy se politické napětí

---

[21] KUEHL, Daniel T. From Cyberspace to Cyberpower: Defining the Problem. In KRAMER, Franklin D. (ed). *Cyberpower and National Security*. Lincoln: University of Nebraska Press, 2009, s. 28. Dostupné na <http://ctnsp.dodlive.mil/files/2014/03/cyberpower-i-chap-02.pdf>.

[22] Tamtéž, s. 30.

[23] Kuehl přidává pro představu celkem 13 různých definic kyberprostoru, KUEHL: *From Cyberspace*…, s. 27.

[24] BASTL, Martin, GRUBEROVÁ, Zuzana. Kyberprostor jako „pátá doména“? *Vojenské rozhledy*, 2013, roč. 22 (54), č. 4, s. 11.

[25] KOSACHEV, Konstantin. *An insult to our war dead* [online]. theguardian.com, 6. března 2007 [cit. 10. prosince 2017]. Dostupné na <https://www.theguardian.com/commentisfree/2007/mar/06/comment.secondworldwar>.

[26] *A Cyber Riot* [online]. economist.com, 10. května 2007 [cit. 10. prosince 2017]. Dostupné na <http://www.economist.com/node/9163598>.

[27] V této kapitole budou pojmy „kybernetická operace“ a „kybernetický útok“ užívány jako synonyma.

mezi Estonskem a Ruskou federací začalo zmírňovat.[28] Celý kybernetický incident lze dle stupně intenzity, užitých prostředků a cílů rozdělit na dvě fáze. První fáze, trvající od 27. dubna do 29. dubna, zahrnovala DoS[29] útoky na vládní webové stránky a na některá online působící média, která měla za úkol informovat o probíhajících nepokojích a násilnostech. Útoky nebyly koordinované ani sofistikované. Jejich následky byly vcelku bez obtíží odstraněny.[30] K této fázi lze doplnit, že dle estonských oficiálních kruhů bylo možné na ruskojazyčných internetových fórech nalézt návod, jak pomocí DoS útoků zaútočit na estonské vládní instituce a vyjádřit tím svůj odmítavý postoj k estonské politice.[31] Tato skutečnost je velmi důležitá pro pochopení rozsahu hrozeb, které s sebou prostředí kyberprostoru přináší. Zvláště v situaci, kdy již není obtížné potenciálně podpořit válečné úsilí jedné strany za použití počítače a návodu, který je poskytnut na internetu.[32] Druhou fázi lze charakterizovat komplexnějšími a lépe koordinovanými útoky. Výrazem sofistikovanosti bylo především užití DDoS útoků[33] a botnetů.[34] Útoky cílily jak na vládní webové stránky a vládní komunikační kanály, tak na soukromé subjekty, mezi kterými byla například největší soukromá banka Hansapank.[35]

Lze shrnout, že Estonsko bylo útokem zaskočeno. Dočasně byl omezen přístup na webové stránky významných ústavních činitelů – vlády, premiéra, prezidenta a dalších státních institucí.[36] Estonsko se dostalo do situace, kdy dočasně nebylo schopné sdělit okolním státům, že je cílem rozsáhlých kybernetických útoků. Následky útoků pocítili i obyvatelé Estonska, když po déle jak hodinu nebyly dostupné telefonní linky na záchrannou službu a hasiče.[37] Zasažením bankovní sítě byla způsobena rozsáhlá škoda na finančních tocích.[38]

---

[28] TIKK, Eneken, KASKA, Kadri, VIHUL, Liis. *International Cyber Incidents: Legal Considerations*. Tallinn: Cyber Defence Centre of Excellence, 2010, s. 18.

[29] DoS neboli „denial of service" útok je jedna z forem kybernetického útoku na internetovou službu. Jejím cílem je vyřazení napadeného zařízení z činnosti nebo snížení jeho výkonu. Srov. KOLOUCH: *Cybercrime*…, s. 295.

[30] TIKK, KASKA, VIHUL: *International Cyber*…, s. 18.

[31] FINN, Peter. *Cyber Assaults on Estonia Typify a New Battle Tactic* [online]. washingtonpost.com, 19 června 2007 [cit. 10. prosince 2007]. Dostupné na <http://www.washingtonpost.com/wpdyn/content/article/2007/05/18/AR2007051802122.html>.

[32] Tamtéž.

[33] Jedná se o DoS útok vedený z více zařízení, kterých můžou být i tisíce. Viz ŘEHKA, Karel. *Informační válka*. 1. vydání. Praha: Academia, 2017, s. 195.

[34] Botnet je síť různých, internetem vzájemně propojených zařízení, kterou může její vlastník využít k provedení dalšího útoku. Tamtéž, s. 194. Dále např. EVRON, Gadi. Bettling Botnets and Online Mobs: Estonia's Defence Efforts during the Internet War. *Georgetown Journal of International Affairs*, 2008, roč. 9, č. 1, s. 121 - 126.

[35] RICHARDS, Jason. Denial-of-Service: The Estonian Cyberwar and Its Implications for U. S. National Security. *International Affairs Review*, 2009, roč. 18, č. 2. Dostupné na <http://www.iar-gwu.org/node/65>.

[36] Cílem útoku se stala téměř všechna ministerstva a estonská policie. Srov. TIKK, KASKA, VIHUL: *International Cyber*…, s. 22.

[37] *Newly nasty* [online]. economist.com, 24 května 2007 [cit. 10. prosince 2017]. Dostupné na <http://www.economist.com/node/9228757>.

[38] Blíže WEISS, Michael. *Here Come the Cyber Wars: Are We Ready* [online]? reason.com, 17. srpna 2007 [cit. 10. prosince 2017]. Dostupné na <http://reason.com/archives/2007/08/17/here-come-the-cyber-wars>.

Odborná veřejnost zkoumala, kdo byl původcem těchto útoků. Z analýz expertů vyplynulo, že minimálně od druhé fáze již nebylo v silách běžného počítačového uživatele provést takto rozsáhlý a propracovaný útok. Útok vykazoval známky centrálního řízení a kontroly. Technicky byl velmi komplexní a jednotlivé útoky přicházely ve správný čas. Jistě se také neobešel bez dostatečného lidského a finančního zázemí.[39] Estonsko připisovalo útok Ruské federaci, jelikož v něm spatřovalo reakci na své rozhodnutí přemístit sovětský pomník. Z vyšetřování dále vyplynulo, že některé IP adresy útočníků byly napojeny na ruské vládní instituce.[40] Ruská federace se však od incidentu distancovala a jakékoli zapojení odmítla.[41]

1.2.2 Konflikt v Gruzii

Odlišná situace nastala v srpnu roku 2008 v Gruzii. V tomto období zde probíhal mezinárodní ozbrojený konflikt mezi Gruzií a Ruskou federací. Jádrem sporu bylo demilitarizované území Jižní Osetie, které roku 1991 vyhlásilo jednostranně nezávislost na Gruzii, avšak bez mezinárodní podpory. Na území Jižní Osetie se dále projevovaly separatistické tendence a provokace. Ty vyvrcholily nasazením vládních jednotek Gruzie 7. srpna 2008.[42] Na tuto skutečnost zareagovala Ruská federace provedení rozsáhlé vojenské operace dne 8. srpna 2008 na území Jižní Osetie z titulu závazku ochránit své občany nacházející se na tomto území.[43] Gruzie vnímala akt Ruské federace jako vojenskou agresi a ještě 8. srpna vyhlásila celostátní mobilizaci.[44] Boje trvaly až do uzavření příměří dne 12. srpna. 2008.[45]

Kybernetické útoky na Gruzii ale začaly ještě dříve, než na její území vstoupila vojska Ruské federace. Již 20. července 2008 se webové stránky prezidenta Mikkheila Saakashviliho staly cílem DoS útoku, v jehož důsledku byly po dobu 24 hodin nepřístupné.[46] 8. srpna, v den vstupu vojsk Ruské federace na území Gruzie, došlo k DDoS útokům zaměřeným na vládní webové stránky, centrální vládní síť a domovské stránky některých ministerstev. Pro účely této práce je vhodné poznamenat, že se jednalo o první případ kybernetické operace v kontextu ozbrojeného konfliktu.[47]

---

[39] TIKK, KASKA, VIHUL: *International Cyber…*, s. 23.
[40] LANDLER, MARKOFF: *In Estonia…*
[41] Tamtéž.
[42] *War in South Ossetia: Georgia started it* [online]. theguardian.com, 1. října 2009 [cit. 10. prosince 2017]. Dostupné na <https://www.theguardian.com/commentisfree/2009/oct/01/russia-georgia-south-ossetia>.
[43] TIKK, KASKA, VIHUL: *International Cyber…*, s. 68. K doktríně ochrany vlastních občanů v zahraničí srov. THOMSON, Andrew W. R. Doctrine of the Protection of Nationals Abroad: Rise of the Non-Combatant Evacuation Operation. *Washingston University Global Studies Law Review*, 2012, roč. 11, č. 3, s. 628 - 666.
[44] Viz *Declaration of Universal Mobilization by Georgian President Mikheil Saakahvili* [online]. vk.com, 10. srpna 2008 [cit. 18. února 2018]. Dostupné na <https://vk.com/topic-4143158_6733001>.
[45] *Russia „ends Georgia operation"* [online]. news.bbc.co.uk, 12 srpna 2008 [cit. 10. prosince 2017]. Dostupné na <http://news.bbc.co.uk/2/hi/europe/7555858.stm>.
[46] ASHMORE, William C. Impact of Alleged Russian Cyber Attacks. *Baltic Security & Defence Review*, 2009, roč. 11, s. 10.
[47] MARKOFF, John. *Before the Gunfire, Cyberattacks* [online]. nytimes.com, 12. srpna 2008 [cit. 10. prosince 2017]. Dostupné na <http://www.nytimes.com/2008/08/13/technology/13cyber.html>.

Kybernetické útoky se především soustřeďovaly na ovlivňování veřejného mínění. Útočníci užívali rozličné metody kybernetických útoků, jako např. DDoS útoky nebo vytváření falešných webových stránek.[48] Oproti incidentu v Estonsku útočníci využili i tzv. SQL Injection[49] útoků, které je obtížnější rozpoznat, jelikož ke svému provedení vyžadují méně počítačů než například botnet útoky. Jejich použití naznačuje zapojení subjektu, který disponoval dostatečnými prostředky a odborností pro provedení takové operace.[50]

Nebyl nalezen žádný přesvědčivý důkaz, že by za kybernetickými útoky stál jakýkoliv stát. Rozsah a efektivita užitých prostředků ale napovídá, že za kybernetickými operacemi nemohl být jednotlivec. Naopak, i jedna z částí vyšetřování poukazuje na zapojení ruské teroristické organizace RBN.[51]

1.2.3 Program Stuxnet

Počítačový program Stuxnet byl odhalen v roce 2010. Jednalo se o historicky prvního počítačového červa,[52] jehož cílem se mělo stát konkrétní zařízení se specifickými parametry. Zařízením měl být zvláštní typ řídicího systému užívaného k provozu nukleárních elektráren.[53] Červ mohl být šířen i bez přístupu daného zařízení k síti, například pomocí přenosných zařízení, ale i skrze počítače připojené k internetu. Také měl v sobě naprogramované důmyslné mechanismy proti odhalení.[54] Stuxnet byl vytvořen ke zpomalení vývoje íránského jaderného programu. Do systémů jaderného zařízení ve městě Natanz byl umístěn skrze flash disk jednoho ze zaměstnanců s cílem zasáhnout centrifugy sloužící k obohacování jaderného paliva. To se tomuto programu povedlo, a výsledkem bylo pravděpodobné zpoždění vývoje íránského jaderného programu o tři roky.[55] Kromě íránského jaderného zařízení byl však Stuxnet detekován i v jiných zařízeních téměř po celém světě. Není mnoho publikovaných zpráv o tom, zda i v nich způsobil nějakou škodu. O přítomnosti Stuxnetu ve svých informačních systémech referovaly například Indonésie, Indie, Pákistán, Čína nebo Spojené státy americké. K vývoji programu se oficiálně nepřihlásila vláda žádného státu. Na základě výzkumu a dle vyjádření nejmenovaných státních

---

[48] THOMAS, Timothy L. The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia. *Journal of Slavic Military Studies*, 2009, roč. 22 s. 55-59.
[49] Blíže ŘEHKA: *Informační…,* s. 197.
[50] ASHMORE: *Impact of…*, s. 11.
[51] TIKK, KASKA, VIHUL: *International Cyber…*, s. 74.
[52] Heslo „worm" v internetovém slovníku technických výrazů označuje počítačový program, který je schopen vytvářet kopie sebe samého. Program se šíří z počítače na počítač, infikuje celý systém a způsobuje škody. Dokáže penetrovat počítačovou paměť skrze počítačovou síť, vypočítat síťovou adresu jiného počítače a rozesílat své kopie na tyto adresy. Technický slovník je dostupný na <http://www.techdictionary.com/search_action.lasso>.
[53] PEAGLER, Jordan. The Stuxnet Attack: A New Form of Warfare and the (In)Aplicability of Current International Law. *Arizona Journal of International & Comparative Law*, 2014, roč. 31, č. 2, s. 402.
[54] Tamtéž.
[55] RICHMOND, Jeremy. Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modification to the Law of Armed Conflict? *Fordham International Law Journal*, 2012, roč. 35, s. 857.

zaměstnanců Spojených států amerických, označují média a počítačoví odborníci za jeho tvůrce Spojené státy americké společně se státem Izrael.[56]

Stuxnet nelze vnímat jako pouhý kybernetický incident, který by byl srovnatelný s kybernetickými operacemi v Estonsku nebo Gruzii. Do okamžiku jeho detekování bylo cílem kybernetických operací narušení nebo manipulace s daty, vytváření falešných webových stránek za účelem podpory zúčastněného aktéra nebo blokování internetových účtů a komunikací. Na rozdíl od operací v Estonsku nebo Gruzii je na Stuxnet nutné nahlížet jako na první kybernetickou zbraň, čímž dochází k přesunu z oblasti kybernetické bezpečnosti do oblasti kybernetického válečnictví.[57] Stuxnet kromě tradičních účinků kybernetických operací zaznamenaných do této doby ukázal světu nový prvek kybernetického boje, kterým bylo způsobení kinetických následků v podobě fyzických účinků na hardware. Tímto okamžikem přestává být vedení boje výhradní doménou fyzického světa a možnosti vedení boje se objevují i v kyberprostoru.

1.2.4 Právní výzvy spojené s incidenty

Nejasnosti ohledně aplikace pravidel mezinárodního práva na kybernetické prostředí vyvolávají řadu otázek, které mohou mít zásadní důsledky.

Cílem kybernetických útoků v Estonku byla vládní i nevládní informační infrastruktura. Tím, že Estonsko jako stát začlenilo ve vysoké míře informační a komunikační technologie do fungování veřejné správy, pocítilo následky kybernetických operací více než např. Gruzie. Estonsko si mohlo položit otázku, zda tyto kybernetické útoky znamenaly porušení jeho suverenity, potažmo zda se mohlo jednat o porušení zákazu užití síly dle čl. 2 odst. 4 Charty OSN.[58] Pokud by byla odpověď kladná, další krokem by mohla být analýza, zda se jednalo o ozbrojený útok ve smyslu čl. 51 Charty OSN, který by umožnil Estonku využít svého práva na sebeobranu. Estonsko je také členem Severoatlantické aliance,[59] proto by v případě vyhodnocení kybernetických operací jako ozbrojených útoků mohlo vyvolat reakci skrze článek 5 Severoatlantické smlouvy.[60] Situace je

---

[56] NAKASHIMA, Ellen, WARRICK, Joby. Stuxnet was *work of U. S. and Israeli experts, officials say* [online]. washingtonpost.com, 2. června 2012 [cit. 23. ledna 2018]. Dostupné na <https://www.washingtonpost.com/world/nationalsecurity/stuxnetwasworkofusandisraeliexpertsofficialssay/2012/06/01/gJQAlnEy6U_story.html?utm_term=.46da1cb989bf>.

[57] SINGER, Peter W. Stuxnet and Its Hiden Lessons on the Ethics of Cyberweapons. *Case Western Reserve Journal of International Law*, 2015, roč. 47, s. 83.

[58] Charta Spojených národů ze dne 26. června 1945, vyhlášena pod č. 30/1947 Sb., ve znění předpisů č. 127/1965 Sb. a č. 36/1999 Sb. Dále v textu jako „Charta OSN". Příklad je pouze ilustrativní, problematika Ius ad bellum není obsahem této práce.

[59] Dále v textu práce jako „NATO".

[60] Čl. 5 Severoatlantické smlouvy ze dne 4. dubna 1949, vyhlášené pod č. 66/1999 Sb.: „*Smluvní strany se dohodly, že ozbrojený útok proti jedné nebo více z nich v Evropě nebo Severní Americe bude považován za útok proti všem, a proto se dohodly, že dojde-li k takovémuto ozbrojenému útoku, každá z nich, uplatňujíc právo na individuální nebo kolektivní sebeobranu uznané článkem 51 Charty OSN, pomůže smluvní straně nebo stranám takto napadeným tím, že neprodleně podnikne sama a v součinnosti s ostatními*

ovšem složitější, jelikož v případě estonského incidentu se nepodařilo prokázat původce těchto útoků. To znamená, že není jisté, proti komu by Estonsko, popř. NATO mohlo uplatnit právo na sebeobranu. Označení aktéra, který je za útoky mezinárodněprávně odpovědný, je proto zásadní. V úvahu by mohl přijít koncept přičitatelnosti jednání státu, který je v doktríně i praxi mezinárodního práva znám, ale jeho uplatnění v kyberprostoru je fakticky problematické.[61]

Situace byla jiná v Gruzii, kde kybernetické operace probíhaly souběžně s těmi konvenčními. Jelikož zde došlo k užití síly ze strany Gruzie i Ruské federace, je nutné incident označit jako mezinárodní ozbrojený konflikt, z čehož plynou důsledky pro aplikaci příslušné mezinárodněprávní úpravy. Vojenské operace obou států nepochybně podléhaly úpravě mezinárodního humanitárního práva. Je ovšem sporné, zda se tato právní úprava vztahovala i na příslušné kybernetické operace. Pokud ano, bylo by nezbytné dále zkoumat, zda byly tyto útoky v souladu se zásadami a pravidly mezinárodního humanitárního práva. Například zda vytváření falešných webových stránek nebylo porušením zásady rozlišování, když jejich účinek cílil především na civilní obyvatelstvo.[62] Dále jelikož nebylo bezpochyby prokázáno, že by kybernetické operace byly řízeny Ruskou federací, vyvstává otázka, zda Ruská federace neporušila své mezinárodní závazky, když nezakročila proti původcům těchto útoků.[63] V této souvislosti se lze ptát, zda mohla Gruzie během probíhajícího ozbrojeného konfliktu použít sílu proti nestátnímu aktérovi operujícím z území jiného státu, kterým byla například teroristická organizace RBN.[64]

Konečně objev Stuxnetu vnesl do diskuze o možných prostředcích a metodách vedení boje novou rovinu, když se jednalo o první opravdovou kybernetickou zbraň a mohlo by na tento program být nahlíženo jako na prostředek vedení boje dle mezinárodního humanitárního práva. Myšlenku lze rozvinout ve smyslu možné existence ozbrojeného konfliktu na území Íránu. Jelikož se ovšem Stuxnet rozšířil i mimo cílené zařízení, tj. i mimo Írán, nabízí se otázka, zda mohl probíhat ozbrojený konflikt ve všech zemích, kde byla zjištěna jeho přítomnost. Opět zde hraje významnou roli absence prokázání původce programu. Pokud jej nelze určit, je nejisté, jakou povahu by případný ozbrojený konflikt měl, a kteří aktéři by byly jeho stranami. Dále nelze opomenout

---

stranami takovou akci, jakou bude považovat za nutnou, včetně použití ozbrojené síly, s cílem obnovit a zachovat bezpečnost severoatlantického prostoru…“ NATO později, na summitu ve Varšavě, plně uznalo, že kybernetické útoky mohou být srovnatelné s těmi konvenčními a je nutno s nimi počítat v rámci své kolektivní sebeobrany. Srov. Warsaw Summit Communiqué ze dne 9. června 2016, bod 70. Dostupné na <https://www.nato.int/cps/en/natohq/official_texts_133169.htm>.

[61] Vzhledem k propojenosti kybernetické infrastruktury a metodám maskování původce operace je vysoce obtížné identifikovat konkrétní odpovědnou fyzickou osobu stojící za útokem. Blíže podkapitola 2.3.1.

[62] Následky vytváření falešných webových stránek neměly na obyvatelé srovnatelné účinky jako kinetické operace, proto nedošlo k porušení zásady rozlišování. Blíže podkapitola 2.3.

[63] Každý stát má závazek vědomě neumožnit využití svého území k aktům, které poškozují práva jiného státu. MSD: *Corfu Channel case,* Judgement of April 9th, 1949, I. C. J. Reports 1949*,* odst. 22.

[64] Blíže k problematice VAN DER VYVER, Johan D. The ISIS Crisis and the Development of International Humanitarian Law. *Emory International Law Review*, 2016, roč. 30, č. 4, s. 531 - 563.

fakt, že se červ rozšířil i na jiná zařízení mimo původní cíl, čímž mohlo dojít ke kolizi s jednou ze základních zásad právní úpravy, a to zásadou rozlišování.

Možnosti kyberprostoru zasáhnout významné oblasti státní informační infrastruktury nutí státy uvažovat nad přehodnocením dosavadních pravidel mezinárodního práva. Státy se však musí vypořádat s prvky, jež odlišují kyberprostor od ostatních oblastí právní úpravy mezinárodního práva, kterými jsou například mořské právo, vesmírné právo aj.

2 Kyberprostor v kontextu mezinárodního humanitárního práva

Bylo již řečeno, že v současné vojenské doktríně je kyberprostor považován za pátou doménu vedení vojenských operací. Na rozdíl od ostatních domén, tedy země, moře, vzduchu a vesmíru, ale neexistuje explicitní smluvní úprava ani obyčejová pravidla mezinárodního práva upravující vedení vojenských operací v tomto prostoru. Na první pohled by tedy bylo možné jednoduše konstatovat, že právní úprava mezinárodního humanitárního práva nemá působnost v případě vojenských operací v kyberprostoru a státy nejsou omezeny žádnými pravidly pro vedení kybernetických operací. Pokud se ale blíže zaměříme na některá ustanovení právní úpravy, zjistíme, že se toto právní odvětví vyznačuje určitým specifickým znakem. Jeho systém je vystavěn tak, aby nevznikaly mezery v právní úpravě v důsledku technologického vývoje a rozvoje, tedy aby se zamezilo nemožnosti aplikace mezinárodního humanitárního práva na zbraně, které neexistovaly v době přijetí platného práva. Právní úprava obsahuje k překlenutí mezer několik nástrojů. Předtím, než budou analyzovány, je vhodné zmínit Tallinnský manuál, jehož cílem je vypořádat se implikacemi platné právní úpravy na kybernetické prostředky a metody vedení boje.

2.1 Tallinnský manuál

Projekt Tallinnského manuálu představuje prozatím nejkomplexnější akademickou práci zabývající se mezinárodním právem v souvislosti s kyberprostorem.

V roce 2013 byla publikována první verze s názvem „Tallinnský manuál mezinárodního práva aplikovatelného na kybernetické válečnictví". Jednalo se o projekt dvaceti renomovaných akademiků a praktiků mezinárodního práva, jenž identifikoval a stanovil 95 pravidel mezinárodního práva vztahujících se na kybernetické válečnictví. Rozsah práce byl omezen na oblast užití síly a mezinárodní humanitární právo.[65] Projekt zaštiťovalo CCDCOE,[66] což je mezinárodní vojenská organizace se sídlem v estonském Tallinnu, organizačně náležící pod NATO. Publikace tradicí navazuje na již vzniklé manuály, jimiž jsou San Remo manuál[67] nebo AMW manuál.[68] S těmito manuály ji pojí i to, že se jedná o právně nezávazný dokument. Vyjadřuje pouze právní názory jeho autorů, bez spojitosti s NATO nebo s názory jednotlivých států.[69] Struktura manuálu je dle jeho vedoucího, profesora Schmitta, taková, že základ tvoří tzv. černá pravidla, na jejichž formulaci

[65] SCHMITT, Michael (ed). Tallinn manual on the international law applicable to cyber warfare: Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. New York: Cambridge University Press, 2013, předmluva.
[66] Cooperative Cyber Defence Centre of Excellence.
[67] DOSWALD-BECK, Louise (ed). San Remo Manual on International Law Applicable to Armed Conflict at Sea. New York: Cambridge University Press, 1995, 257 s.
[68] Harvard Program on Humanitarian Policy and Conflict Research. Manual on International Law Applicable to Air and Missile Warfare. New York: Cabridge University Press, 2009, 56 s.
[69] SCHMITT: *Tallinn manual* …, s. 1.

musel být konsensus celého autorského pléna. Pravidla byla doplněna komentářem objasňujícím tzv. šedé zóny právní úpravy, a dále nastíněny problematické aspekty, na kterých nebylo dosaženo žádné shody.[70] Černá pravidla mají představovat takový stav práva, jaký je, tedy lex lata. Jako prameny pro formulaci pravidel autoři užili tradiční instrumenty mezinárodního humanitárního práva jako Haagské[71] a Ženevské úmluvy,[72] dále Studii MVČK o obyčejovém mezinárodním humanitárním právu,[73] a také již zmíněný San Remo manuál a AMW manuál. Důležité byly i vojenské manuály, mj. vojenský manuál Spojených států amerických, což bylo důležité pro identifikaci obyčejových norem především s ohledem na to, že Spojené státy nejsou smluvní stranou Dodatkového protokolu I k Ženevským úmluvám z roku 1949.[74]

Po vydání první verze následovaly práce na verzi druhé, ve snaze rozšířit záběr dokumentu i na právní úpravu mimo ozbrojený konflikt. Druhá verze tak obsahuje celkem 154 pravidel. Rozšíření obsahu bylo zvoleno především s ohledem na skutečnost, že od vydání první verze v roce 2013 bylo možné zaznamenat minimum případů, ve kterých by některá formulovaná pravidla byla použitelná. Absolutní většina kybernetických aktivit totiž probíhá mimo ozbrojený konflikt.[75] Kromě obsahu se druhá verze liší od té první ještě v jednom aspektu, a to dílčí změnou v procesu jejího vytváření. Během vývoje první verze zachovaly jednotlivé státy odstup a nijak se do přípravných prací nezapojovaly. Naproti tomu během prací na druhé verzi hostilo nizozemské ministerstvo zahraničních věcí tzv. Haagský proces, v rámci kterého vyzvalo jednotlivé státy, aby neoficiálně okomentovaly pracovní verzi. Tohoto procesu se zúčastnilo přes 50 států, které připojily své psané komentáře. I na jejich základě vznikla konečná verze. Opět však platí, že názory vyjádřené ve druhé verzi stále nejsou oficiálním postojem ani vyjádřením daných států, ale pouze autorů práce.[76] Druhá verze byla oficiálně publikována v roce 2017.

Autoři v obou verzích manuálu deklarují, že jejich cílem nebylo určit, jak bude právo regulovat kybernetické operace v budoucnu, ale jaký je stav práva ke dni vydání jednotlivých verzí. Zdůrazňují, že jejich názory nevyjadřují názory států ani organizací, jichž jsou členy. To samé platí

---

[70] Blíže k metodologii manuálu srov. SCHMITT, Michael. *CyCon 2012, Tallin Manual Part I* [online] youtube.com, 29. září 2012 [cit. 1. února 2018]. Dostupné na < https://www.youtube.com/watch?v=wY3uEo-Itso>.

[71] Soubor Úmluv přijatých na Haagských mírových konferencích v roce 1899 a 1907.

[72] Ženevská úmluva o zlepšení osudu raněných a nemocných příslušníků ozbrojených sil v poli, Ženevská úmluva o zlepšení osudu raněných, nemocných a trosečníků ozbrojených sil na moři, Ženevská úmluva o zacházení s válečnými zajatci, Ženevská úmluva o ochraně civilních osob za války, tyto vyhlášeny pod č. 65/1954 Sb.

[73] DOSWALD-BECK, Louise, HENCKAERTS, Jean-Marie (eds). Customary International Humanitarian Law. Volume I: Rules. New York: Cambridge University Press, 2005. 628 s.

[74] Dodatkový protokol k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí mezinárodních ozbrojených konfliktů ze dne 8. června 1977, vyhlášen pod č. 168/1991 Sb. Dále v textu jen „Protokol I".

[75] SCHMITT, Michael (ed). Tallinn manual 2.0 on the international law applicable to cyber operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excelence. New York: Cambridge University Press, 2017, předmluva.

[76] Tamtéž, s. 6.

pro identifikovaná obyčejová pravidla. Toto je nutné si uvědomit při práci s manuálem a jeho analýze.[77] Autoři se opírají pouze a jen o svoji autoritu jakožto autoritu uznávaných odborníků ve svých oborech. Význam manuálu je tak především v sumarizované právní analýze dotčených oblastí mezinárodního práva v kontextu kybernetických operací, doplněné debatou nad šedými oblastmi právní úpravy a identifikaci důležitých a často sporných otázek.[78] Manuál proto na základě své kvalitní metodologie a odbornosti autorského kolektivu bude podpůrným pramenem mezinárodního práva ve smyslu čl. 38 odst. 1 písm. d) Statutu Mezinárodního soudního dvora.[79]

Přijetí manuálu odbornou i laickou veřejností bylo různorodé. Část veřejnosti jej vnímala jako nejdůležitější dokument v oblasti kybernetického válečnictví a jasné pozitivum.[80] Jiní vnímají manuál jako prostředek, který může vést k legitimizaci kybernetické války. Dle jejich názorů aplikace tradičního mezinárodního humanitárního práva na kybernetickou oblast přináší nebezpečné závěry pro celý kybernetický svět.[81]

2.2 Nástroje pro překlenutí mezer

2.2.1 Martensova klauzule

V době přijímání prvních komplexních smluvních nástrojů mezinárodního humanitárního práva si státy byly vědomy, že do právní úpravy nelze zahrnout všechny myslitelné situace a způsoby vedení boje. V preambuli IV. Haagské úmluvy z roku 1907 o zákonech a obyčejích války pozemní, jejíž přílohou je i Řád zákonů a obyčejů války pozemní, je uvedeno, že „*Dokud nebude přijat komplexnější kodex válečného práva, považují Vysoké smluvní strany za vhodné deklarovat, že v případech nezahrnutých do jimi přijatého Řádu, obyvatelé a válčící osoby zůstávají pod ochranou a vládou principů mezinárodního práva, jak plynou ze zvyklostí mezi civilizovanými národy, ze zákonů humanity a příkazů veřejného*

---

[77] Zde je vhodné podotknout, že veřejnost tuto skutečnost často nebere v potaz. Manuál považuje za projekt NATO, nebo US Cyber Command (a potažmo Spojených států amerických). Srov. ADAMS, Michael J. *A Warning About Tallinn 2.0… Whatever It Says* [online]. lawfareblog.com, 4. ledna 2017 [cit. 11. ledna 2018]. Dostupné na <https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says>.

[78] Čas ukáže, jaké pozice vůči manuálu zaujmou státy. Zvláštní postavení již nyní mají Spojené státy americké, kde lze nalézt shodu mezi veřejně projevenými autoritativními názory na mezinárodní právo v kontextu kyberprostoru a obsahem manuálu. Blíže KESSLER, Oliver, WERMER, Wouter. Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare. *Leiden Journal of International Law*, 2013, roč. 26, č. 4, s. 806. Dále KOH, Harold Hongju. International Law in Cyberspace. *Harvard International Law Journal Online*, 2012, roč. 54, č. 4854, s. 1 - 12. Dostupné na <http://digitalcommons.law.yale.edu/fss_papers/4854/>.

[79] Statut Mezinárodního soudního dvora ze dne 26. června 1945, vyhlášen pod č. 30/1947 Sb., ve znění předpisů č. 127/1965 Sb. a 36/1999 Sb.

[80] BOWCOTT, Owen. *Rules of cyberwar: don't target nuclear plants or hospitals, says Nato manual* [online]. theguardian.com, 18 března 2013 [cit. 11. ledna 2018]. Dostupné na <https://www.theguardian.com/world/2013/mar/18/rules-cyberwarfare-nato-manual>.

[81] V tomto smyslu se vyjádřili i představitelé Ruské Federace, CHERNENKO, Alena. *Russia warns against NATO document legitimizing cyberwars* [online]. rbth.com, 29 květen 2013 [cit. 11. ledna 2018]. Dostupné na <https://www.rbth.com/international/2013/05/29/russia_warns_against_nato_document_legitimizing_cyberwars_26483.html>.

svědomí.“[82] Klauzule se stala předmětem mnoha výkladů. Dle restriktivního výkladu neobsahuje žádné pravidlo chování, pouze ideově potvrzuje platnost obyčejových pravidel i navzdory přijetí smluvních norem. Teleologický výklad reaguje na skutečnost, že žádný smluvní nástroj mezinárodního humanitárního práva není úplný. Bez této klauzule by každý prostředek nebo metoda vedení boje explicitně nezakázaný smluvní úpravou mohl být sám o sobě dovolený.[83] Extenzivní výklad dovozuje, že klauzule neodkazuje pouze na smluvní nebo obyčejové právo, ale i na „příkazy“ či „požadavky“ veřejného svědomí. Poukazuje tak na přirozenoprávní povahu dané normy, díky které je nutné použít na prostředky a metody vedení boje i obecné principy mezinárodního humanitárního práva. Klauzule je především výrazem zásady lidskosti.[84]

Kodifikaci klauzule obsahuje Protokol I v čl. 1 odst. 2: „*V případech, na které se nevztahuje tento protokol nebo jiné mezinárodní dohody, civilisté a kombatanti zůstávají pod ochranou a v rámci působnosti zásad mezinárodního práva vyplývajících z ustálených obyčejů, ze zásad lidskosti a z požadavků společenského svědomí.*“ Formulace ustanovení byla vložena do textu protokolu právě z důvodu, že žádná kodifikace nemůže dopodrobna obsáhnout všechny myslitelné situace nebo případy a předvídat vývoj společnosti. Její systematické umístění do úvodních ustanovení dokumentu podtrhuje zásadu lidskosti a její privilegované postavení v systému mezinárodního humanitárního práva. Ustanovení má navíc povahu obyčejového pravidla, jak vyplývá z judikatury mezinárodních soudů.[85] Mezinárodní soudní dvůr se již jednou vypořádal se situací, kdy panovala nejistota ohledně aplikace některých ustanovení mezinárodního práva na prostředky explicitně neřešené právní úpravou. Předmětem jeho poradního stanoviska byla legalita hrozby nebo užití jaderných zbraní. MSD poukázal na to, že všechny státy jsou zavázány těmi pravidly Protokolu I, která jsou pouhým výrazem již existujících obyčejových pravidel.[86] Dále zdůraznil, že: „*Z pouhého faktu, že určité typy zbraní nebyly zvláště řešeny na Konferenci v letech 1974 - 1977, nelze vyvozovat žádné věcné právní závěry (substantive issues) vztahující se k otázkám, které jejich užití vyvolávají.*“[87] Tyto závěry je nutné analogicky vztáhnout i na případ kybernetických prostředků a metod vedení. Základní principy a pravidla právní úpravy vystihují podstatu celého právního odvětví a zdůrazňují jeho humanitární charakter, jenž prozařuje celým systémem mezinárodního humanitárního práva. Tato pravidla a principy

---

[82] Autorem této formulace byl Fyodor Fyodorovich Martens, proto se pro klauzuli vžilo označení „Martensova klauzule“.
[83] PICTET, Jean a kol. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Geneva: Martinus Nijhoff Publishers, 1987, odst. 55. Srov. také Stálý dvůr mezinárodní spravedlnosti: *The Case of the S.S. „Lotus“,* Judgement of 7th September, 1927, Series A.–No. 10, str. 19.
[84] TICEHURST, Rupert. The Martens clause and the Laws of Armed Conflict. *International Review of the Red Cross,* 1997, č. 317. Dostupné na <https://www.icrc.org/eng/resources/documents/article/other/57jnhy.htm>.
[85] MSD: *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), Merits, Judgement, I. C. J. Reports 1986, odst. 218.
[86] MSD: *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I. C. J. Reports 1996, odst. 84.
[87] Tamtéž.

je nezbytné použít na všechny formy vedení boje i na všechny typy zbraní, jak ty z minulosti, přítomnosti i budoucnosti.[88] Není proto důvod, aby se systematicky přistupovalo odlišně k jaderným zbraním a kybernetickým zbraním, které proto budou podléhat základním zásadám mezinárodního humanitárního práva.

2.2.2 Čl. 36 Dodatkového protokolu I

Dalším ustanovením upravujícím vývoj a nasazení nových zbraní je čl. 36 Protokolu I. Ten stanovuje, že „*Při studiu, vývoji, získávání nebo zavádění nových druhů zbraní, prostředků nebo způsobů vedení boje je Vysoká smluvní strana povinna určit, zda jejich použití není za některých nebo za všech okolností zakázáno tímto Protokolem nebo jinou normou mezinárodního práva aplikovatelnou na tuto Vysokou smluvní stranu.*“ Ustanovení představuje jediný propojovací článek mezi čl. 35 Protokolu I obsahujícím základní pravidla způsobů a prostředků vedení boje a možností států vyvíjet zbraně nové.[89] Státy jsou dle čl. 36 zavázány provést zhodnocení toho, zda jimi vyvíjená zbraň neodporuje pravidlům obsaženým v Protokolu I nebo v jiných použitelných pravidlech mezinárodního práva.[90] Zhodnocení by mělo odpovídat běžnému užití zbraně v čase takového posuzování. Pokud stát zhodnocení neprovede, bude odpovědný v každém případě, kdy bude zbraní způsobena protiprávní škoda.[91] Státy v průběhu tohoto procesu ovšem nemusí analyzovat všechny myslitelné situace nasazení zbraně, protože téměř každá zbraň muže být použita způsobem odporujícím mezinárodnímu humanitárnímu právu.[92] Dle doktríny čl. 36 obsahuje dále závazek vytvořit vnitrostátní procedury pro účely stanovení legality dotčené zbraně. O formě této procedury, nikoliv konkrétním obsahu, musejí být ostatní smluvní státy na vyžádání informovány. Výsledek vlastního zhodnocení není právně závazný a nemá žádné účinky pro ostatní státy.[93]

Ustanovení je ovšem závazné pouze pro smluvní strany Protokolu I, jelikož se nejedná o kodifikaci obyčejového pravidla.[94] Pro nesmluvní státy lze obdobné pravidlo dovodit z čl. 1 IV.

---

[88] Tamtéž, odst. 86.

[89] Čl. 35:

1. *V ozbrojeném konfliktu nemají strany v konfliktu neomezené právo volby způsobů a prostředků vedení boje.*
2. *Je zakázáno používat zbraní, munice, materiálů a způsobů vedení boje, které by svou povahou způsobovaly nadměrná zranění nebo zbytečné útrapy.*
3. *Je zakázáno používat způsobů nebo prostředků vedení boje, jejichž cílem je způsobit, nebo u nichž se dá očekávat, že mohou způsobit rozsáhlé, dlouhodobé a vážné škody na životním prostředí.*

[90] Odlišný mechanismus monitorování legality zbraní obsahuje čl. 8 Úmluvy o zákazu nebo omezení použití některých konvenčních zbraní, které mohou způsobovat nadměrné utrpení nebo mít nerozlišující účinky, vyhlášené pod č. 21/1999 Sb., ve znění předpisu č. 115/2006 Sb. m. s. Blíže také International Commitee of the Red Cross. A Guide to the Legal Review of New Weapons, Means and Methods of Warfare. Measures to Implement Article 36 of Additional Protocol I of 1977. Geneva, 2006, s. 6.

[91] PICTET: *Commentary*…, odst. 1466.

[92] Tamtéž, odst. 1469. Jako komplementární doplněk článku 36 působí článek 82, který stanovuje povinnost zajistit přítomnost právních poradců v ozbrojených silách při aplikaci Ženevských úmluv a jejich protokolů.

[93] Tamtéž, odst. 1470 a 1481.

[94] SCHMITT: *Tallinn manual 2.0*…, s. 465.

Haagské úmluvy z roku 1907[95] a společného čl. 1 Ženevských úmluv z roku 1949.[96] Tyto články stanovují obecnou povinnost používat prostředky a metody vedení boje v souladu s pravidly mezinárodního humanitárního práva, jež jsou pro smluvní státy závazné.[97] Oproti ustanovení čl. 36 Protokolu I je závazek užší, jelikož se vztahuje pouze na nabývání a používání zbraní, nikoliv např. na jejich vývoj. Užší je též v tom, že se soulad prostředků a metod posuzuje pouze vzhledem k mezinárodnímu humanitárnímu právu, a nikoliv jiným použitelným normám mezinárodního práva.

Proces zhodnocení může být zvlášť problematický v kontextu kybernetických prostředků a metod vedení boje, které samy o sobě předpokládají vysokou úroveň znalostí informačních technologií a v důsledku jejich malé četnosti či zkušenosti s nimi je obtížné predikovat jejich fungování a účinek.[98] Může se proto stát, že se určitý program vyvinutý jako bojový prostředek cestou k cíli skrze kyberprostor pozmění, a poté bude mít jiné následky, než měla jeho originální verze.[99] Je tak obtížné, až technicky nemožné přesně předpovídat chování dané zbraně.[100] V obecné rovině bude potřeba zvážit, zda kybernetické prostředky nebo metody v běžném operačním nasazení nezpůsobují nadměrné utrpení, zda nejsou nerozlišující povahy per se a zda existuje zvláštní smluvní ustanovení nebo obyčejové pravidlo, které by jejich nasazení upravovalo.

Lze shrnout, že právní úprava obsahuje nástroje, díky kterým lze vůbec uvažovat o její možné aplikaci v souvislosti s kybernetickými prostředky a metodami vedení boje. Ke konečnému potvrzení aplikace je nutné dále analyzovat některé problematické aspekty působnosti.

2.3 Působnost norem mezinárodního humanitárního práva

2.3.1 Působnost ratione materiae

Základním předpokladem pro určení působnosti je existence mezinárodního ozbrojeného konfliktu dle společného článku 2 Ženevských úmluv z roku 1949[101] nebo vnitrostátního

---

[95] Čl. 1 IV. Haagské úmluvy z roku 1907 o zákonech a obyčejích války pozemní: „*Smluvní mocnosti vydají rozkazy svým pozemním ozbrojeným silám tak, aby byly v souladu s Řádem války pozemní, připojeného k této Úmluvě.*"

[96] Společný článek 1: „*Vysoké smluvní strany se zavazují, že za všech okolností budou zachovávati tuto Úmluvu a zajistí její zachovávání.*"

[97] Povinnost ve vztahu k prostředkům vedení boje již vykrystalizovala v obyčejovou normu, srov. SCHMITT: *Tallinn manual 2.0*…, s. 465.

[98] Právní úprava neobsahuje žádný standard nebo požadavky, jimiž mají být zbraně hodnoceny.

[99] Tak může být obtížná simulace prostředí, ve kterém bude kybernetický prostředek účinkovat. Tato simulace bude vyžadovat pokročilé techniky počítačových modelací. Tamtéž, s. 467.

[100] Podobně je náročné provést test přiměřenosti užití dané zbraně, blíže viz podkapitola 3.2.

[101] Společný článek 2: „*Nehledíc na ustanovení, která mají nabýt účinnosti již v míru, bude se tato úmluva vztahovati na všechny případy vyhlášené války nebo jakéhokoliv jiného ozbrojeného konfliktu vzniklého mezi dvěma nebo více Vysokými smluvními stranami, i když válečný stav není uznáván jednou z nich. Úmluva se bude rovněž vztahovati na všechny případy částečné nebo úplné okupace celého území některé Vysoké smluvní strany, i když se tato okupace nesetká s řádným vojenským odporem.*"

ozbrojeného konfliktu podle společného článku 3 těchto úmluv[102] či dle čl. 1 Dodatkového protokolu k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí ozbrojených konfliktů nemajících mezinárodní charakter.[103]

Jelikož smluvní úprava neobsahuje záměrně definici mezinárodního ozbrojeného konfliktu, je nutné nahlédnout do doktríny a judikatury. Komentář MVČK ke společnému článku 2 definuje mezinárodní ozbrojený konflikt jako „*Jakékoliv neshody vzniklé mezi dvěma státy vedoucí k nasazení členů ozbrojených sil jsou ozbrojeným konfliktem ve smyslu článku 2, dokonce i když jedna ze Stran popírá existenci válečného stavu. Není podstatné, jak dlouho konflikt trvá, jaký je rozsah krutostí, nebo jak početné jsou účastnící se ozbrojené síly.*“[104] V souladu s touto ustálenou definicí doplňuje komentář MVČK k Protokolu I, že „*…humanitární právo ovládá jakýkoliv spor mezi dvěma státy zahrnující užití ozbrojených sil. Délka trvání konfliktu ani jeho intenzita nehrají roli: právo musí být aplikováno v plném rozsahu vyžadovaném situací chráněných osob a objektů.*“[105] Judikatura přijala k vymezení situace ozbrojeného konfliktu vlastní definici: „*ozbrojený konflikt existuje kdykoliv dojde k uchýlení se k užití ozbrojených sil mezi státy.*“[106] Nečiní větší obtíže určit, zda došlo k užití ozbrojených sil mezi státy, pokud byly využity tradiční, tj. konvenční, kinetické prostředky vedení boje. V případě kybernetických prostředků a metod vedení boje může být situace komplikovanější.

Kybernetické prostředky jsou svojí povahou nekinetické a představa jejich nasazení jako bojových prostředků implikujících užití ozbrojené síly vyžaduje přinejmenším dobrou představivost. Často se bude jednat až o nepřímé následky kybernetických operací. Pokud jsou kybernetické operace součástí širšího vedení bojových operací, jako tomu bylo například v rámci

---

[102] Společný článek 3: „*V případě ozbrojeného konfliktu, který nemá mezinárodní ráz a který vznikne na území některé z Vysokých smluvních stran…*“

[103] Čl. 1 odst. 1 Dodatkového protokolu k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí ozbrojených konfliktů nemajících mezinárodní charakter, , ze dne 8. června 1977, vyhlášeného pod č. 168/1991 Sb.: „*Tento Protokol, který rozvíjí a doplňuje společný článek 3 Ženevských úmluv z 12. srpna 1949 a nemění existující podmínky jeho aplikace, se bude vztahovat na všechny ozbrojené konflikty, které nejsou obsaženy v článku 1 Dodatkového protokolu k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí mezinárodních ozbrojených konfliktů a k nimiž dochází na území Vysoké smluvní strany mezi jejími ozbrojenými silami a disidentskými ozbrojenými silami nebo jinými organizovanými ozbrojenými skupinami vykonávajícími pod odpovědným velením takovou kontrolu nad částí jejího území, která jim umožňuje vést trvalé a koordinované vojenské operace a aplikovat tento Protokol.*“
Odst. 2: „*Tento Protokol nebude aplikován v případě vnitřních nepokojů a napětí, jako jsou vzpoury, izolované a sporadické násilné činy a ostatní činy podobné povahy, které se nepovažují za ozbrojené konflikty.*“ Dále v textu jako „Protokol II“.

[104] International Commitee of the Red Cross. *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field.* 2. vydání. 2016, odst. 222. Komentář dále doplňuje, že původní definice obsažená ve verzi komentáře z roku 1958 je příliš úzká. Je proto správné označit jako situace mezinárodního ozbrojeného konfliktu i situace, kdy dochází k užití síly ze strany jednoho státu vůči jinému, nikoliv pouze v případě vzájemného uchýlení se k užití síly ze strany obou státu. Proto bude jako mezinárodní ozbrojený konflikt označena i situace námořní nebo vzdušné blokády jednoho státu vůči druhému. V kybernetickém kontextu se nabízí otázka, zda a za jakých podmínek by se mohlo jednat o kybernetickou blokádu. Srov. RYAN, Johny. „*iWar": A New Threat, its Convenience – and our Increasing* [online]. nato.int., 2007 [cit. 11. ledna 2018]. Dostupné na <htt ps://www.nato.int/docu/review/2007/issue4/english/analysis2.html>.

[105] PICTET: *Commentary*…, odst. 62.

[106] ICTY: *The Prosecutor v. Tadić*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT 94-1-A, 2 October 1995, odst. 70.

incidentu mezi Gruzií a Ruskou federací v roce 2008, není pochyb o existenci mezinárodního ozbrojeného konfliktu.[107] Mohlo by se tedy zdát, že konflikt vedený pouze kybernetickými prostředky postrádá definiční prvek ozbrojeného konfliktu.[108] Většina odborníků se ovšem přiklání k názoru, že i samotné vedení kybernetických operací[109] může vyvolat ozbrojený konflikt, pokud jsou následkem kybernetických operací smrt nebo zranění osob nebo poškození či zničení majetku. V takovém případě není důvod právně rozlišovat situace nasazení konvenčních zbraní a užití kybernetických zbraní s obdobným účinkem.[110] Podobně jako u konvenčních zbraní musí být ovšem kybernetické operace provedeny v kontextu ozbrojeného konfliktu.[111] Pokud kybernetické operace nebudou provedeny v kontextu ozbrojeného konfliktu a nebudou mít srovnatelné následky se zbraněmi konvenčními, nelze uvažovat o působnosti právní úpravy. V úvahu přichází oblast špionáže a možné porušení zásady neintervence ve smyslu čl. 2 odst. 1 Charty OSN.[112] Lze shrnout, že použití kybernetických prostředků a metod vedení boje lze v určitých případech označit za uchýlení se k užití ozbrojených sil ve smyslu definic mezinárodního ozbrojeného konfliktu.

Mezinárodní ozbrojený konflikt ovšem musí být nejen „ozbrojený", ale také mezinárodní, tzn., že nepřátelství musí probíhat alespoň mezi dvěma státy. Určení, zda je nepřátelství vedeno mezi dvěma státy, musí být provedeno na základě právní úpravy přičitatelnosti jednání státu upravené v rámci odpovědnosti státu. Působnost se tedy nebude vztahovat pouze na akty členů ozbrojených složek státu, ale musí být rozšířena i na činnost dalších osob jednajících jako státní agenti de iure nebo de facto.[113] Jednání přičitatelné státu by mohlo být jednání nestátní ozbrojené skupiny, která je pod celkovou kontrolou jednoho ze států vedoucího nepřátelství vůči jinému, což by vedlo k charakterizaci konfliktu jako mezinárodního.[114] Pokud tedy stát vykonává celkovou

---

[107] SCHMITT: *Tallinn Manual 2.0*…, s. 376.
[108] ICRC*: Commentary on the first*…, odst. 254.
[109] Zda je pro aplikaci mezinárodního humanitárního práva dostačující i jediná kybernetická operace s následky srovnatelnými s těmi kinetickými srov. SCHMITT: *Tallinn manual 2.0*…, s. 383.
[110] SCHMITT, Michael. Classification of Cyber Conflict. *Journal of Conflict & Security Law*, 2012, roč. 17, č. 2, s. 251.
[111] SCHMITT: *Tallinn manual 2.0*…, s. 375.
[112] Pokud se stát A pokusí získat pomocí kybernetické operace obchodní tajemství soukromé korporace ve státě B, mohlo by se jednat o narušení suverenity státu B a porušení zásady rovnosti. Nikoliv o užití síly ze strany státu A.
[113] MELZER, Nils. *Cyberwarfare and International Law.* UNIDIR Resources, 2011, s. 24. Dostupné na http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf. Dále srov. čl. 7 a 8 International Law Commission. *Draft Articles on Responsibility of States for Internationally Wrongful Acts with commentaries.* Yearbook of the International Law Commission, Vol. II, Part Two, A/CV.4/SER.A/2001Add1 (Part 2), 2001.
[114] „*Kontrola vyžadovaná mezinárodním právem může být považována za existující, když má stát (nebo v kontextu ozbrojeného konfliktu, Strana konfliktu) roli v organizování, koordinaci nebo plánování vojenských akcí vojenské skupiny, včetně jejího financování, výcviku a vybavování nebo poskytování operační podpory této skupině.*" ICTY: *The Prosecutor v. Tadić,* Judgement of the Appeals Chamber, IT-94-1-A, 15 July 1999, odst. 137. Mezinárodní právo zná i jinou teorii přičitatelnosti jednání státu. Jedná se o tzv. teorii efektivní kontroly nad osobami. Jelikož se však jedná o přísnější standard, než představuje teorie celkové kontroly, byla by její aplikace v souvislosti s kybernetickými prostředky a metodami vedení boje velmi neefektivní. K teorii efektivní kontroly srov. MSD: *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of

kontrolu nad organizovanou skupinou hackerů, která naboural kritické body strategické infrastruktury jiného státu a tím způsobí značné škody, lze situaci mezi oběma státy charakterizovat jako mezinárodní ozbrojený konflikt.[115] Test celkové kontroly nelze užít v případě jednání jednotlivce nebo skupiny nevykazující dostatečnou úroveň organizace. V takovém případě by jedinci nebo skupina museli dostat specifické příkazy nebo instrukce od státu ohledně svého chování.[116] Posuzování existence celkové kontroly nad určitou nestátní skupinou, stejně jako určení zdroje nebo původce kybernetické operace, popřípadě existence specifických instrukcí, může ale působit významné důkazní obtíže kvůli povaze kyberprostoru.[117]

Vzhledem k četnosti a často skutkové složitosti vnitrostátních ozbrojených konfliktů, majících převážně asymetrický charakter, představuje problematika působnosti právní úpravy u těchto konfliktů soustavnou výzvu současnému mezinárodnímu právu.[118] Prvek zapojení kybernetických prostředků a metod vedení boje situaci dále komplikuje.

Právní úprava obsažená ve společném článku 3 Ženevských úmluv a v čl. 1 Protokolu II upravuje rozdílné předpoklady pro vymezení vnitrostátního ozbrojeného konfliktu. Vnitrostátní ozbrojený konflikt se od toho mezinárodního liší jednak povahou bojujících stran,[119] ale především vyžadovanou mírou intenzity bojových operací a určitým stupněm organizovanosti bojujících stran.[120] Možným ukazatelem určujícím intenzitu konfliktu může být závažnost jednotlivých útoků, jejich potenciál přerůst v ozbrojená střetnutí, územní rozsah a trvání takových útoků, mobilizace a počet zapojení vládních sil včetně množství a distribuce zbraní mezi stranami konfliktu.[121] Ozbrojenou skupinu lze považovat za organizovanou, pokud vykazuje znaky vytvořené hierarchie a struktury velení, jež umožňuje dle potřeby měnit taktiku vedení nepřátelství. Po vojenském vzoru má stanovenou strukturu hodností nebo rozdělení úkolů a je schopna vytrvale vést vojenské

America), Merits, Judgement, I. C. J. Reports 1986, odst. 166. Komplexní analýza problematiky přičitatelnosti jednání státu v kyberprostoru však jde nad rámec této práce.

115 SCHMITT: *Tallinn manual 2.0*…, s. 381.

116 ICTY: *The Prosecutor v. Tadić,* Judgement of the Appeals Chamber, IT-94-1-A*,* 15 July 1999, odst. 137. Dobrým příkladem může být incident v Estonsku v roce 2007, který na základě důkazní nouze nemohl být posouzen jako mezinárodní ozbrojený konflikt.

117 MELZER: *Cyberwarfare*…, s. 24.

118 FAIX, Martin. *Law of Armed Conflict and Use of Force. Part Two-Limiting the Effects of War: International Law of Armed Conflict*. Olomouc: Vydavatelství Univerzity Palackého, 2013, s. 18.

119 Bojujícími stranami nejsou státy.

120 ICTY: *The Prosecutor v. Tadić,* Judgement of the Appeals Chamber, IT-94-1-A*,* 15 July 1999, odst. 70. Na tuto koncepci navázal v čl. 8 odst. 2 písm. d) Římský statut Mezinárodního trestního soudu, ze dne 17. července 1998, vyhlášen pod č. 84/2009 Sb. m. s., ve znění předpisu č. 16/2016 Sb. m. s. Dále také ICTY: *The Prosecutor v. Furundžija,* Trial Chamber Judgement, IT-95-17/1-T, 10 December 1998, odst. 59 a ICTY: *The Prosecutor v. Delalić,* Trial Chamber Judgement, IT-96-21-T, 16 November 1998, odst. 183.

121 ICTY: *The Prosecutor v. Mrkšić*, Trial Chamber II Judgement, IT-95-13/1-T, 27 September 2007, odst. 407.

operace ve větším měřítku.[122] Protokol II navíc vyžaduje, aby nestátní disidentská ozbrojená skupina nebo jiná ozbrojená skupina vykonávala kontrolu nad částí území.[123]

Při použití výše vymezených podmínek existence vnitrostátního ozbrojeného konfliktu na prostředí kybernetických operací lze dojít k závěru, že samotné kybernetické operace prováděné v rámci širší skupiny naplní kritéria vnitrostátního ozbrojeného konfliktu v úplném minimu případů. Většina případů kybernetických operací spočívá v znepřístupnění určitých síťových služeb, narušení nebo zničení dat a síťovém využití jiných zařízení. Tyto operace, i když by byly provedeny ve větším měřítku, nejspíše nedosáhnou intenzity požadované pro stanovení existence ozbrojeného konfliktu.[124] Kritérium intenzity by mohlo být naplněno pouze v případě, kdyby kybernetické operace byly vedeny spolu s těmi kinetickými v dostatečném rozsahu a intenzitě. Popřípadě pokud by samotné kybernetické operace byly svojí povahou velmi násilné a narušovaly by většinu důležitých státních funkcí. Ještě komplikovanější může být naplnění kritéria organizovanosti. Pro hackerské skupiny je typické, že jejich organizovanost probíhá virtuálně. To znamená, že se neorganizují na určitém fyzickém místě jako jiné ozbrojené skupiny, ale organizují se online, v kyberprostoru.[125] Není také výjimkou, že kybernetické útoky vedené větším počtem útočníků neprobíhají koordinovaně ve smyslu jednotného velení, ale původce útoku vymyslí určitý algoritmus útoku, který poté využívají ostatní útočníci, aniž by byli součástí větší skupiny.[126] Ozbrojená skupina působící online bude pouze velmi obtížně vykonávat kontrolu nad určitou částí území, což se neobejde bez fyzické přítomnosti vlastních členů. Taktéž si nelze dobře představit, že by taková skupina mohla být schopna implementovat Protokol II.[127]

2.3.2 Působnost ratione tempore, personae a loci

Působnost ratione tempore je tradičně chápána jako časové ohraničení působnosti konkrétní právní úpravy. Působnost mezinárodního humanitárního práva existuje od okamžiku faktického započetí okupace nebo nepřátelství do momentu dosažení míru.[128] Časová působnost nečiní v kontextu kyberprostoru aplikační nejasnosti. Totéž platí pro působnost osobní. V kyberprostoru jsou a budou primárním adresátem norem mezinárodního práva státy. V určitých případech mohou

---

[122] ICTY: *The Prosecutor v. Limaj*, Trial Chamber II Judgement, IT-03-66-T, 30 November 2005, odst. 129.
[123] Kontrola musí skupině umožňovat provádění trvalých a koordinovaných vojenských operací a aplikovat pravidla obsažená v Protokolu II. Naproti tomu společný článek 3 Ženevských úmluv kritérium kontroly nevyžaduje. Může se však jednat o podpůrný prvek pro určení existence ozbrojeného konfliktu.
[124] SCHMITT: *Tallinn manual 2.0*…, s. 389.
[125] Zda může být skupina, která se organizuje pouze virtuálně, označena za organizovanou, je sporné. Bude záležet na dalších prvcích organizovanosti, jakými mohou být řízený výběr cílů nebo společné vytváření nástrojů pro operace.
[126] Viz. poznámka pod čarou č. 31.
[127] PICTET: *Commentary*…, odst. 4470.
[128] DAVID: *Mezinárodní*…, s. 389.

být subjekty i hackerské skupiny nebo jednotlivci, pokud budou například součástí opozičních skupin nebo národně-osvobozeneckých hnutí.

Problematičtější je aplikace místní působnosti norem, tedy působnosti ratione loci. Místní působnost určuje, na jakém území bude nutné dané normy aplikovat. Vymezení místní působnosti nenalezneme ve smluvním právu, jeho obsahem se však zabývala judikatura. Ta na základě obyčejových pravidel dovodila, že „*mezinárodní humanitární právo se aplikuje na celém území válčících stran nebo, v případě vnitrostátních ozbrojených konfliktů, na celém území pod kontrolou bojující strany, bez ohledu na to, zda tam probíhají skutečné boje nebo nikoliv.*“[129] Právní úprava tak pracuje s vymezením území jako prostoru náležejícího určitému subjektu. Jak bylo vysvětleno v podkapitole 1.1, kyberprostor s těmito termíny neoperuje. Neexistuje ekvivalent území válčící strany v kyberprostoru. Pravidla místní působnosti bude možné užít pouze na fyzickou vrstvu kyberprostoru, tj. na kybernetickou infrastrukturu, popřípadě na cíle kybernetických operací mající fyzický rozměr.[130]

Posledním krokem pro vymezení situací, na které bude nezbytné aplikovat právní úpravu, je určení, kdy lze kybernetické operace považovat za útok ve smyslu mezinárodního humanitárního práva.

2.4 Kybernetická operace jako útok ve smyslu mezinárodního humanitárního práva

Účelem a smyslem mezinárodního humanitárního je mj. stanovit stranám ozbrojeného konfliktu omezení ve volbě prostředků a metod vedení boje.[131] Tato omezení se nevyhýbají vedení boje či nepřátelství v kyberprostoru, tedy kybernetickým prostředkům a metodám vedení boje.[132] Je vhodné vymezit a důrazně odlišovat situace, kdyby se určité jednání označilo za kybernetický útok, avšak právní terminologií by se o útok nejednalo. Důraz na rozlišování terminologie nabývá na významu tím, že pouze ve specifických situacích, které lze subsumovat pod skutkové podstaty právních norem mezinárodního humanitárního práva, lze na takové situace nazírat jeho optikou. Vhodným příkladem může být incident v Estonsku z roku 2007. Ačkoliv novináři často zmiňovali kybernetické útoky ve vztahu ke skutkovému stavu incidentu, nebyla naplněna kritéria ozbrojeného

[129] ICTY: *The Prosecutor v. Tadić*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT 94-1-A, 2 October 1995, odst. 70.
[130] Fyzickým rozměrem bude v případě útoku na určitá data lokalita zařízení, které je uchovává, např. konkrétní server. Viz SCHMITT: *Tallinn manual 2.0*…, s. 378. Na druhou stranu je možné, aby stát skrze kybernetickou operaci porušil pravidla mezinárodního práva týkajících se neutrality, pokud je tato operace vedena přes zařízení neutrálních států. Blíže k problematice kybernetických operací a práva neutrality srov. např. ROSCINI, Marco. *Cyber Operations and the Use of Force in International Law*. 1. vydání. New York: Oxford University Press, 2014, s. 246 - 277.
[131] ONDŘEJ, Jan a kol. *Mezinárodní humanitární právo*. 1. vydání. Praha: C. H. Beck, 2010, s. 7.
[132] V anglicky psané literatuře se užívá zastřešujícího pojmu „Cyber Warfare“ pro označení kybernetických prostředků a metod vedení boje. Pojmosloví v češtině není ustálené.

konfliktu. Nejednalo se proto o kybernetické útoky v právním slova smyslu, ale o kybernetické operace mimo působnost mezinárodního humanitárního práva.

Pojem kybernetická operace obecně vyjadřuje redukci informace do elektronického formátu a její přemístění mezi fyzickými komponenty kybernetické infrastruktury.[133] Vojenské manuály dále kategorizují kybernetické operace jako kybernetické útoky (*computer network attacks*), síťová využití (*computer network exploitations*) a síťové obranné operace (*computer network defence*).[134] Kybernetické útoky jsou ve vojenské doktríně vymezeny jako „*akce vykonané skrze užití počítačové sítě, jejichž účelem je narušení, zapření, znehodnocení nebo zničení informace obsažené v počítačích nebo počítačových sítích, nebo počítačů či počítačových sítí.*“[135] Tato definice slouží pouze k operačně-doktrinálnímu odlišení vojenských operací, označovaných jako kybernetické útoky, od ostatních kategorií vojenských operací. Neříká nic o právní povaze takové operace. Nepřesná označování kybernetických operací za útoky působí nejasnosti a vyvolává kontroverze mezi právníky z různých právních odvětví.[136] Je proto nezbytné vymezit, které kybernetické operace lze označit za útoky ve smyslu mezinárodního humanitárního práva.

Vztah kybernetických operací a pojmu útok patří k těm nejdiskutovanějším otázkám, kterých se dotýká téměř každá práce psaná na téma kyberprostoru a mezinárodního práva. Pojem útok odkazuje na určitý druh vojenských operací vedených během ozbrojeného konfliktu, na který se aplikují příslušné zákazy a omezení plynoucí z právní úpravy.[137] Definici pojmu útok nalezneme v čl. 49 odst. 1 Protokolu I: „*Útoky jsou násilné činy proti protivníkovi, a to jak útočné, tak i obranné povahy*.“ Jádrem problematiky je myšlenka, zda lze považovat kybernetické operace za násilné činy nebo nikoliv, především s ohledem na jejich nekinetickou povahu. Některé kybernetické operace totiž působí pouze nepříjemnosti (*inconvenience*) či malou škodu. Příkladem může být dočasné narušení komerční nebo vojenské počítačové sítě, proniknutí k osobním údajům osob, popřípadě omezená přístupnost k některým webovým stránkám.[138] Následky kybernetických operací tak vždy nenaplní hranici nutnou pro jejich označení za násilné činy ve smyslu čl. 49 odst. 1 Protokolu I. Stanovení

---

[133] MELZER: *Cyberwarfare*…, s. 5.

[134] U.S. Department of Defense. Law of War Manual. June 2015 (updated December 2016), s. 1013. Dostupné na <https://www.defense.gov/Portals/1/Documents/law_war_manual15.pdf>.

[135] REMUS, Titiriga. Cyber-attacks and International law of Armed Conflicts: A „Jus ad Bellum“ Perspective. *Journal of International Commercial Law and Technology*, 2013, roč. 8, č. 3, s. 179. Stejně NATO. *Glossary of Terms and Definitions*. AAP-06. Edition 2014. Dostupné na <http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6EN.pdf>.

[136] Blíže SCHMITT, Michael. „Attack“ as a Term of Art in International Law: The Cyber Operations Context. In CZOSSECK, Christian, OTTIS, Rain, ZIOLKOWSKI, Katharina (eds). *Proceedings of the 4th International Conference on Cyber Conflict*. Tallinn: CCDCOE Publications, 2012, s. 284.

[137] Čl. 51 odst. 2 věta první Protokolu I: „*Civilní obyvatelstvo jako takové, jakož i jednotlivé civilní osoby nesmějí být předmětem útoku.*“ Shodně SCHMITT: *„Attack“ as a*…, s. 286. Schmitt také zdůrazňuje rozdíl v pojmech „útok“ ve smyslu Ius in bello a „ozbrojený útok“ ve smyslu Ius ad bellum.

[138] Často se bude jednat o případy kybernetické špionáže nebo kybernetických psychologických operací. Srov. KODAR, Erik. Applying the law of armed conlfict to cyber attacks: From the Martens Clause to Additional Protocol I. *ENDC Proceedings*, 2012, roč. 15, s. 111.

hranice může být komplikované, což dokazuje i četnost diskuze vedené na toto téma.[139] Při textaci čl. 49 odst. 1 bylo myšleno především na civilní obyvatelstvo. Článek by proto měl být vykládán extenzivně především v případě, že by následky kybernetických operací měla být postižena civilní populace.[140] Naplnění pojmu „násilí" v čl. 49 odst. 1 má být určeno na základě následků vojenských operací, které budou v případě osob a objektů fyzické, a pouze v případě osob i duševní.[141] Násilnými akty ale nemohou být rozuměny pouze akty, jejichž následkem je působení kinetické energie. I chemické nebo biologické zbraně nemají obvykle kinetické účinky na své cíle, ačkoliv je všeobecně uznáváno, že konstituují útoky, které jsou předmětem mezinárodního humanitárního práva.[142]

Odborníci se shodují, že pro určení rozsahu termínu útok ve smyslu čl. 49 odst. 1 Protokolu I je rozhodující, jaký efekt může být vyvolán kybernetickou operací, nikoliv vlastní povaha kybernetické operace.[143] Tento závěr je správný. Pokud by se lpělo na přístupu zdůrazňujícím povahu kybernetické operace, tedy tzv. „instrument-based" přístupu, celé spektrum kybernetických operací s ničivými důsledky by nemohlo být kvalifikováno jako útoky.[144] Pojmu násilí je tak nutné rozumět ve smyslu násilných následků, nikoliv násilných činů.[145]

Shoda ale nepanuje na kvalifikaci kybernetických operací, jejichž následkem je obsazení nebo neutralizace objektu. Tyto operace způsobí blokaci nebo znepřístupnění obvyklé funkce daného objektu, avšak fakticky nemusí způsobit jeho poškození. Zastánci výkladu, že i takovéto kybernetické operace lze podřadit pod kybernetické útoky, argumentují čl. 52 odst. 2 Protokolu I, který ve své druhé větě staví naroveň obsazení a neutralizaci vojenského objektu jeho částečnému nebo celkovému zničení.[146] Odpůrci tohoto výkladu poukazují na systematiku protokolu a význam slov v čl. 49 odst. 1, ze kterých je patrné, že kybernetické operace, pokud nejsou již svojí povahou násilné, musí mít alespoň násilné důsledky. Svá tvrzení dále opírají o další ustanovení protokolu,

---

139 Srov. DOSWALD-BECK. Louise. Some Thoughts on Computer Network Attack and the International Law of Armed Conflict. *International Law Studies*, 2002, roč. 76, s. 165. Dále např. DINSTEIN, Yoram. Computer Network Attacks and Self-Defence. *International Law Studies*, 2002, roč. 76, s. 103.

140 PICTET: *Commentary*…, odst. 1884.

141 KODAR: *Applying*…, s. 112. Příkladem duševních následků může být šíření strachu nebo teroru prostřednictvím kybernetických operací ve smyslu čl. 51 odst. 2 Protokolu I. Takovými následky ale nebude například šíření propagandy zaměřené na civilní obyvatelstvo.

142 ICTY: *The Prosecutor v. Tadić*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995, odst. 120 a 124.

143 SCHMITT, Michael. Wired Warfare: Computer Network Attack and Jus in Bello. *International review of the Red Cross*, 2002, roč. 84, č. 846, s. 373.

144 SCHMITT: *Tallinn manual 2.0*…, s. 415.

145 Tamtéž. Tak kybernetická operace, jejímž následkem by byla změna fungování systému ovládajícího elektrárnu a její požár, bude považována za násilný čin ve smyslu čl. 49 odst. 1 Protokolu I. V případě užití „instrument-based" přístupu by ovšem tato operace, svojí povahou a provedením nenásilná, nemohla být považována za násilný čin.

146 MELZER: *Cyberwarfare*…, s. 26. Také DORMANN, Knut. The Applicability of the Aditional Protocols to Computer Network Attacks: An ICRC Viewpoint. In BYSTRÖM, Karin (ed). *International Expert Conference on Computer Network Attack and the Applicability of International Humanitarian Law*. Stockholm: Swedish National Defence College, 2004, s. 4.

například čl. 51 odst. 5 písm. b), kde nenalezneme zmínku o obsazení nebo neutralizaci.[147] Lze souhlasit, že v určitých případech by i kybernetická operace způsobující neutralizaci objektu mohla dosáhnout úrovně útoku. Mohlo by tomu tak být v případě, pokud by k obnovení obvyklých funkcí objektu musely být fyzicky vyměněny některé jeho komponenty. Pokud by ovšem k obvyklému fungování zařízení stačil jeho restart, nepanuje obecná shoda na kvalifikaci dané kybernetické operace.[148]

Pojem útok je jedním ze zásadních institutů právní úpravy a nejasnost jeho vztahu ke kybernetickým operacím přispívá k právní nejistotě stran konfliktu. Je zde vhodné zmínit další úvahu, která se v literatuře objevila a představuje názorový střet pozice MVČK a pozice vojenské mezinárodněprávní doktríny. Debata se týká výkladu ustanovení čl. 48 Protokolu I, který upravuje, že „*K zajištění respektování ochrany civilního obyvatelstva a objektů civilního rázu budou strany v konfliktu vždy činit rozdíl mezi civilním obyvatelstvem a kombatanty a mezi objekty civilního rázu a vojenskými objekty a v souladu s tím provedou své operace pouze proti vojenským objektům.*" Ustanovení reflektuje obyčejové mezinárodní právo a je vyjádřením jedné z kardinálních zásad mezinárodního humanitárního práva, a to zásady rozlišování.[149] Část autorů se přiklání k výkladu, s odkazem na systematiku, smysl a účel Protokolu I, že slovem operace se v daném článku nemyslí všechny vojenské operace, ale pouze vojenské operace dosazující hranice útoku. Prokazuje to i dlouhodobá praxe států, na základě které jsou nenásilné psychologické operace mířené vůči civilnímu obyvatelstvu v souladu s právem. Takovými operacemi jsou například shazování letáků a radiové vysílání. Kybernetická operace tak může cílit na civilní osoby a objekty, pokud nedosáhne hranice útoku.[150] Druhá část odborníků naopak argumentuje, že i vojenské operace, které nebude možné označit jako útoky, musejí být ovládány zásadou rozlišování. Pokud by byly vedeny proti civilním osobám nebo objektům, budou porušovat mezinárodní právo bez ohledu na své následky.[151] Lze souhlasit, že mezinárodní humanitární právo chrání civilní obyvatelstvo především před útoky a jejich následky pro civilní obyvatelstvo. Proto bude nejprve nezbytné provést analýzu operace, zda dosáhla úrovně útoku, a poté se teprve zabývat legalitou jejího cíle. Právní úprava nechrání civilní obyvatelstvo před všemi myslitelnými následky vojenských operací, ale pouze před těmi násilnými.

---

[147] SCHMITT, Michael. Cyber Operations and the Jus in Bello: Key Issues. *International Law Studies*, 2011, roč. 87, s. 95.
[148] Srov. SCHMITT: *Tallinn manual 2.0*…, s. 417 a diskuzi tam uvedenou.
[149] MSD: *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I. C. J. Reports 1996, odst. 78. Dle MSD nesmí státy cílit své útoky na civilisty, nepoužívá termín operace.
[150] SCHMITT: *„Attack" as a*…, s. 289. Na podobném základě by byla v souladu s právem kybernetická operace, jejímž cílem by bylo rušení internetového vysílání. Blíže International Commitee of the Red Cross. *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Report prepared by the ICRC.* 32nd International Conference of the Red Cross and Red Crescent, Geneva 2015, s. 41.
[151] Tamtéž s. 42. Objevují se i názory, že nutnost aplikace omezení plynoucích z mezinárodního humanitárního práva se neváže na skutečnost, zda kybernetické operace dosahují hranice „útoku", ale zda je lze subsumovat pod pojmy „vedení nepřátelství" nebo „přímá účast v nepřátelství". Srov. MELZER: *Cyberwarfare* …, s. 27.

Lze shrnout, že mezinárodní humanitární právo obsahuje pravidla, která mohou sloužit jako nástroje pro jeho aplikaci na kybernetické prostředky a metody vedení boje. V případech, kdy bude dána jeho působnost, bude nutné užít zásady právní úpravy na kybernetické operace vedené v souvislosti s ozbrojeným konfliktem a zkoumat, jaké důsledky může tato aplikace přinést.

3 Aplikace zásad mezinárodního humanitárního práva na kybernetické operace

Cílem právní úpravy mezinárodního humanitárního práva je v souladu s požadavkem humanity zabránit nadměrnému utrpení bojujících stran a omezit dopad bojových operací na civilní obyvatelstvo. Každá vojenská operace musí být provedena v souladu se zásadami právní úpravy.[152] Kyberprostor, a v jeho kontextu prováděné vojenské operace, nejsou výjimkou. Jak bylo naznačeno v kapitole I, kyberprostor se ale zásadně odlišuje od ostatních domén vedení bojových operací. Jeho strukturální odlišnost bude mít zásadní vliv na plánování a přípravu bojových operací. Je proto důležité zabývat se konkrétní podobou aplikace jednotlivých zásad.

3.1 Zásada rozlišování

Zásada rozlišování stanovuje bojujícím stranám závazek útočit pouze na vojenské cíle, tj. na vojenské objekty a kombatanty. Zásada je vyjádřena v čl. 48 a 52 odst. 2 Protokolu I[153] a má povahu obyčejového pravidla.[154] Pravidlo je použitelné pro mezinárodní i vnitrostátní ozbrojený konflikt. V kontextu kyberprostoru může být určení toho, které osoby nebo objekty jsou civilní nebo vojenské povahy, nejednoznačné a činit praktické obtíže. Obtížné může být i samotné vymezení pojmu objekt. Jasná a pevně stanovená hranice mezi civilními a vojenskými objekty neexistuje.[155]

3.1.1 Rozlišení vojenských a civilních objektů

Pokud bude mít kybernetická operace obdobné účinky jako ta kinetická, lze vycházet při aplikaci zásady rozlišování ze stejných předpokladů jako v případě kinetického útoku. Objekt musí splňovat kritéria povahy, umístění, účelu a použití, která jsou základními determinanty pro určení charakteru cíle. Až poté, co bude některé z těchto kritérií naplněno, je nezbytné analyzovat kritéria účinného příspěvku a zjevné vojenské výhody. To je možné demonstrovat na případu zničení kasáren. Kasárna budou vojenským objektem, jelikož bezpochyby naplní kritéria čl. 52 odst. 2. Není pak rozdíl mezi kinetickým raketovým útokem s cílem zničit tuto budovu, a tím kybernetickým, jehož následek bude stejný.[156] Jinak tomu ovšem bude v případě zařízení, které svojí

---

[152] Jednání, které závažně porušuje mezinárodní humanitární právo, může být válečným zločinem. K problematice, zda lze kybernetickými prostředky spáchat válečné zločiny srov. FIDLER, David P. Cyber War Crimes: Islamic State Atrocity Videos and the Laws of War. *Computer Law Review International*, 2015, roč. 16, č. 6, s. 161 - 166.

[153] Čl. 52 odst. 2 Protokolu I: „*Útoky musí být přísně omezeny na vojenské objekty. Pokud jde o objekty, omezují se vojenské objekty na ty objekty, které svou povahou, umístěním, účelem nebo použitím představují účinný příspěvek k vojenským akcím a jejichž celkové nebo částečné zničení, obsazení nebo neutralizace poskytuje za daných okolností zjevnou vojenskou výhodu.*"

[154] DOSWALD-BECK, HENCKAERTS: *Customary International…*, s. 25.

[155] Blíže DINSTEIN, Yoram. Legitimate Military Objectives Under The Current Jus In Bello. *International Law Studies,* 2002, roč. 78, s. 139-144.

[156] MAVROPOULOU, Elizabeth. Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks. *Journal of Law and Cyber Warfare*, 2015, roč. 23, s. 38.

povahou slouží jak vojenským, tak civilním účelům. Striktně vzato téměř každá část kybernetické infrastruktury může sloužit ze své povahy zároveň civilním i vojenským účelům (*dual-use target*).[157] Podobnou úvahu lze vztáhnout na soukromé korporace, které se zabývají informačními technologiemi a úzce spolupracují s vládními složkami.[158] Pokud by se setrvalo na zavedených intepretací pojmu vojenský cíl, bylo by možné dojít k závěru, že celý kyberprostor je legálním vojenským cílem.[159] Každý objekt, jehož užívání nebo budoucí užívání vytváří účinný příspěvek k vojenským akcím, je nutné právně označit jako legální vojenský cíl, a jako takový může být cílem útoku během ozbrojeného konfliktu.[160] Nexus mezi účinným příspěvkem a vojenskou akcí byl definován odlišně z pozice Spojených států amerických, navzdory jeho obyčejové povaze.[161] Spojené státy nejsou smluvní stranou Protokolu I, přesto považují pravidlo obsažené v čl. 52 odst. 2 za obyčejové, ale interpretují jej šířeji. Podle Spojených států mohou naplnit definici vojenského objektu i ekonomické cíle (*war-fighting and war-sustaining targets*), které přispívají k válečnému úsilí a podporují nepřímo, ale efektivně schopnosti nepřátelské strany.[162] Tato interpretace není správná. V situaci, kdy většina armádních složek užívá stejné části kybernetické infrastruktury jako civilní obyvatelstvo, by mělo označení této infrastruktury včetně ekonomických objektů za vojenský cíl fatální důsledky především pro civilní obyvatelé.[163] Tato úvaha nabývá na významu také tím, že v budoucích ozbrojených konfliktech bude kybernetická infrastruktura nejen prostředkem útoku, ale i vlastním cílem vojenských operací v závislosti na technické vyspělosti bojujících stran.[164] Dalším korektivem pro určení legality cíle v kyberprostoru je požadavek, aby zničení nebo neutralizace daného cíle poskytovala zjevnou vojenskou výhodu.[165] Tato výhoda musí být konkrétní a definovatelná, ne pouze možná a neurčitá, či jenom politická.[166]

---

[157] Tzn. každý počítač, server, síťový uzel aj. Objekt má ale v daný moment pouze jeden status, a to buď vojenský, nebo civilní.

[158] Pokud například Microsoft poskytuje podporu válečnému úsilí Spojených států amerických tím, že podporuje jejich vojenské operace a poskytuje uživatelskou podporu vládní infrastruktuře, mohl by být označen za vojenský cíl. Srov. JENSEN, Eric Talbot. Unexpected Consequences From Knock-On Effects: A Different Standard for Computer Network Operations? *American University International Law Review*, 2003, roč. 18, č. 5, s. 1160-1168. A dále DROEGE, Cordula. Get off my cloud: cyberwarfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, 2012, roč. 94, č. 866, s. 566.

[159] Vojenský kód může cestovat skrze kyberprostor rozdělen na různé balíky dat, které mohou jednotlivě cestovat skrze různé civilní části kybernetické infrastruktury. Tyto jednotlivé části by mohly být označeny za vojenské objekty. Viz GEIß, Robin, LAHMANN, Henning. Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space. *Israel Law Review*, 2012, roč. 45, s. 385.

[160] Tamtéž, s 383.

[161] DOSWALD-BECK, HENCKAERTS: *Customary International…*, s. 29.

[162] MAVROPOULOU: *Targeting…*, s. 40. Dále srov. ROSCINI: *Cyber Operations…*, s. 186.

[163] JENSEN, Eric Talbot. Cyber Warfare and Precaution Against the Effects of Attacks. *Texas Law Review*, 2010, roč. 88, s. 1522.

[164] GEIß, LAHMAN: *Cyber Warfare…*, s. 384. Ovládnutí klíčových komponent kyberprostoru nepřátelské strany bude stejně důležité pro vítězství v konfliktu jako ovládnutí vzdušného prostoru během tradičního konfliktu.

[165] Čl. 52 odst. 2 Protokolu I in fine.

[166] DINSTEIN, Yoram. *Conduct of Hostilities under the Law of International Armed Conflict*. 2. vydání. Cambridge: University Press, 2010, s. 93.

V kyberprostoru může být naplnění tohoto požadavku problematické, jelikož jednou z vlastností kyberprostoru je jeho propojenost. To znamená, že v případě narušení nebo zničení určitého komunikačního kanálu, kterým data cestují, si datový tok najde pro svoji další cestu jiný kanál. Poté nelze dobře tvrdit, že zničení konkrétní kybernetické infrastruktury poskytuje zjevnou vojenskou výhodu, pokud chyběl širší zájem na jejím zničení než v souvislosti s tokem dat.[167]

Jinou otázkou zůstává, zda navzdory své nehmotné povaze, mohou být vojenským objektem samotná data nebo počítačové programy. Pojem objekt v čl. 52 odst. 2 by měl být vykládán jako něco hmotného a viditelného.[168] Většina autorů Tallinnského manuálu se shoduje, že v rámci platného mezinárodního humanitárního práva by pojem „objekt" neměl zahrnovat data.[169] Úmluvy se mají vykládat v dobré víře, v souladu s obvyklým významem, který je dáván výrazům v nich užitých a jejich celkové souvislosti.[170] Ani přípravné práce, ani komentář k Protokolu I neudávají důvod, na základě kterého by bylo možné data subsumovat pod pojem objekt. Pojem data tak zahrnuje nehmotné předměty, které svojí povahou nemohou ani výkladem spadat pod právní význam pojmu objekt.[171] Kybernetickou operaci cílící na data nebude možné kvalifikovat jako útok ve smyslu čl. 49 Protokolu I bez dalšího. Pokud by ovšem tato operace měla zásadní důsledky pro funkčnost daného zařízení, považovalo by se za cíl dané zařízení, a ne pouze cílená data.[172]

Zřetelný příklad vojenského cíle v kyberprostoru může být webová stránka, která předává opakovaně kódované zprávy povstalecké skupině na území jedné z bojujících stran, čímž účinně přispívá k vedení bojových operací proti vládním ozbrojeným silám.[173] Kybernetická infrastruktura, která tvoří technickou podporu této webové stránce, by byla vojenským cílem.[174] Složitější situací může být využití sociálních sítí jako Facebook k podpoře válečného úsilí, což je poměrně často se vyskytující jev ze strany teroristických organizací. Tyto sítě obsahují obrovskou spoustu dat, která většinou nemají žádnou spojitost s ozbrojeným konfliktem, a proto nelze označit celou sociální síť za vojenský cíl.[175] Vojenským cílem by byla pouze kybernetická infrastruktura podporující daný segment celé sítě. Následuje však otázka, zda je vůbec technicky možné provést útok pouze na tuto část infrastruktury.[176]

Zajímavým příkladem objektu, který je možné využívat k vojenským i civilním účelům, je počítač. Počítač sám o sobě nebude vojenským cílem, jelikož nenaplňuje žádné kritérium

---

[167] GEIß, LAHMAN: *Cyber Warfare*…, s. 388.
[168] PICTET: *Commentary…,* odst. 2007 a 2008.
[169] SCHMITT: *Tallinn manual 2.0*…, s. 437.
[170] Č. 31 odst. 1 Vídeňské úmluvy o smluvním právu, vyhlášené pod č. 15/1988 Sb., ve znění předpisu č. 9/2014.
[171] SCHMITT: *Tallinn manual 2.0…,* s. 437.
[172] Tamtéž.
[173] Vytvoření a využívání takové webové stránky je dobrým příkladem kybernetické metody vedení boje.
[174] Tamtéž, s. 440.
[175] DROEGE: *Gett Off…,* s. 569.
[176] Tamtéž.

uvedené v čl. 52 odst. 2. Avšak může se jím stát. Lze mít za to, že bude-li sloužit jako uložiště vojenských dat, splní stanovená kritéria a bude vojenským cílem.[177] Typičtějším příkladem vojenského cíle však bude spíše počítač vybavený programy pro přímou podporu bojující strany. Pokud bude navíc využíván ve vojenském zařízení, bude se nepochybně jednat o vojenský cíl. Složitější situace by nastala v případě, pokud by se náhodný počítač stal součástí rozsáhlého botnet útoku.[178] V takové situaci by se dalo uvažovat o naplnění kritéria účelu a užití dle čl. 52 odst. 2, protože cílem botnet útoku může být neutralizace daného objektu pomocí DDoS útoků. V tomto případě by se jednalo i o účinné přispění, které je úzce a zřejmě spojeno s vojenskou operací, jelikož by bez zapojení daného počítače útok nemusel proběhnout.[179] Počítač by se tak stal vojenským objektem, legálním cílem vojenského útoku, aniž by o tom jeho majitel mohl nebo musel vědět. Samotný počítač tedy může být za určitých podmínek kvalifikován jako vojenský objekt.[180]

3.1.2 Rozlišení osob chráněných a nechráněných

Základní vymezení statusu chráněných osob, tj. civilistů, obsahuje čl. 50 odst. 1 Protokolu I: „*Civilní osoba je osoba, která nepatří do žádné z kategorií osob uvedených v článku 4 A 1), 2), 3) a 6) Třetí Úmluvy a v článku 43 tohoto Protokolu. V případě pochybnosti, zda je osoba civilní osobou, bude taková osoba považována za osobu civilní.*“ Tuto negativní definici ještě doplňuje čl. 51 odst. 3, na základě kterého požívají civilisté ochrany, pokud se přímo neúčastní nepřátelství.[181] Naproti tomu kombatanty jsou dle čl. 43 odst. 2 členové ozbrojených sil strany konfliktu s výjimkou zdravotnického a duchovního personálu a osob hors de combat dle čl. 41. Tyto osoby mají právo účastnit se nepřátelství a požívají imunity kombatantů.[182] Možnost cílení kombatantů se proto odvíjí od jejich postavení v rámci určité organizační jednotky. U civilistů záleží na jejich konkrétním jednání.[183] Vymezení kombatantů je v právní úpravě poměrně ustálené a nečiní interpretační problémy. Diskutovaným aspektem u vymezení kombatantů v kontextu kyberprostoru je nutnost jejich vizuálního odlišení od civilní populace během provádění bojových operací. Tento závazek, kodifikován v čl. 44 odst. 3

---

[177] DINSTEIN, Yoram. The Principle of Distinction and Cyber War in International Armed Conflicts. *Journal of Conflict & Security Law*, 2012, roč. 17, č. 2, s. 263.
[178] GEIß, LAHMAN: *Cyber Warfare*…, s. 385.
[179] DOSWALD-BECK: Some Thoughts…, s. 166. Podobná situace by nastala v případě, kdyby byl do počítače umístěn červ nebo virus, a pouze čekal na pokyn pro své další působení a šíření. Zde může být problematické, zda lze počítač, jehož součástí je mallware, označit za vojenský cíl, ačkoliv v daný moment nijak nepřispívá k budoucí vojenské operaci a nenaplňuje žádné další kritérium čl. 52 odst. 2 Protokolu I. Právní úprava nestanovuje žádný standard pro prokázání způsobilosti objektu sloužit vojenskému účelu a ani nestanovuje žádné kritérium pro hodnocení informace, na základě níž bude tato způsobilost prokazována. Blíže srov. SCHMITT: *Tallinn manual 2.0*…, s. 440.
[180] Ačkoliv jeho majitel bude považován za civilistu.
[181] Pojem přímé účasti v nepřátelství není přesně definován ve smluvním ani obyčejovém právu. Pokus o jeho vymezení byl proveden na půdě MVČK, srov. MELZER, Nils. *Interpretative Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*. ICRC, 2009. 85 s. Dále v textu jako „Výkladová směrnice“.
[182] Tzn., že pokud provádějí své vojenské operace v souladu s mezinárodním právem, nelze je za tato jednání trestně stíhat druhou stranou konfliktu, ačkoliv by se podle vnitrostátní úpravy mohlo jednat o kriminální činy.
[183] SCHMITT: *Tallinn manual 2.0*…, s. 425.

Protokolu I, je odrazem obyčejového práva.[184] Povinnost spočívá v tom, že každý kombatant musí být označen rozlišujícím znakem viditelným na dálku a nosit zbraně viditelně.[185] Je sporné, zda je tento požadavek aplikovatelný i na kybernetické operace, popřípadě jaký smysl by tato aplikace měla. Historicky byl tento závazek nutný pro jasné vymezení bojujících stran na bojišti s úmyslem omezit počet civilních obětí vojenských operací v souladu s požadavkem humanity.[186] Jelikož ale vojenský specialista provádějící kybernetickou operaci pravděpodobně nebude přítomen přímo na bojišti, postrádá tento závazek smysl a neměl by být nutně aplikován. Rozlišení osoby by mohlo být patrné z jiných okolností.[187] Pokud by bojující strana chtěla přesto plně dostát tomuto závazku alespoň v teoretické rovině, mohla by kybernetický útok provádět například pouze z elektronicky označené IP adresy, nebo ze speciálně vytvořené IP adresy, která by vešla v obecnou známost jako náležící konkrétní bojující straně. Ve výsledku ale nemusí být pro toto rozlišování praktický důvod, jelikož původce kybernetického útoku bude buď kombatant, nebo civilista přímo se účastnící nepřátelství, a proto bude v obou případech legálním cílem odvetného útoku.[188]

Kybernetické prostředky a metody vedení boje vyžadují vysoký stupeň odbornosti, lze proto předpokládat vyšší zapojení civilních expertů do vedení bojových činností.[189] Nabízí se otázka, zda, popřípadě v jakých případech by mohlo být možné označit tyto osoby za kombatanty nebo civilisty přímo se účastnící nepřátelství.

Členy ozbrojených složek budou v obecné rovině členové pravidelných ozbrojených sil a ozbrojených skupin, kterými mohou být dobrovolnické nebo povstalecké skupiny, přiřazené k pravidelným ozbrojeným silám. Vzhledem k nutnosti vysoké míry specializace pro vedení kybernetických operací je potřebné zvážit postavení civilních společností, které na základě smluvních ujednání vykonávají specifické kybernetické operace. Bylo-li by možné podřadit tuto skupinu osob do kategorie ozbrojených složek nebo ozbrojených organizovaných skupin, náležel by jim status kombatanta a bylo by možné je považovat za legální cíl bez dalšího. Pokud nikoliv, náležel by jim status civilistů. Ochranu před útoky by nepožívali pouze po dobu své přímé účasti v nepřátelství.[190] Při hodnocení statusu je nutné vycházet z míry integrace dané skupiny do hierarchie ozbrojených složek a z úkolů zde plnících. Pokud kontraktoři přispívají efektivně

---

[184] DOSWALD-BECK, HENCKAERTS: *Customary International*…, s. 384.
[185] Čl. 4 A odst. 2) písm. b) Ženevské úmluvy o zacházení s válečnými zajatci, vyhlášené pod č. 65/1954 Sb.
[186] WATTS, Sean. Combatant Status and Computer Network Attack. *Virginia Journal of International Law*, 2009, roč. 50, č. 2, s. 439.
[187] Například z okolnosti, že daná osoba sedí za vojenským počítačem ve středisku kybernetických operací.
[188] DINNISS, Heather A. Harrison, SCHMITT, Michael N. *Computers and War: the Legal Battlespace.* Background Paper Prepared for Informal High-Level Expert Meeting on Current Challenges to International Humanitarian Law, Cambridge, June 25-27, 2004, s. 12.
[189] TURNS, David. Cyber Warfare and the Notion of Direct Participation in Hostilities. *Journal of Conflict & Security Law*, 2012, roč. 17, č. 2, s. 279.
[190] MELZER: *Interpretative*…, s. 39.

k bojové činnosti ozbrojených sil a vykonávají soustavnou bojovou funkci, mělo by na takovou skupinu být nahlíženo jako na organizovanou ozbrojenou skupinu, tj. kombatanty.[191] Stejný závěr platí i pro členy složek zpravodajských služeb specializujících se na kybernetické operace, i když nemusí být formálně součástí ozbrojených složek.[192] Naopak pokud nebudou kontraktoři organizačně ani úkolově začleněni do role, ve které by mohli vykonávat soustavnou bojovou funkci,[193] bude jim náležet status civilistů. Takové osoby budou pod ochranou mezinárodního humanitárního práva do té doby, dokud se jako jedinci nebudou přímo účastnit nepřátelství.

Absence smluvního nebo obyčejového vymezení pojmu přímé účasti v nepřátelství představuje v kontextu kyberprostoru zvláštní úskalí. Výkladová směrnice MVČK stanoví, že pojem přímé účasti v nepřátelství se vztahuje na specifická jednání, jež jsou prováděná jednotlivci jako část vedení nepřátelství mezi stranami ozbrojeného konfliktu.[194] Tato jednání musí dále kumulativně splňovat kritérium určité míry a závažnosti újmy způsobené jednáním, vztah přímé příčinné souvislosti mezi jednáním a jeho následkem a konečně zde musí být nexus ve vztahu k ozbrojenému konfliktu.[195] Způsobená újma musí mít přímý vliv na vedení vojenských operací a příčinná souvislosti nesmí obsahovat mezičlánek, tedy způsobená škoda musí být přímo zamýšleným následkem operace. U posuzování újmy je možné postupovat analogicky jako při hodnocení kybernetické operace ve světle č. 49 Protokolu I. Dovození přímé příčinné souvislosti však může být u kybernetických operací problematické, vzhledem k jejich často nepřímým účinkům.[196] Určení, zda se konkrétní civilní osoba přímo účastní nepřátelství, není jednoznačné a nemá ani pevné teoretické zakotvení. To je možné demonstrovat na následujícím příkladu. Lze si představit situaci, kdy se civilista zapojí do kybernetických aktivit souvisejících s vedením nepřátelství pomocí svého počítače, aniž by nutně musel vynaložit další snahu.[197] Jeho cílem bude podpora jedné ze stran konfliktu a na internetu získá návod, jako toho docílit. Pokud by tyto aktivity dosáhly hranice útoku, mohl by i na základě jediného kliknutí myši tento civilista ztratit ochranu a být legálním cílem vojenského útoku.[198]

Míra zapojení civilních osob do kybernetických aktivit může mít různou podobu. Lze shrnout, že standard přímé účasti v nepřátelství bude bezpochyby naplněn v případě zapojení

---

[191] Tamtéž. Je vhodné doplnit, že status kombatanta existuje pouze v mezinárodním ozbrojeném konfliktu.
[192] Srov. Čl. 43 odst. 3 Protokolu I.
[193] Např. poskytují pouze servisní podporu, aktualizaci software apod.
[194] MELZER: *Interpretative*…, s. 43.
[195] Tamtéž, s. 46.
[196] TURNS: *Cyber Warfare*…, s. 287.
[197] Naopak v případě konvenčních zbraní by se jednalo o patření si vlastní zbraně, výrobu improvizovaných výbušných zařízení aj.
[198] K tomu blíže poznámka pod čarou č. 31. Dále k jednotlivým kritériím přímé účasti v nepřátelství v kontextu kybernetických operací srov. SCHMITT: *Tallinn manual 2.0*…, s. 429.

civilní osoby do ofensivní kybernetické operace, která bude dosahovat hranice předpokládané čl. 49.[199]

Je patrné, že aplikace zásady rozlišování na kybernetické prostředky a metody vedení boje vyvolává spíše otázky, místo aby poskytovala uspokojující odpovědi. Rozlišení vojenského a civilního objektu bude nezbytné určit případ od případu a stejný závěr platí i pro rozlišení osob.

3.1.3 Zákaz proradnosti

Za zásady rozlišování plyne stranám konfliktu další závazek, a to zákaz zabít, zranit nebo zajmout protivníka užitím proradnosti. Zákaz je upraven v čl. 37 odst. 1 Protokolu I. Za proradné činy jsou považovány ty, které zneužívají dobré víry protivníka a vyvolávají u něj mylnou domněnku, že má právo na ochranu nebo že je povinen ochranu poskytnou podle norem mezinárodního práva aplikovaných v ozbrojených konfliktech.[200] Za proradný čin by mohlo být považováno zaslání emailu, v němž bude jedna z bojujících stran vystupovat jako představitel MVČK a pod tímto označením si sjedná schůzku s druhou bojující stranou. Poté, co druhá strana v dobré víře dorazí na sjednané místo, podnikne na ni letecký nálet. Následkem pak bude smrt všech osob na daném místě.[201]

3.2 Zásada přiměřenosti a zákazu nerozlišujících útoků

I když bude kybernetický útok veden na vojenský cíl, nebude možné, podobně jako u kinetických operací, vyloučit způsobení vedlejších škod na civilních osobách či objektech. Aby se předcházelo těmto situacím, je stranám konfliktu stanoven závazek vynaložit při vedení vojenských operací nepřetržitou péči[202] tomu, aby bylo ušetřeno civilní obyvatelstvo, civilní osoby a objekty civilního rázu.[203] Právní úprava na tyto situace reaguje zakotvením zásady přiměřenosti obsažené v čl. 51 odst. 5 písm. b)[204] a čl. 57 odst. 2) písm. a) bod iii Protokolu I, který je kodifikací obyčejového pravidla aplikovatelného pro mezinárodní i vnitrostátní ozbrojený konflikt.[205] Přiměřenost takového útoku[206] se posuzuje dle vztahu důvodně předvídatelné vedlejší škody a předpokládané vojenské výhody, jež bude útokem získána.

---

[199] DINNISS, SCHMITT: *Computers…,* s. 13.
[200] Čl. 37 odst. 1 Protokolu I. K jednotlivým prvkům zákazu srov. PICTET: *Commentary…,* odst. 1500.
[201] SCHMITT: *Tallinn manual 2.0*…, s. 493.
[202] K obsahu pojmu nepřetržitá péče srov. JENSEN, Talbot Eric. Cyber Attacks: Proportionality and Precautions in Attack. *International Law Studies*, 2013, roč. 89, s. 203.
[203] Čl. 57 Protokolu I.
[204] Zákaz tzv. nerozlišujících útoků, tedy takových, které svým charakterem nebo provedením nejsou schopné rozlišit povahu cíle.
[205] DOSWALD-BECK, HENCKAERTS: *Customary International…*, s. 46.
[206] Analýza přiměřenosti se bude aplikovat pouze na kybernetické operace dosahující úrovně útoku, jak napovídá samotný Protokol I, když v čl. 57 odst. 1 užívá slovní spojení vojenské operace, ale v odst. 2 hovoří o útocích. Blíže JENSEN: *Cyber Attacks…,* s. 204.

Z hlediska testu přiměřenosti jsou kybernetické prostředky a metody vedení boje vhodnou alternativou k tradičním bojovým prostředkům. Povaha kybernetických útoků představuje nové možnosti pro minimalizaci vedlejších škod a náhodných zranění. Kde bylo dříve nezbytné použít konvenční útok k neutralizaci vojenského objektu, je nyní možné jej pomocí kybernetických prostředků „vypnout" nebo jinak blokovat jeho operativní funkce.[207] Na druhou stranu je to právě povaha kybernetických prostředků a jejich operační prostředí, díky kterým nabývají na významu nepředvídané následky nebo v literatuře užívané „knock-on" efekty. Těmi jsou efekty, s nimiž se při plánování operace nepočítalo, ale objevily se v důsledku zásahu dalších osob nebo jiných okolností.[208]

Pokud bude velitel plánovat kybernetický útok, bude muset učinit vše možné, aby si ověřil, že cílem útoku nejsou civilní osoby, ani objekty civilního rázu. Musí učinit veškerá možná preventivní opatření při volbě prostředků a způsobů útoku, aby zabránil a omezil náhodné ztráty na životech civilních osob a poškození civilních objektů.[209] Konečně útok nezahájí, pokud lze předpokládat, že způsobí náhodné ztráty na životech civilních osob nebo poškození civilních objektů, které by převyšovaly předpokládanou konkrétní a přímou vojenskou výhodu.[210] Jelikož vedení kybernetických operací vyžaduje vysokou odbornost, nabízí se úvaha, do jaké míry musí tuto odbornost naplňovat i velitel při plánování operace. Pokud by velitel musel zvážit opravdu všechny možné varianty následků jeho útoku, stalo by se plánování takového útoku operativně nevýhodným a použitelným pouze v malém množství případů. Vhodnější variantou se zdá být určení následků útoku jako těch, které lze rozumně předpokládat na základě dostupných informací v okamžiku rozhodování o útoku.[211]

Není to pouze útočící strana, která má závazek vyhnout se vedlejším škodám na civilistech nebo civilních objektech druhé strany a v maximální možné míře[212] je chránit před následky svých operací. I strana, na kterou je útočeno, má závazek učinit kroky k ochraně jejího civilního obyvatelstva a civilních objektů před útoky a jejich následky.[213] Kroky k naplnění tohoto závazku mohou být oddělení vojenské a civilní kybernetické infrastruktury, odpojení počítačových systémů

---

[207] SCHMITT: *Wired Warfare*…, s. 394.

[208] Například vyřazením železniční stanice z provozu by mohlo dojít i k vyřazení informačních systémů fungujících na stejné infrastruktuře. Za nepředvídaný následek lze považovat šíření Stuxnetu i mimo íránské jaderné zařízení.

[209] Velitel by tak měl využívat takové kybernetické prostředky, které při náhodném rozšíření na jiné civilní zařízení nezpůsobí takovou škodu, jakou měly způsobit původnímu cíli. Jinak by takový útok měl být považován za nerozlišující.

[210] Čl. 57 odst. 2 písm. a) bod i-iii. Protokolu I.

[211] ICTY: *The Prosecutor v. Galić*, Trial Chamber II Judgement, IT-98-29-T, 5 December 2003, odst. 58. Velitel například nemůže předvídat, že se mallware implementovaný kybernetickou operací do určitého vojenského systému dostane i do jiného civilního systému skrze flash disk, který si voják odnese domů nedbaje bezpečnostních postupů.

[212] Termín „v maximální možné míře" se interpretuje jako prakticky možné, nikoliv teoreticky možné. Blíže PICTET: *Commentary…,* odst. 2245.

[213] Čl. 58 odst. 1 Protokolu I.

podporujících kritickou infrastrukturu od internetu či vytváření týmů pro řešení kybernetických hrozeb.[214]

3.3 Zásada vojenské nezbytnosti a zákazu nadměrného utrpení

Zásada vojenské nezbytnosti tvoří druhý kardinální princip právní úpravy.[215] Strany ozbrojeného konfliktu jsou omezeny ve volbě prostředků a metod vedení boje. Je zakázáno nasazení a užití takových prostředků a metod, které způsobují nadměrná zranění nebo zbytečné útrapy.[216] Aby byl kybernetický útok jako prostředek nebo metoda vedení boje v souladu s touto zásadou, musí splňovat dvě kritéria. Musí být vojensky nezbytný a být proveden v souladu se zásadou humanity, tj. nesmí způsobit nadměrná zranění nebo zbytečné útrapy.

Možnosti kybernetických útoků rozšiřují seznam cílů, jež byly pro velitele dříve nedostupné.[217] Zároveň představují alternativu ke konvenčním operacím, na základě které lze dojít ke stejnému vojenskému výsledku za použití lidštějších prostředků. Ve většině případů bude nasazení kybernetických prostředků a metod v souladu se zásadou vojenské nezbytnosti a lidskosti. To nevylučuje, aby ve specifických případech došlo k porušení této zásady způsobem použití prostředku, který způsobí zbytečné či nadměrné utrpení. Tallinnský manuál uvádí příklad kombatanta, který má kardiostimulátor s vestavěným defibrilátorem, jenž je přístupný přes internet. Pokud by bojující strana ovládla přístroj kybernetickým útokem a pomocí defibrilátoru způsobila smrt kombatanta v důsledku zástavy srdce, byl by útok v souladu se zásadou. Zásadu by naopak porušil útok, který by kombatantovi způsobil nadměrné útrapy tím, že by se jeho srdce několikrát zastavilo, poté obnovilo svoji funkci, a až následkem tohoto opakovaného procesu by kombatant zemřel.[218]

---

[214] Takové týmy se označují jako CERT (*Computer Emergency Response Team*) a CIRC (*Computer Incident Response Capability*). Srov. ŘEHKA: *Informační…*, s. 172.
[215] MSD: *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I. C. J. Reports 1996, odst. 79.
[216] Čl. 35 odst. 1 a 2 Protokolu I.
[217] JENSEN: *Unexpected…*, s. 1166.
[218] SCHMITT: *Tallinn manual 2.0…*, s. 455.

Závěr

Mezinárodní právo zatím nenašlo jasnou odpověď na otázky kladené v souvislosti s kyberprostorem, a to jak v době ozbrojeného konfliktu, tak v době míru.

Kyberprostor se vyznačuje specifickými rysy oproti tradičním operačním doménám. Na rozdíl od země nebo moře nemá kyberprostor fyzické hranice. Nejedná se o přírodní jev, který by bylo možné ovládnout a určitým způsobem rozdělit jako je tomu u země nebo moře. Jelikož je kyberprostor produktem lidské činnosti, jsou to lidé, kteří mají zásadní vliv na jeho formování.

Vývoj mezinárodního humanitárního práva ve vztahu ke kybernetickým prostředkům a metodám vedení boje může směřovat třemi směry.

První směr spočívá v odmítnutí působnosti právní úpravy na kyberprostor en bloc z důvodu, že žádné smluvní nástroje ani obyčejová pravidla nepočítají s kyberprostorem a není dobře možné existující pravidla aplikovat na tak odlišné prostředí, jakým kyberprostor bezpochyby je. V kapitole 2 bylo prokázáno, že samotná právní úprava tento směr překonává, jelikož obsahuje nástroje pro překlenutí mezer a bylo by i proti duchu mezinárodního humanitárního práva, aby jeho působnost nedosáhla na konkrétní prostředky a metody vedení boje.

Druhým směrem je přijetí nové smluvní úpravy, která by se explicitně zabývala aplikací mezinárodního humanitárního práva na kybernetické prostředky a metody vedení boje. Návrhy takovýchto úmluv lze v odborné literatuře nalézt, a často se jedná o propracované dokumenty vycházející z důkladné analýzy oblasti.[219] Obecně je možné konstatovat, že právní věda mezinárodního práva se touto problematikou vehementně zabývá, avšak bez náležité odezvy jednotlivých států. A jsou to právě státy, kdo jsou v oblasti mezinárodního práva tvůrci právních norem, nikoliv akademici, jejichž názory mohou mít maximálně podpůrnou roli při poznávání mezinárodního práva. To je nutné vzít na vědomí v souvislosti s tím, že doposud nebyly státy schopny dosáhnout jakéhokoliv konsenzu nebo pokroku při zvažování aplikace mezinárodního práva na kyberprostor. Důkazem toho je i nepřijetí závěrečné zprávy na páté schůzi skupiny vládních expertů pod záštitou OSN v červnu roku 2017. Zájmy států a jejich názory na problematiku jsou příliš odlišné. Lze sledovat názorové neshody mezi státy technologicky vyspělými a těmi méně vyspělými.[220] Situaci komplikuje dále skutečnost zmíněná v kapitole I, a to nutnost spolupráce s definičními autoritami při vyjednávání nové právní úpravy a potřeba

[219] Srov. BROWN, Davis. A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict. *Harvard International Law Journal*, 2006, roč. 47, č. 1, s. 179 – 221.
[220] SOESANTO, Stefan, D'INCAU, Fosca. *The UN GGE is Dead: Time to fall forward* [online]. ecfr.eu, 15. srpna 2017 [cit. 16. února 2018]. Dostupné na <http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance>.

multidisciplinárního náhledu na celou problematiku kyberprostoru. V dohledné době je proto spíše nepravděpodobné, že by byla přijata jakákoliv smluvní úprava.

Třetím směrem ve vývoji právní úpravy je vyčkat na praxi států a dosavadní normy aplikovat pomocí evolutivního výkladu. Toto řešení se jeví jako nejpravděpodobnější a zároveň nejefektivnější. Pokud státy nejsou schopny a ochotny vytvořit společnou smluvní úpravu, bude záležet na jejich faktickém chování a veřejně projevených právních názorech. Na základě toho může být kyberprostor regulován skrze utvářející se obyčejová pravidla. Vzniku obyčejových norem však může bránit skutečnost, že se ekonomicky a technologicky významné státy staví do kontrapozice k alespoň částečně ustáleným názorům druhé skupiny států.[221] Čas nakonec ukáže, jakou praxi jednotlivé státy mezinárodního společenství přijmou.

Co se týče aplikace současného mezinárodního humanitárního práva na kybernetické operace, bylo prokázáno, že strany ozbrojeného konfliktu budou vázány jeho pravidly při použití kybernetických prostředků a metod vedení boje. Neexistuje žádný důvod, aby měly odlišný právní režim vojenské operace tradiční kinetické povahy, a ty kybernetické dosahující obdobných následků. Naznačuje to i samotná právní úprava, která zásadně nerozlišuje povahu užitých prostředků nebo metod vedení boje. Stanovuje pouze požadavky, které tyto prostředky a metody musí splňovat nebo zakazuje konkrétní způsob jejich užití. Toto tvrzení nevylučuje existenci sporných oblastí, které činí aplikaci právní úpravy problematickou. Těmito oblastmi jsou například právní úprava zásady rozlišování, určení standardu péče při vyhodnocování přiměřenosti kybernetické operace a problematika přičitatelnosti jednání státu v kyberprostoru.

Doposud jsme naštěstí nebyli svědky rozsáhlých kybernetických operací srovnatelných s tradičními způsoby vedení boje. Není tedy možné v této době zhodnotit, jak by se s problematickými aspekty právní úpravy vypořádaly státy, došlo-li by k nasazení takovýchto bojových prostředků. Debata o problematických oblastech tak zůstává na akademické úrovni.

Lze uzavřít, že hypotéza této práce o aplikovatelnosti mezinárodního humanitárního práva na kybernetické prostředky a metody vedení boje byla potvrzena.

Kybernetické operace neprobíhají v právním vzduchoprázdnu. Pokud budou naplněny obecné předpoklady působnosti mezinárodního humanitárního práva, bude jej nutné aplikovat i v kyberprostoru.

[221] SCHMITT, Michael N, VIHUL, Liis. *The Nature of International Law Cyber Norms*. Tallinn Paper. No. 5, Special Expanded Issue, CCDCOE, 2014, s. 30.

Seznam použité literatury

Monografie a sborníky

ANDRUŠKO, Alena. *Internet, informační společnost a autorské právo*. 1. vydání. Praha: Wolters Kluwer ČR, 2016. 276 s.

TIKK, Eneken, KASKA, Kadri, VIHUL, Liis. *International Cyber Incidents: Legal Considerations*. Tallinn: Cyber Defence Centre of Excellence, 2010. 130 s.

DAVID, Vladislav a kol. *Mezinárodní právo veřejné s kazuistikou*. 2. aktualizované a přepracované vydání. Praha: Leges, 2011. 448 s.

DINSTEIN, Yoram. *Conduct of Hostilities under the Law of International Armed Conflict*. 2. vydání. Cambridge: University Press, 2010. 320 s.

DORMANN, Knut. The Applicability of the Aditional Protocols to Computer Network Attacks: An ICRC Viewpoint. In BYSTRÖM, Karin (ed). *International Expert Conference on Computer Network Attack and the Applicability of International Humanitarian Law*. Stockholm: Swedish National Defence College, 2004, s. 1 – 12.

FAIX, Martin. *Law of Armed Conflict and Use of Force. Part Two-Limiting the Effects of War: International Law of Armed Conflict*. Olomouc: Vydavatelství Univerzity Palackého, 2013. 211 s.

GÁBRIŠ, Tomáš. *Cyber Law: textbook*. 1. vydání. Bratislava: Univerzita Komenského v Bratislavě, 2014. 249 s.

GOLDSMITH, Jack, WU, Tim. *Who Controls the Internet? Illusions of Borderless World*. New York: Oxford University Press, 2006. 226 s.

International Commitee of the Red Cross. *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*. 2. vydání. 2016. 1280 s.

International Law Commission. *Draft Articles on Responsibility of States for Internationally Wrongful Acts with commentaries*. Yearbook of the International Law Commission, Vol. II, Part Two, A/CV.4/SER.A/2001Add1 (Part 2), 2001.

KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, 2016. 522 s.

KUEHL, Daniel T. From Cyberspace to Cyberpower: Defining the Problem. In KRAMER, Franklin D. (ed). *Cyberpower and National Security*. Lincoln: University of Nebraska Press, 2009, s. 24 – 42.

MALANCZUK, Peter. *Akehurst's Modern Introduction to International Law*. 7. vydání. New York: Routledge, 1997. 449 s.

ONDŘEJ, Jan a kol. *Mezinárodní humanitární právo*. 1. vydání. Praha: C. H. Beck, 2010. 559 s.

PICTET, Jean a kol. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Geneva: Martinus Nijhoff Publishers, 1987. 1597 s.

POLČÁK. Radim. *Internet a proměny práva*. Praha: Auditorium, 2012. 388 s.

ROSCINI, Marco. *Cyber Operations and the Use of Force in International Law*. 1. vydání. New York: Oxford University Press, 2014. 307 s.

ŘEHKA, Karel. *Informační válka*. 1. vydání. Praha: Academia, 2017. 218 s.

SCHMITT, Michael. „Attack" as a Term of Art in International Law: The Cyber Operations Context. In CZOSSECK, Christian, OTTIS, Rain, ZIOLKOWSKI, Katharina (eds). *Proceedings of the 4th International Conference on Cyber Conflict*. Tallinn: CCDCOE Publications, 2012, s. 283 – 294.

Manuály, vojenské příručky a studie

DOSWALD-BECK, Louise (ed). San Remo Manual on International Law Applicable to Armed Conflict at Sea. New York: Cambridge University Press, 1995. 257 s.

DOSWALD-BECK, Louise, HENCKAERTS, Jean-Marie (eds). Customary International Humanitarian Law. Volume I: Rules. New York: Cambridge University Press, 2005. 628 s.

Harvard Program on Humanitarian Policy and Conflict Research. Manual on International Law Applicable to Air and Missile Warfare. New York: Cambridge University Press, 2009. 56 s.

International Commitee of the Red Cross. A Guide to the Legal Review of New Weapons, Means and Methods of Warfare. Measures to Implement Article 36 of Additional Protocol I of 1977. Geneva, 2006. 34 s.

MELZER, Nils. Interpretative Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law. ICRC, 2009. 85 s.

National Military Strategy for Cyberspace Operations (NMS-CO), Chairman of the Joint Chiefs of Staff, Department of Defence, vydáno 11 prosince 2006, Washington D. C. USA.

SCHMITT, Michael (ed). Tallinn manual 2.0 on the international law applicable to cyber operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excelence. New York: Cambridge University Press, 2017. 594 s.

SCHMITT, Michael (ed). Tallinn manual on the international law applicable to cyber warfare: Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. New York: Cambridge University Press, 2013. 282 s.

U.S. Department of Defense. Law of War Manual. June 2015 (updated December 2016), s. 1013. Dostupné na <https://www.defense.gov/Portals/1/Documents/law_war_manual15.pdf>.

Články z odborných časopisů

ASHMORE, William C. Impact of Alleged Russian Cyber Attacks. *Baltic Security & Defence Review*, 2009, roč. 11, s. 4 – 40.

BASTL, Martin, GRUBEROVÁ, Zuzana. Kyberprostor jako „pátá doména"? *Vojenské rozhledy*, 2013, roč. 22 (54), č. 4, s. 10 – 21.

BROWN, Davis. A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict. *Harvard International Law Journal*, 2006, roč. 47, č. 1, s. 179 – 221.

DINSTEIN, Yoram. Computer Network Attacks and Self-Defence. *International Law Studies*, 2002, roč. 76, s. 99 – 119.

DINSTEIN, Yoram. Legitimate Military Objectives Under The Current Jus In Bello. *International Law Studies,* 2002, roč. 78, s. 139 – 172.

DINSTEIN, Yoram. The Principle of Distinction and Cyber War in International Armed Conflicts. *Journal of Conflict & Security Law*, 2012, roč. 17, č. 2, s. 261 – 277.

DOSWALD-BECK. Louise. Some Thoughts on Computer Network Attack and the International Law of Armed Conflict. *International Law Studies*, 2002, roč. 76, s. 163 – 185.

DROEGE, Cordula. Get off my cloud: cyberwarfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, 2012, roč. 94, č. 866, s. 533 – 578.

EVRON, Gadi. Bettling Botnets and Online Mobs: Estonia's Defence Efforts during the Internet War. *Georgetown Journal of International Affairs*, 2008, roč. 9, č. 1, s. 121 – 126.

FIDLER, David P. Cyber War Crimes: Islamic State Atrocity Videos and the Laws of War. *Computer Law Review International*, 2015, roč. 16, č. 6, s. 161 – 166.

GEIß, Robin, LAHMANN, Henning. Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space. *Israel Law Review*, 2012, roč. 45, s. 381 – 399.

JENSEN, Eric Talbot. Cyber Warfare and Precaution Against the Effects of Attacks. *Texas Law Review*, 2010, roč. 88, s. 1522 – 1556.

JENSEN, Eric Talbot. Unexpected Consequences From Knock-On Effects: A Different Standard for Computer Network Operations? *American University International Law Review*, 2003, roč. 18, č. 5, s. 1146 – 1187.

JENSEN, Talbot Eric. Cyber Attacks: Proportionality and Precautions in Attack. *International Law Studies*, 2013, roč. 89, s. 198 – 217.

JOHNSON, David R., POST, David G. Law and Bordes – the Rise of Law in Cyberspace. *Stanford Law Review*, 1997, roč. 48, s. 1367 – 1402.

KESSLER, Oliver, WERMER, Wouter. Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare. *Leiden Journal of International Law*, 2013, roč. 26, č. 4, s. 793 – 810.

KLEINWACHTER, Wolfgang. From Self – Governance to Public-Private Partnership: The changing Rule of governments in the Management of the Internet's Core Resources. *Loyola of Los Angeles Law Review*, 2003, roč. 36, č. 3, s. 1103 – 1126.

KODAR, Erik. Applying the law of armed conlfict to cyber attacks: From the Martens Clause to Additional Protocol I. *ENDC Proceedings*, 2012, roč. 15, s. 107 – 132.

KOH, Harold Hongju. International Law in Cyberspace. *Harvard International Law Journal Online*, 2012, roč. 54, č. 4854, s. 1 - 12.

MAVROPOULOU, Elizabeth. Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks. *Journal of Law and Cyber Warfare*, 2015, roč. 23, s. 23 – 93.

MENTHE, Darrel C. Jurisdiction in Cyberspace: A Theory of International Spaces. *Michigan Telecommunications and Technology Law Review*, 1998, roč. 4, č. 1, s. 69 – 103.

PEAGLER, Jordan. The Stuxnet Attack: A New Form of Warfare and the (In)Aplicability of Current International Law. *Arizona Journal of International & Comparative Law*, 2014, roč. 31, č. 2, s. 399 – 432.

POST, David G. Governing Cyberspace. *Wayne Law Review*, 1996, roč. 43, č. 1, s. 155 – 171.

REMUS, Titiriga. Cyber-Attacks and International law of Armed Conflicts: A „Jus ad Bellum" Perspective. *Journal of International Commercial Law and Technology*, 2013, roč. 8, č. 3, s. 179 – 189.

RICHARDS, Jason. Denial-of-Service: The Estonian Cyberwar and Its Implications for U. S. National Security. *International Affairs Review*, 2009, roč. 18, č. 2. Dostupné na <http://www.iar-gwu.org/node/65>.

RICHMOND, Jeremy. Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modification to the Law of Armed Conflict? *Fordham International Law Journal*, 2012, roč. 35, s. 843 – 893.

SCHMITT, Michael. Classification of Cyber Conflict. *Journal of Conflict & Security Law*, 2012, roč. 17, č. 2, s. 245 – 260.

SCHMITT, Michael. Cyber Operations and the Jus in Bello: Key Issues. *International Law Studies*, 2011, roč. 87, s. 89 – 110.

SCHMITT, Michael. Wired Warfare: Computer Network Attack and Jus in Bello. *International review of the Red Cross*, 2002, roč. 84, č. 846, s. 365 – 399.

SINGER, Peter W. Stuxnet and Its Hiden Lessons on the Ethics of Cyberweapons. *Case Western Reserve Journal of International Law*, 2015, roč. 47, s. 79 – 84.

THOMAS, Timothy L. The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia. *Journal of Slavic Military Studies*, 2009, roč. 22, s. 31 – 67.

THOMSON, Andrew W. R. Doctrine of the Protection of Nationals Abroad: Rise of the Non-Combatant Evacuation Operation. *Washingston University Global Studies Law Review*, 2012, roč. 11, č. 3, s. 628 – 666.

TICEHURST, Rupert. The Martens clause and the Laws of Armed Conflict. *International Review of the Red Cross*, č. 317, 1997. Dostupné na <https://www.icrc.org/eng/resources/documents/article/other/57jnhy.htm>.

TURNS, David. Cyber Warfare and the Notion of Direct Participation in Hostilities. *Journal of Conflict & Security Law*, 2012, roč. 17, č. 2, s. 279 – 297.

VAN DER VYVER, Johan D. The ISIS Crisis and the Development of International Humanitarian Law. *Emory International Law Review*, 2016, roč. 30, č. 4, s. 531 – 563.

WATTS, Sean. Combatant Status and Computer Network Attack. *Virginia Journal of International Law*, 2009, roč. 50, č. 2, s. 392 – 444.

Internetové zdroje

A Cyber Riot [online]. economist.com, 10. května 2007 [cit. 10. prosince 2017]. Dostupné na <http://www.economist.com/node/9163598>.

ADAMS, Michael J. *A Warning About Tallinn 2.0… Whatever It Says* [online]. lawfareblog.com, 4. ledna 2017 [cit. 11. ledna 2018]. Dostupné na <https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says>.

BOWCOTT, Owen. *Rules of cyberwar: don't target nuclear plants or hospitals, says Nato manual* [online]. theguardian.com, 18března 2013 [cit. 11. ledna 2018]. Dostupné na <https://www.theguardian.com/world/2013/mar/18/rules-cyberwarfare-nato-manual>.

Declaration of Universal Mobilization by Georgian President Mikheil Saakahvili [online]. vk.com, 10. srpna 2008 [cit. 18. února 2018]. Dostupné na <https://vk.com/topic-4143158_6733001>.

CHERNENKO, Alena. *Russia warns against NATO document legitimizing cyberwars* [online]. rbth.com, 29 květen 2013 [cit. 11. ledna 2018]. Dostupné na <https://www.rbth.com/international/2013/05/29/russia_warns_against_nato_document_legitimizing_cyberwars_26483.html>.

KOSACHEV, Konstantin. *An insult to our war dead* [online]. Theguardian.com, 6. března 2007 [cit. 10. prosince 2017]. Dostupné na <https://www.theguardian.com/commentisfree/2007/mar/06/comment.secondworldwar>.

MARKOFF, John. *Before the Gunfire, Cyberattacks* [online]. nytimes.com, 12. srpna 2008 [cit. 10. prosince 2017]. Dostupné na <http://www.nytimes.com/2008/08/13/technology/13cyber.html>.

NAKASHIMA, Ellen, WARRICK, Joby. *Stuxnet was work of U. S. and Israeli experts, officials say* [online]. washingtonpost.com, 2. června 2012 [cit. 23. ledna 2018]. Dostupné na <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.46da1cb989bf>.

NATO. *Glossary of Terms and Definitions.* AAP-06. Edition 2014. Dostupné na <http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6EN.pdf>.

NAZARIO, Jose. *Estonian DDoS Attacks – A summary to date* [online]. arbornetworks.com, 17 května 2007 [cit. 10. prosince 2017]. Dostupné na <https://www.arbornetworks.com/blog/asert/estonian-ddos-attacks-a-summary-to-date/>.

Newly nasty [online]. economist.com, 24 května 2007 [cit. 10. prosince 2017]. Dostupné na <http://www.economist.com/node/9228757>.

Russia „ends Georgia operation" [online]. news.bbc.co.uk, 12 srpna 2008 [cit. 10. prosince 2017]. Dostupné na <http://news.bbc.co.uk/2/hi/europe/7555858.stm>.

RYAN, Johny. *„iWar": A New Threat, its Convenience – and our Increasing* [online], nato.int., 2007 [cit. 11. ledna 2018]. Dostupné na <https://www.nato.int/docu/review/2007/issue4/english/analysis2.html>.

SCHMITT, Michael. *CyCon 2012, Tallin Manual Part I* [online] youtube.com, 29. září 2012 [cit. 1. února 2018]. Dostupné na <https://www.youtube.com/watch?v=wY3uEo-Itso>.

SOESANTO, Stefan, D'INCAU, Fosca. *The UN GGE is Dead: Time to fall forward* [online]. ecfr.eu, 15. srpna 2017 [cit. 16. února 2018]. Dostupné na <http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance>.

TechDictionary. Dostupné na <http://www.techdictionary.com/search_action.lasso>.

War in South Ossetia: Georgia started it [online]. theguardian.com, 1. října 2009 [cit. 10. prosince 2017]. Dostupné na <https://www.theguardian.com/commentisfree/2009/oct/01/russia-georgia-south-ossetia>.

Warsaw Summit Communiqué ze dne 9. června 2016, bod 70. Dostupné na <https://www.nato.int/cps/en/natohq/official_texts_133169.htm>.

WEISS, Michael. *Here Come the Cyber Wars: Are We Ready* [online]? reason.com, 17. srpna 2007 [cit. 10. prosince 2017]. Dostupné na <http://reason.com/archives/2007/08/17/here-come-the-cyber-wars>.

Rozhodnutí soudů a jiných tribunálů

ICTY: *The Prosecutor v. Delalić,* Trial Chamber Judgement, IT-96-21-T, 16 November 1998.

ICTY: *The Prosecutor v. Furundžija,* Trial Chamber Judgement, IT-95-17/1-T, 10 December 1998.

ICTY: *The Prosecutor v. Galić*, Trial Chamber II Judgement, IT-98-29-T, 5 December 2003.

ICTY: *The Prosecutor v. Limaj*, Trial Chamber II Judgement, IT-03-66-T, 30 November 2005.

ICTY: *The Prosecutor v. Mrkšić*, Trial Chamber II Judgement, IT-95-13/1-T, 27 September 2007.

ICTY: *The Prosecutor v. Tadić*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT 94-1-A, 2 October 1995.

ICTY: *The Prosecutor v. Tadić,* Judgement of the Appeals Chamber, IT-94-1-A, 15 July 1999.

Mezinárodní soudní dvůr: *Corfu Channel case*, Judgement of April 9th, 1949, I. C. J. Reports 1949.

Mezinárodní soudní dvůr: *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I. C. J. Reports 1996.

Mezinárodní soudní dvůr: *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), Merits, Judgement, I. C. J. Reports 1986.

Stálý dvůr mezinárodní spravedlnosti: *The Case of the S.S. „Lotus"*, Judgement of 7th September, 1927, Series A.–No. 10.

Stálý rozhodčí soud: *Island of Palmas case* (Netherlands, USA), arbitral award, 4 April 1928.

Právní předpisy a jiné právní dokumenty

Právní předpisy

Dodatkový protokol k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí mezinárodních ozbrojených konfliktů ze dne 8. června 1977, vyhlášen pod č. 168/1991 Sb.

Dodatkový protokol k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí ozbrojených konfliktů nemajících mezinárodní charakter, ze dne 8. června 1977, vyhlášen pod č. 168/1991 Sb.

Charta Spojených národů ze dne 26. června 1945, vyhlášena pod č. 30/1947 Sb., ve znění předpisů č. 127/1965 Sb. a č. 36/1999 Sb.

IV. Haagská úmluva z roku 1907 o zákonech a obyčejích války pozemní, s Řádem války pozemní jako přílohou.

Římský statut Mezinárodního trestního soudu ze dne 17. července 1998, vyhlášen pod č. 84/2009 Sb. m. s., ve znění předpisu č. 16/2016 Sb. m. s.

Severoatlantická smlouva ze dne 4. dubna 1949, vyhlášena pod č. 66/1999 Sb.

Smlouva o zásadách činnosti států při výzkumu a využívání kosmického prostoru včetně Měsíce a jiných nebeských těles ze dne 7. února 1968, vyhlášena pod č. 40/1968 Sb.

Statut Mezinárodního soudního dvora ze dne 26. června 1945, vyhlášen pod č. 30/1947 Sb., ve znění předpisů č. 127/1965 Sb. a 36/1999 Sb.

Úmluva o mezinárodním letectví ze dne 7. prosince 1944, vyhlášena pod č. 147/1947 Sb.

Úmluva o zákazu nebo omezení použití některých konvenčních zbraní, které mohou způsobovat nadměrné utrpení nebo mít nerozlišující účinky, vyhlášena pod č. 21/1999 Sb., ve znění předpisu č. 115/2006 Sb. m. s.

Úmluva Organizace spojených národů o mořském právu, vyhlášena pod č. 240/1996 Sb.

Vídeňská úmluva o smluvním právu, vyhlášena pod č. 15/1988 Sb., ve znění předpisu č. 9/2014.

Ženevská úmluva o ochraně civilních osob za války, vyhlášena pod č. 65/1954 Sb.

Ženevská úmluva o zacházení s válečnými zajatci, vyhlášena pod č. 65/1954 Sb.

Ženevská úmluva o zlepšení osudu raněných a nemocných příslušníků ozbrojených sil v poli, vyhlášena pod č. 65/1954 Sb.

Ženevská úmluva o zlepšení osudu raněných, nemocných a trosečníků ozbrojených sil na moři, vyhlášena pod č. 65/1954 Sb.

Jiné právní dokumenty

DINNISS, Heather A. Harrison, SCHMITT, Michael. *Computers and War: the Legal Battlespace*. Background Paper Prepared for Informal High-Level Expert Meeting on Current Challenges to International Humanitarian Law, Cambridge, June 25-27, 2004, s. 1 – 18.

International Commitee of the Red Cross. *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Report prepared by the ICRC*. 32nd International Conference of the Red Cross and Red Crescent, Geneva 2015, s. 1 – 61.

MELZER, Nils. *Cyberwarfare and International Law*. UNIDIR Resources, 2011. 37 s. Dostupné na <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>.

SCHMITT, Michael N. VIHUL, Liis. *The Nature of International Law Cyber Norms*. Tallinn Paper. No. 5, Special Expanded Issue, CCDCOE, 2014, s. 1 – 30.

Abstrakt

Diplomová práce se zaměřuje na vztah mezinárodního humanitárního práva a kyberprostoru. Jejím cílem je identifikovat specifické vlastnosti kyberprostoru s ohledem na možnosti jeho mezinárodněprávní regulace. Dále je cílem práce určit, zda lze mezinárodní humanitární právo aplikovat na kybernetické prostředky a metody vedení boje bez existence explicitní právní úpravy. Obsah práce je rozdělen do tří kapitol. První kapitola charakterizuje kyberprostor jako svébytné prostředí, které svojí povahou představuje výzvu současnému mezinárodnímu právu veřejnému. Druhá kapitola obsahuje rozbor Tallinnského manuálu, jenž představuje komplexní pramen poznání vztahu mezinárodního práva veřejného a kybernetických operací. V kapitole je dále provedena analýza působnosti norem mezinárodního humanitárního práva v kontextu kybernetických prostředků a metod vedení boje. Obsahem třetí kapitoly je aplikace základních zásad mezinárodního humanitárního práva na kybernetické prostředky a metody vedení boje, včetně identifikace problematických aspektů.

Abstract

The aim of this master's thesis is to deal with the link between international humanitarian law and the cyberspace. The goal of the thesis is to identify specific features of the cyberspace with the focus on the possibilities of its regulation by public international law. Then, the thesis will answer the question whether international humanitarian law is applicable to cyber means and methods of warfare, even without explicit treaty or customary rule. Thesis is divided into three chapters. First chapter deals with the notion of cyberspace as the unique operational environment which, by its nature, poses a challenge to the current public international law. Second chapter contains an analysis of the Tallinn manual, which is the complex source of findings on the link between public international law and cyber operations. Then, this chapter analyzes the scope of international humanitarian law in the context of cyber warfare. Finally, third chapter deals with the application of basic principles of international humanitarian law on the cyber warfare, including the identification of the problematic aspects.

Klíčová slova

Mezinárodní humanitární právo, kyberprostor, kybernetická operace, kybernetický útok, Tallinnský manuál, kybernetické prostředky a metody vedení boje, vedení nepřátelství.

Key words

International humanitarian law, cyberspace, cyber operation, cyber attack, Tallinn manual, cyber means and methods of warfare, conduct of hostilities.