UNIVERZITA KARLOVA

Právnická fakulta

Kateřina Surá

Aplikace mezinárodního humanitárního práva na kybernetické vedení boje

Diplomová práce

Vedoucí diplomové práce: doc. JUDr. PhDr. Veronika Bílková, Ph.D., E.MA.

Katedra mezinárodního práva

Datum vypracování práce (uzavření rukopisu) : 2. prosince 2019

Prohlášení

Prohlašuji, že jsem předloženou diplomovou práci vypracovala samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.
Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 111 362 znaků včetně mezer.

Kateřina Surá

V Praze dne 2. prosince 2019

Poděkování

Na tomto místě bych chtěla poděkovat paní doc. JUDr. PhDr. Veronice Bílkové, Ph.D., E.MA. za její trpělivost, vstřícnost, odborné rady a komentáře při psaní této diplomové práce, ale také za její neutuchající pozitivní přístup ve výuce mezinárodního práva, který se pro mne stal velkou inspirací.
Dále bych chtěla vyjádřit svůj dík panu Nobuo Hayashi za jeho upřímný zájem o téma této diplomové práce a laskavé poskytnutí své práce před její publikací.
V neposlední řadě bych chtěla poděkovat svojí rodině za neutuchající podporu po celou dobu studia.

Obsah

Úvod

Diplomová práce s názvem *Aplikace mezinárodního humanitárního práva na kybernetické vedení boje* se zabývá možnostmi aplikace mezinárodního humanitárního práva v kybernetickém prostoru. K výběru tématu diplomové práce vedl autorku dlouhodobý a hluboký zájem o odvětví mezinárodního práva veřejného, především tedy mezinárodního humanitárního práva, jehož studiu měla možnost se věnovat nejen na Právnické fakultě Univerzity Karlovy v Praze, ale také na Právnické fakultě Univerzity v Oslo, a to v rámci ročního studijního pobytu. K tomuto se přidal navíc zájem o aktuální dění a s tím spojená praktická možnost aplikace mezinárodního humanitárního práva v současném světě. Je totiž neoddiskutovatelným faktem, že využívání kybernetického prostoru pro všechny aspekty lidských aktivit je na vzestupu. Ne jinak je tomu i v případě aktivit válečných, a to přesto, že žádný ze států dosud nevydal prohlášení, že by se stal obětí kybernetického útoku, jež by buď inicioval vznik ozbrojeného konfliktu, nebo byl jeho součástí.

Předmětem předkládané diplomové práce je snaha o zodpovězení otázky, *zda je možné na válečné aktivity prováděné prostředky moderních technologií aplikovat existující mezinárodní humanitární právo, a pokud ano, pak do jaké míry*. Mezinárodní společenství převážně zastává názor, že současné mezinárodní právo, do čehož je zahrnuto i mezinárodní humanitární právo, se v kybernetickém prostoru aplikuje, a není tak třeba vzniku nových norem. Právně závazné určení však dosud neexistuje.

V tomto ohledu je tedy stěžejním zdrojem Tallinnský manuál 2.0 o mezinárodním právu aplikovatelném na kybernetické operace[1] z roku 2017, který vznikl pod záštitou výzkumného centra NATO CCD COE v Tallinnu. Jedná se o soubor 154 pravidel z různých oblastí mezinárodního práva – kromě práva ozbrojených konfliktů také oblast lidských práv, mezinárodní odpovědnosti či použití síly v mezinárodních vztazích. Všechna tato pravidla jsou vyjádřením *lex lata*, a to především obyčejového práva, popřípadě smluvního, u kterého však není pochyb o jeho obyčejové povaze. Toto je z hlediska přesvědčivosti velice důležitý element, neboť v oblasti, kde neexistuje praxe států ani *opinio iuris*, je obzvlášť složité artikulovat obecně uznávané argumenty. Z důvodu absence jakéhokoli podobného uceleného instrumentu je Tallinnský manuál užíván jako základní zdroj poznání, třebaže se jedná o právně nezávazné vyjádření názoru expertů, kteří se na jeho tvorbě podíleli.

[1] SCHMITT, Michael N. a Liis VIHUL. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence; general editor Michael N. Schmitt; managing editor Liis Vihul*. Second edition. New York, NY, USA: Cambridge University Press, 2017.

Diplomová práce se skládá z úvodu, čtyř kapitol, které tvoří stěžejní část práce, a závěru. Úvod práce slouží k seznámení se s tématem diplomové práce, důvodem pro napsání a výzkumnou otázkou. Dále také stručně popisuje aktuální právní stav v oblasti kybernetického vedení ozbrojeného boje, především zdůrazňuje důležitost Tallinnského manuálu a vysvětluje, z jakého důvodu je v diplomové práci v takovém rozsahu používán.

První kapitola obsahuje velice stručný popis základních elementů mezinárodního humanitárního práva, tedy jeho povahu, stěžejní smluvní úpravu a rozbor pojmu ozbrojeného konfliktu a s tím souvisejícího rozdělení ozbrojených konfliktů na mezinárodní a vnitrostátní. V neposlední řadě je do první kapitoly zařazen také stručný vývoj válečnictví dle amerického vojenského teoretika W. S. Linda, který je dle názoru autorky vhodným úvodem k rozboru válčených aktivit v kybernetickém prostoru.

Druhá kapitola vysvětluje základní pojmy nezbytné pro popis kybernetického vedení boje. Jsou jimi kybernetický prostor, kybernetická operace a kybernetický útok.

Účelem třetí kapitoly je podrobit základní principy, na nichž je založeno mezinárodní humanitární právo, rozboru z hlediska jejich možné aplikovatelnosti v kybernetickém prostoru. Impulsem pro tento přezkum nebyla pouze důležitost postavení těchto principů v rámci odvětví mezinárodního humanitárního práva, třebaže se jedná o primární předpoklad, ale také skutečnost, že principy humanity, nezbytnosti, přiměřenosti a rozlišování byly ve zprávě odborníků v oblasti informačních a telekomunikačních technologií[2] pro Valné shromáždění OSN výslovně zmíněny jako aplikovatelné v kybernetickém prostoru.

Čtvrtá kapitola na základě předchozího zkoumání přichází se čtyřmi vybranými problematickými aspekty aplikovatelnosti mezinárodního humanitárního práva na kybernetické vedení boje. Tedy upozorňuje na nesrovnalosti takového charakteru, které nelze překonat pouhým výkladem existujících norem. Jedná se o problematičnost určení autorství kybernetické operace, teritoriální limitace kybernetické operace, a také komplikovanost zaručení ochrany civilistů a nemocničních zařízení v kybernetickém prostoru.

Závěr shrnuje poznatky ze všech čtyř kapitol a formuluje odpověď na výzkumnou otázku stanovenou v úvodu diplomové práce.

Dále je text opatřen poznámkovým aparátem a doplněn seznamem použitých pramenů, abstraktem v českém a anglickém jazyce a klíčovými slovy.

[2] UN Doc. A/70/174 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. [online] 22 July 2015. Bod 28, pís. b).

Pro ilustraci dané problematiky jsou v textu často využívány jako příklady již proběhnuvší kybernetické operace. Autorka tím poukazuje i na praktické problémy spojené s tímto způsobem vedení boje.

Většina materiálů zabývajících se danou problematikou, včetně Tallinnského manuálu či materiálů Mezinárodního výboru Červeného kříže, je dostupná pouze v anglickém jazyce, tudíž je v diplomové práci často užíváno překladu autorky. Pro zabránění nesrovnalostem je při citaci uvedeno i originální anglické znění. V případě, že existuje oficiální překlad do českého jazyka, je užito tohoto překladu.

1. Charakteristika mezinárodního humanitárního práva a stručný vývoj moderního válečnictví

Mezinárodní humanitární právo (dále také jen jako „MHP“), označované též „právo ozbrojených konfliktů“ či „válečné právo“, je odvětvím mezinárodního práva veřejného. Tvoří jej normy obyčejové i smluvní povahy, které jsou specificky vázány na situaci ozbrojeného konfliktu a jejichž úkolem je ochrana osob, jež se bojů přímo neúčastní či z nich byly vyřazeny, a také omezení způsobů a prostředků k vedení takových bojů.[3] Obecně lze tedy říci, že MHP slouží k humanizaci ozbrojených konfliktů.

1.1. *Ius ad bellum* a *ius in bello*

Kromě výše uvedených pojmů se k označení mezinárodního humanitárního práva užívá také pojmu *ius in bello* (neboli „právo ve válce“). Tento pojem doslova vystihuje možnosti aplikace MHP – uplatňuje se pouze v rámci již existujícího ozbrojeného konfliktu. Otázku jeho vzniku, resp. legalitu použití síly proti jinému státu, reguluje *ius ad bellum* (neboli „právo na válku“) či některými autory používaný pojem *ius contra bellum* (tedy „právo proti válce“).[4] Třebaže se *ius contra bellum* může jevit jako výstižnější pro označení norem, jejichž účelem je de facto zabránění používání síly mezi státy, bude se autorka držet klasického dělení na *ius in bello* a *ius ad bellum.*

Vznik *ius ad bellum* spojujeme až s počátkem 20. století jako odpověď na hrůzy světových válek. Do té doby bylo rozpoutání války poměrně častým způsobem řešení sporů mezi státy. Přes dílčí úspěchy v oblasti rozlišování války zakázané a legální či zákazu útočné války došlo k obecnému zákazu použití síly až přijetím Charty Organizace spojených národů v roce 1945, kde se v čl. 2 odst. 4 stanovuje, že *„všichni členové se vystříhají ve svých mezinárodních stycích hrozby silou nebo použití síly jak proti územní celistvosti nebo politické nezávislosti kteréhokoli státu, tak jakýmkoli jiným způsobem neslučitelným s cíli Organizace spojených národů.“* Užití pojmu „síla“ spíše než „válka“ souvisí nejen s opouštěním tohoto pojmu mezinárodním společenstvím, ale má také praktické hledisko – vylučuje se tímto polemika nad tím, zda určitý konflikt naplňuje kritéria války či nikoli. Charta OSN výslovně uvádí pouze 2 výjimky ze zákazu použití síly. Těmito výjimkami jsou opatření Rady bezpečnosti

[3] ICRC. *Mezinárodní humanitární právo: odpovědi na vaše otázky*. Editor Veronika BÍLKOVÁ, Marek JUKL. Praha: Český červený kříž, 2009, s. 5.
[4] ONDŘEJ, Jan, Pavel ŠTURMA, Veronika BÍLKOVÁ a Dalibor JÍLEK. *Mezinárodní humanitární právo.* 1. vydání. Praha: C. H. Beck, 2010, s. 3.

OSN při ohrožení míru, porušení míru nebo útočném činu (dle čl. 42 Charty OSN) a právo na individuální a kolektivní sebeobranu (dle čl. 51 Charty OSN).[5]

V případě, kdy *ius ad bellum* přestane plnit svoji funkci, tedy dojde k porušení zákazu užití síly, začínají se uplatňovat normy *ius in bello*, a to bez ohledu na to, kdo takové porušení způsobil, či jak k němu došlo – normy *ius in bello* jsou zcela nezávislé na normách *ius ad bellum*.[6]

Ius in bello, normy regulující chování stran ve válce, provázejí lidstvo stejně dlouho, jako války samotné. K jeho modernímu rozvoji dochází od poloviny 19. století a je spojováno se jménem ženevského obchodníka Henry Dunanta, který se stal svědkem bídného osudu raněných v bitvě u Solferina. Z jeho podnětu tak byl v Ženevě již roku 1863 vytvořen předchůdce Mezinárodního výboru Červeného kříže a následujícího roku byla svolána mezinárodní konference, na níž byla přijata Ženevská úmluva o zlepšení osudu raněných v polních armádách.[7] Tato úmluva položila základ tzv. ženevského práva, tedy toho odvětví MHP, jehož úkolem je ochrana obětí bojů: raněných, nemocných, trosečníků, válečných zajatců a civilistů. *Gros* je obsaženo ve čtyřech Ženevských úmluvách z roku 1949 a v Dodatkových protokolech k těmto úmluvám z roku 1977.[8] Pravidla ženevského práva jsou nederogovatelná, tedy není jakýmkoli způsobem možné omezit jejich působnost či se vzdát ochrany, jež je jimi chráněným osobám poskytována. Na druhou stranu je však možné, aby si strany konfliktu ujednaly rozšíření práv chráněných osob.[9]

Předmětem haagského práva je naproti tomu úprava dovolených a zakázaných prostředků a způsobů vedení boje. Tvoří jej velká řada úmluv, stěžejními jsou Úmluva o zákonech a obyčejích války pozemní a Řád války pozemní přijaté na mírových konferencích v Haagu v letech 1899 a 1907. Není však vhodné vnímat tyto dvě oblasti odděleně, neboť spolu úzce souvisejí a současný vývoj ještě více přispívá k jejich překrývání.

Tato práce se nadále bude věnovat převážně problematice *ius in bello*, avšak pro uvedení do kontextu považovala autorka za nutné toto dělení uvést.

---

[5] FLECK, Dieter. *The Handbook of International Humanitarian Law*. Third edition. Oxford: Oxford University Press, 2013. s. 1.
[6] Srov. Preambule k Dodatkovému protokolu I
[7] ONDŘEJ J. et al. *Mezinárodní humanitární právo. op. cit.* s. 97.
[8] ŽÚ o zlepšení osudu raněných a nemocných příslušníků ozbrojených sil v poli (ŽÚ I), ŽÚ o zlepšení osudu raněných, nemocných a trosečníků ozbrojených sil na moři (ŽÚ II), ŽÚ o zacházení s válečnými zajatci (ŽÚ III), ŽÚ o ochraně civilních osob za války (ŽÚ IV), DP o ochraně obětí mezinárodních ozbrojených konfliktů (DP I), DP o ochraně obětí ozbrojených konfliktů nemajících mezinárodní charakter (DP II)
[9] ONDŘEJ J. et al. *Mezinárodní humanitární právo. op. cit.* s. 144.

1.2. Pojem „ozbrojený konflikt“ a klasifikace ozbrojených konfliktů

„Ozbrojený konflikt“ je stěžejním pojmem MHP, neboť veškeré normy MHP jsou přímo vázány na situaci ozbrojeného konfliktu. Vymezení tohoto pojmu je tedy klíčové, avšak nikoli bezproblémové, jak bude popsáno dále.

Dříve běžně používaný pojem „válka“ (podle něhož se původně celé odvětví nazývalo „válečné právo“) byl ve 20. století postupně nahrazen pojmem „ozbrojený konflikt“. Jak již bylo uvedeno v předchozí kapitole, opouštění pojmu válka mělo své praktické důvody – aby se jednalo o válku, musely boje dosáhnout určité intenzity a taktéž se předpokládalo její řádné vyhlášení. Jednoduše se tak státy mohly vyhnout plnění svých povinností uložených jim válečným právem tím, že boje probíhající mezi nimi nepovažovaly za válku. Proto došlo k tomu, že se přistoupilo k pojmu „ozbrojený konflikt“ jako k určujícímu bodu pro aplikaci MHP.[10]

Ačkoli je ozbrojený konflikt nepochybně pojmem obsahově širším než válka, žádný z pramenů MHP jej nedefinuje. Toto „vakuum“ prolomil až v roce 1995 Mezinárodní trestní tribunál pro bývalou Jugoslávii (ICTY) v případu Tadić, kdy poskytnul následující definici: *„Ozbrojený konflikt existuje vždy, když dojde k uchýlení se k ozbrojené síle mezi státy, nebo déletrvajícímu ozbrojenému násilí mezi vládní autoritou a organizovanými ozbrojenými skupinami či mezi takovými skupinami uvnitř státu.“*[11]

Mezinárodní výbor Červeného kříže (MVČK či anglická zkratka ICRC) pak v březnu roku 2008 ve svém *opinion paper* ohledně pojmu ozbrojený konflikt přichází s definicí vnitrostátního ozbrojeného konfliktu, jež reflektuje výše uvedenou definici ICTY, a to že *„ozbrojené konfrontace musí dosáhnout minimální úrovně intenzity a strany zapojené v konfliktu musí vykazovat minimum organizace“*.[12]

Je zjevné, že třebaže definice odpovídá na otázku, co je ozbrojený konflikt, sama přichází s dalšími vágními pojmy. Můžeme se ptát, kde je stanovena hranice, která určuje *„minimální úroveň intenzity“* či *„minimum organizace“*. Na druhou stranu je však nutné vzít do úvahy, že

[10] Například společný článek 2 Ženevských úmluv stanovuje, že: *„nehledíc na ustanovení, která mají nabýti účinnosti již v míru, bude se tato úmluva vztahovati na všechny případy vyhlášené války nebo jakéhokoli jiného ozbrojeného konfliktu vzniklého mezi dvěma nebo více Vysokými smluvními stranami, i když válečný stav není uznáván jednou z nich“*.

[11] *„An armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State.“* ICTY, *Prosecutor v. Duško Tadić*, Case No. IT-94-1-AR72, Appeals Chamber, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, par. 70.

[12] *„The armed confrontation must reach a minimum level of intensity and the parties involved in the conflict must show a minimum of organisation.“* ICRC, *How is the Term „Armed Conflict“ Defined in International Humanitarian Law?* Opinion Paper. March 2008. s. 5.

přílišná rigidnost takové definice by mohla vést k aplikačním problémům s ohledem na okolnosti a charakter jednotlivých případů a ke zvýšení rizika jejího zneužití.[13] Flexibilita definice ozbrojeného konfliktu nabývá na důležitosti i z hlediska vývoje trendů v oblasti vedení konfliktů v současném světě, o kterém se bude hovořit v následující podkapitole.

MHP rozlišuje dva druhy ozbrojených konfliktů: mezinárodní a nemezinárodní, resp. vnitrostátní. Toto rozlišení je zcela zásadní z hlediska aplikovatelného právního režimu, v praxi však působí nemalé problémy, neboť hranice mezi nimi není vždy jasná a pevná a charakter konfliktu se může v průběhu jeho trvání změnit.

Z výše uvedené první části definice ICTY v případu Tadić a ze společného článku 2 Ženevských úmluv vyplývá charakteristika mezinárodního ozbrojeného konfliktu: konflikt se odehrává mezi dvěma či více státy (slovy Ženevských úmluv „Vysokými smluvními stranami"). Kromě války či jiného ozbrojeného konfliktu sem spadá také situace částečné nebo úplně okupace.[14] Ve všech těchto případech dochází od okamžiku vypuknutí ozbrojeného konfliktu k aplikaci všech čtyř Ženevských úmluv, Dodatkového protokolu I a všech smluv haagského práva. Důvodem je, že mezinárodní ozbrojený konflikt má velmi vysoký destrukční potenciál, tedy pouhá jeho existence má za účinek aplikaci celého MHP bez ohledu na důvody či intenzitu konfrontace[15] či uznání existence konfliktu jeho stranami. Vychází se tedy z objektivního hlediska, nikoli subjektivního. Do kategorie mezinárodního ozbrojeného konfliktu byly Dodatkovým protokolem I v roce 1977 zahrnuty také boje za národní osvobození.[16]

Vnitrostátní ozbrojený konflikt se od mezinárodního liší v mnoha ohledech. Co se stran konfliktu týče, ve vnitrostátním ozbrojeném konfliktu alespoň jedna ze stran není státem, což znamená, že se jedná o konflikt mezi organizovanými ozbrojenými silami a státem (označovaný jako „vertikální ozbrojený konflikt") či mezi takovými organizovanými ozbrojenými silami navzájem („horizontální ozbrojený konflikt"). Z hlediska teritoriálního rozsahu se jedná o konflikt, který vznikne na území jednoho státu.[17]

Základním právním režimem je společný článek 3 Ženevských úmluv, jako pouhé humanitární minimum, a některé smlouvy haagského práva. Toto se aplikuje na horizontální či vertikální ozbrojený konflikt nižší intenzity. Dosahuje-li konflikt vyšší intenzity a jedná-li

[13] ONDŘEJ J. et al. *Mezinárodní humanitární právo. op. cit.* s. 40.
[14] Společný čl. 2 odst. 2 Ženevských úmluv
[15] *„/.../ regardless of the reasons or the intensity of this confrontation."* ICRC, *How is the Term „Armed Conflict" Defined in International Humanitarian Law?* Opinion Paper. March 2008. s. 1.
[16] *„/.../ ozbrojené konflikty, ve kterých národy bojují proti koloniální nadvládě a cizí okupaci a proti rasistickým režimům, aby uplatnily své právo na sebeurčení /.../"* Čl. 1 odst. 4 Dodatkového protokolu I
[17] Společný čl. 3 Ženevských úmluv

se zároveň o konflikt vertikální, rozšiřuje se aplikovatelný režim o Dodatkový protokol II z roku 1977.[18] Ten sám vymezuje v čl. 1 odst. 1 materiální rozsah aplikace na *„konflikty /.../, k nimž 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.“* Z toho vyplývá, že aby mohlo dojít k aplikaci Dodatkového protokolu II, musí povstalecká skupina (neboť u státu se toto předpokládá) kumulativně vyhovět čtyřem kritériím: odpovědné vedení skupiny, kontrola části území, možnost vést trvalé a koordinované vojenské operace a schopnost aplikovat ustanovení Protokolu.[19]

Důležité je také odlišení vnitrostátního ozbrojeného konfliktu od „*vnitřních nepokojů a napětí, jako jsou vzpoury, izolované a sporadické násilné činy a ostatní činy podobné povahy*“[20] – tyto spadají pod tzv. dolní hranici ozbrojeného konfliktu, a MHP se tak neaplikuje.[21]

1.3. Typologie 5 generací moderního válečnictví

Jak již bylo řečeno, MHP je spojeno s nejkrutější oblastí lidského počínání – válčením. Jeho vývoj byl předpokladem nejen pro samotný vznik MHP, ale také pro jeho další směřování. Pro lepší ilustraci této provázanosti, a také pro nastínění problematiky válčení v kybernetickém prostoru, se autorka rozhodla použít tzv. teorii čtyř generací válčení, jejímž autorem je americký vojenský teoretik William S. Lind.[22] Na tomto místě je důležité zdůraznit, že se nejedná o koncept právní. Navíc je značně zjednodušený a není bezvýhradně přijímán. Pojem „generace“ je zde chápán jako „kvalitativní posun“ a popisuje vývoj od uzavření Vestfálského míru v roce 1648, který vidí jako počátek období moderního válčení.

První generace je spojena s monopolem státu na válku a masovostí armád. Předtím probíhaly konflikty mezi různými entitami, jako jsou rodiny, kmeny či náboženské skupiny. Po Vestfálském míru však primát zaujímá stát a jeho armáda. Je to právě tato generace, která

[18] ONDŘEJ J. et al. *op. cit*. s. 349.
[19] BÍLKOVÁ, Veronika. *Úprava vnitrostátních ozbrojených konfliktů v mezinárodním humanitárním právu.* 2006. Doktorská disertační práce. s. 113.
[20] Čl. 1 odst. 2 Dodatkového protokolu II
[21] BÍLKOVÁ V. *Úprava vnitrostátních ozbrojených konfliktů v mezinárodním humanitárním právu. op. cit*. s. 50.
[22] LIND, William S. (et al.). *The Changing Face of War: Into Fourth Generation.* Marine Corps Gazette, October 1989. s. 22-26. a dále LIND, William S. *Understanding Fourth Generation of War.* Military Review, September/October 2004. s. 12-16.

dala vzniknout znakům, které si s armádou dodnes spojujeme: armádní dril, uniformy, hodnosti a salutování. Masová vojska byla podrobována vojenskému řádu a disciplíně, armáda nastupovala v liniích a kolonách, avšak v protikladu k tomu stálo bojiště, kde po rozpoutání bojů žádný řád nepanoval. Tato taktika se tak spolu se zapojením výdobytků průmyslové revoluce stala obsoletní.

Přibližně kolem roku 1860 můžeme hovořit o formování druhé generace válčení, která však byla plně rozvinuta Francouzi až za první světové války. Základním stavebním kamenem této generace je masivní palebná síla, dělostřelectvo. Po vojácích byla stále vyžadována naprostá disciplína a poslušnost, vlastní iniciativa byla nežádoucí. Ač mluvíme o období počátku 20. století, Lind říká, že *„americká armáda určitým způsobem stále aplikuje tento způsob boje“*,[23] třebaže dělostřelectvo bylo nahrazeno leteckými jednotkami. Nejedná se tedy o lineární vývoj, jak vidíme na výše uvedeném případě, neboť nástup další generace neznamená nutně „ukončení“ generace předchozí. To je patrné i na případu třetí generace, která byla vyvinuta přibližně ve stejném období, avšak jejími tvůrci byli Němci.

V souvislosti se třetí generací válčení mluvíme o tzv. metodě blitzkrieg či manévrovacím válčení. Ze samotného pojmenování blitzkrieg, tedy blesková válka, vyplývá podstata tohoto druhu válčení – rychlost, překvapení a mentální i fyzické narušení struktury nepřítele. Jednotky neútočí lineárně, ale pronikají do nepřítelova týlu, a způsobují tak jeho kolaps zevnitř. Velký důraz je kladen na osobní disciplínu a iniciativu, neboť rozkazy jsou vydávány tak, že stanovují cíle, ale nikoli již metody k jejich dosažení. Rychlost, s jakou pronikají jednotky na území protivníka, však s sebou nese i další negativa, a to vysoké civilní ztráty, kdy civilisté nejsou schopni dostatečně rychle vyklidit obsazované pole.[24]

Největší změnu ve výše popsaném vývoji přinesla čtvrtá generace. Proti sobě již nestojí masové armády států – místo nepřítele zaujímají nestátní aktéři (typickým příkladem může být hnutí Hamás či Al-Káida) s nižším stupněm organizovanosti a výcviku. Tato asymetrie mezi aktéry je definujícím znakem čtvrté generace válčení. Stát ztrácí monopol na válku a je, jak se domnívá Lind *„v této asymetrické, či též guerillové válce, přes veškerou palebnou sílu slabší stranou a prohrává“*.[25] Guerillové válčení není ve vojenství nic nového – jedná se

[23] *„Second Generation war is relevant today because U.S. Army and USMC learned Second Generation war from the French during and after World War I, and it remains the American way of war /.../“* LIND W. S. *Understanding Fourth Generation of War. op. cit*. s. 12.

[24] FOLTÝN, Otakar. *Vojenské aspekty vývoje mezinárodního humanitárního práva na pozadí čtyř generací moderních ozbrojených konfliktů.* In: *Mezinárodní humanitární právo: vznik, vývoj a nové výzvy*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2015. s. 30.

[25] *„/.../ the state loses its monopoly on war. All over the world, state militaries find themselves fighting nonstate opponents /.../. Almost everywhere, the state is losing.“* LIND W. S. *Understanding Fourth Generation of War. op. cit*. s. 13.

o standardní taktiku, která byla užívaná před nástupem monopolu státu (tedy před začátkem moderního válečnictví, jak bylo definováno výše). Konflikty jsou typické nižší intenzitou, delším trváním a také tím, že většinu obětí tvoří civilisté.[26]

V souvislosti s nástupem nových fenoménů jako jsou nanotechnologie, digitální bojiště či bezpilotní prostředky navázali na Lindovu teorii čtyř generací další vojenští teoretici[27] a obohatili ji o generaci pátou (někdy označována také jako „pátý stupeň"). Sám Lind však nesouhlasí s tímto rozšiřováním, kdy dle jeho názoru k posunu dosud nedošlo, neboť „kvalitativním posunem" je myšlen koncept, kdy „*útvary válčící v předchozí generaci nedokáží již porazit útvary generace nové*."[28] Technologický posun, který je jedním ze stěžejních argumentů pro pátou generaci, je dle Linda nedostatečný.

Zastánci páté generace však apelují na nutnost porozumět problematice nové generace válčení, o které mluví jako o stínové či informační válce. Skupiny protivníků se zmenšují až k pouhým jednotlivcům, síla se přesouvá z fyzického bojiště do psychologické a informační roviny. Útoky jsou prováděny tak, aby je v ideálním případě nebylo možné detekovat a bránit se jim. Strana konfliktu jednoduše řečeno bojuje sama se sebou, aniž by věděla, že je ovlivňována protivníkem.[29]

Koncept páté generace je, jak z výše uvedeného vyplývá, nový a určitým způsobem vágní a nedefinovaný. Nepochybně z toho však můžeme vyvodit, že kybernetický prostor a digitální bojiště jsou reálným prostorem pro vedení konfliktů a že podstatně mění zavedené způsoby válčení.

2. Základní pojmy kybernetického prostoru

Pojmy spojené s kybernetickým prostorem, jako je kybernetický útok, kybernetická špionáž či dokonce kybernetická válka, jsou pojmy, které jsou sice v dnešní době hojně používány, avšak nemají ustálené definice, a jsou tak v jednotlivých sférách vnímány různě. Z tohoto důvodu považuje autorka za nutné, aby byly pojmy, které budou stěžejní pro

[26] FOLTÝN O. *Vojenské aspekty vývoje mezinárodního humanitárního práva na pozadí čtyř generací moderních ozbrojených konfliktů op. cit.* s. 31.
[27] Například HAMMES, Thomas X. *Fourth Generation Warfare Evolves, Fifth Emerges.* Military Review, May/June 2007. s. 14-23.
[28] *„/.../ an army from a previous generation cannot beat a force from the new generation. /.../ technological determinism, the false notion that war´s outcome is usually determined by superiority in equipment."* LIND, William S. *On War. Fifth Generation Warfare?* Dostupné z: https://www.lewrockwell.com/2004/02/william-s-lind/fifth-generation-warfare/
[29] Jednou z prací, která se snaží různé názory na další posun ve válčení obsáhnout a systematizovat, je například ABBOTT, Daniel H. *The Handbook of Fifth-Generation Warfare (5GW).* Nimble Books LLC, 2010.

předmět této práce, dostatečně definovány, a to především s ohledem na jejich jednotlivé významy v rámci MHP.

2.1. Kybernetický prostor

Chceme-li zkoumat možnosti aplikace MHP na kybernetické vedení boje, je důležité začít pojmem kybernetický prostor (zkráceně též kyberprostor), který vymezuje novou a specifickou oblast, virtuální prostředí, jež bylo jako první zcela vytvořeno člověkem. Výkladový slovník kybernetické bezpečnosti definuje kybernetický prostor jako: *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“*[30] Tato definice se vyskytuje například v českém zákoně č. 181/2014 Sb., o kybernetické bezpečnosti. Jinou definici nabízí Tallinnský manuál, který uvádí, že kyberprostor je: *„prostředí tvořené fyzickými a nefyzickými komponenty za účelem uchování, změny a výměny dat při použití počítačových systémů.“*[31] Jedná se tedy o virtuální prostředí globálního rozsahu tvořené navzájem propojenými počítačovými systémy, ve kterém dochází ke vzniku a přenosu informací. Zvláštností kyberprostoru je napojení virtuálního prostředí na prvky fyzického světa – počítačové systémy. Ačkoli tedy existuje nezávisle na technickém zařízení, pokud by došlo ke zničení všech zařízení umožňujících vstup do kybernetického prostoru, došlo by v podstatě k jeho zániku.[32]

Pro lepší pochopení toho, jaké možnosti kybernetický prostor skýtá nejen pro vojenské využití, pracují autoři s konceptem tří vrstev: fyzické, logické a sociální.[33] Fyzická vrstva představuje výše zmíněná technická zařízení, která se fyzicky nacházejí v reálném světě (typicky hardware). Logická vrstva zahrnuje aplikační vrstvu (software) a informace, k jejichž výměně potom dochází mezi kyberosobami (čímž máme na mysli identifikace osoby ve virtuálním prostředí), jež jsou společně s osobami reálnými součástí vrstvy sociální.

Vznikem tohoto nového prostředí došlo k tomu, že se velké množství lidských aktivit přesunulo z fyzického světa do toho kybernetického. Totéž nastalo i u aktivit válečných. Tento fenomén nezůstal bez povšimnutí ze strany států (již v roce 2006 to byly Spojené státy

[30] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* 3. aktualiz. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2015. s. 70.
[31] *„The environment formed by physical and non-physical components to store, modify, and Exchange data using computer networks.“* SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 564.
[32] KOLOUCH, Jan, Pavel BAŠTA, Andrea KROPÁČKOVÁ a Martin KUNC. *CyberSecurity.* 1. vyd. Praha: CZ.NIC, 2019. s. 36.
[33] Ibid. s. 37.

americké, které jako první začaly oficiálně vytvářet vojenskou strategii pro kyberprostor[34]), ani mezinárodních organizací. Na Varšavské konferenci v roce 2016 přijalo NATO usnesení, ve kterém uznalo kybernetický prostor jako další operační doménu vedle souše, moře a vzduchu.[35] Na základě tohoto uznání je možné dále rozvíjet obranné aktivity členů NATO proti kybernetickým útokům, především investovat finanční i lidské zdroje či přizpůsobovat organizaci armádních složek těmto novým podmínkám. Také z toho vyplývá, že NATO je připraveno plnit svoje závazky vyplývající z článku 5 Washingtonské úmluvy, tedy zajistit kolektivní sebeobranu v případě útoku na jeden z členských států, i v kybernetickém prostoru.[36]

2.2. Kybernetická operace

Pojmem kybernetická operace označuje Tallinnský manuál *„použití kybernetických prostředků, za pomocí kterých je možné dosáhnout cílů v rámci kyberprostoru."*[37] Jedná se tedy o nejobecnější vyjádření jakékoli aktivity v kyberprostoru, která ovlivňuje chod kybernetické infrastruktury. Typicky se bude jednat o kybernetické operace s negativními následky, jako je narušení dostupnosti, důvěrnosti či celistvost dat.[38]

Příkladem může být DDoS útok (Distributed Denial of Service), v jehož případě jde o využití velkého počtu zařízení k zahlcení cíle požadavky, které v důsledku vedou ke zpomalení či dokonce nepřístupnosti služeb poskytovaných cílem. Notoricky známý je případ Estonska, které se stalo v roce 2007 na celých 22 dní cílem DDoS útoků. Postiženy byly nejen internetové stránky parlamentu, ministerstev a politických stran, ale také některých bank a médií. Nelze s jistotou říci, kdo za těmito operacemi stál, avšak obecně se má za to, že se jednalo o reakci Ruska na přesun památníku osvobození Estonska Sovětským svazem z centra Tallinnu.[39]

---

[34] BASTL, Martin a Zuzana GRUBEROVÁ. *Kyberprostor jako „pátá doména"?* Vojenské rozhledy 4/2013. s. 11.
[35] *Warsaw Summit Communiqué*. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July, 2016. para 70.
[36] Ibid. para 72.
[37] *„The employment of cyber capabilities to achieve objectives in or through cyberspace."* SCHMITT M. *Tallinn Manual 2.0*. *op. cit.* s. 564
[38] Jedná se o tzv. C (confidentiality) – I (integrity) – A (availability) triádu kybernetické bezpečnosti, která představuje základní úkoly kybernetické bezpečnosti. Více například KOLOUCH J. et al. *CyberSecurity*. *op. cit.* s. 45.
[39] TRAYNOR, I. *Russia accused of unleashing cyberwar to disable Estonia*. The Guardian. 17.5.2007. [cit. 28.10.2019]. Dostupné z: https://www.theguardian.com/world/2007/may/17/topstories3.russia

Aby bylo možné aplikovat na kybernetické operace MHP, je nutné, aby se jednalo o kybernetické operace podniknuté v kontextu ozbrojeného konfliktu.[40] Může se tedy jednat v zásadě o dva typy operací: kybernetické operace, které probíhají současně s vedením ozbrojeného konfliktu konvenčními prostředky, avšak nedosahují samy o sobě intenzity útoku, a kybernetické operace, které již dosahují takové intenzity útoku, jak je stanoven v čl. 49 odst. 1 Dodatkového protokolu I. Druhým typem kybernetické operace se bude zabývat následující podkapitola.

U kybernetických operací, které probíhají současně s ozbrojeným konfliktem, jenž je veden konvenčními prostředky, se posuzuje souvislost mezi kybernetickými operacemi a tímto ozbrojeným konfliktem. Co se týče míry této souvislosti, zastávají odborníci, kteří se podíleli na tvorbě Tallinnského manuálu, dva různé přístupy.[41] Dle prvního přístupu je nutné, aby kybernetická operace určitou významnou měrou přispěla k vedenému kinetickému ozbrojenému konfliktu. Pro druhý názor je dostatečné, že kybernetická operace proběhla mezi protivníky, jež proti sobě v rámci ozbrojeného konfliktu stojí. Pro představu můžeme opět použít příklad z nedávné historie, a to z roku 2008, kdy mezi Gruzií a Ruskem došlo k ozbrojenému konfliktu. Již před samotným vstupem ruské armády došlo k prvním kybernetickým operacím proti webovým stránkám prezidenta, vlády, ministerstev zahraničí a obrany, dále potom i proti bankám a médiím.[42] Pro tak blízkou souvislost kinetických bojů a kybernetických operací, je za původce kybernetických operací považováno Rusko. Někteří autoři vyjadřují názor, že ačkoli kybernetické operace probíhaly během ozbrojeného konfliktu a jejich cíli byly také cíle vojenské, čímž máme na mysli především ministerstvo obrany, nebyla jejich souvislost s ozbrojeným konfliktem dostatečná, neboť samy nepůsobily destruktivně vůči osobám ani objektům a vlastně ani nepřesáhly hranici pouhé nepříjemnosti.[43] Naopak Tallinnský manuál uvádí tuto situaci jako příklad, kdy bude MHP aplikovatelné na takto provedené operace, protože je zde očividné, že jejich účelem byla podpora ozbrojeného konfliktu.[44]

Autorka je toho názoru, že kybernetická operace by měla určitou měrou přispívat k vedenému ozbrojenému konfliktu. Opačné stanovisko by totiž vedlo k rozšiřování aplikace

[40] „*Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict.*" SCHMITT M. *Tallinn Manual 2.0. op. cit.* Pravidlo 82.
[41] Ibid. s. 376.
[42] TIKK, Eneken, Kadri KASKA a Liis VIHUL. *International Cyber Incidents: Legal Considerations*. Tallinn: CCD COE, 2010. s. 69 a násl.
[43] BRUNER, Tomáš. *K podmínkám způsobu aplikace mezinárodního humanitárního práva na kybernetické operace.* In: *Mezinárodní humanitární právo: vznik, vývoj a nové výzvy*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2015. s. 168.
[44] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 376.

MHP na situace, které spadají pod jiná mezinárodněprávní odvětví, jako například právo lidských práv. Na druhou stranu, pokud bychom zvolili velmi restriktivní přístup, který by vyžadoval prokázání velkého počtu souvislostí, mohlo by dojít k praktické nemožnosti aplikovat MHP, a tak k neadekvátní reakci na takový typ kybernetických operací.

Odhlédneme-li od skutečnosti, že otázka přičitatelnosti jednání je v kybernetickém prostoru obecně zvláště problematická, bude kvalifikace míry souvislosti kybernetické operace s ozbrojeným konfliktem ještě obtížnější v případě vnitrostátního ozbrojeného konfliktu. Problematické bude především rozlišení mezi kybernetickými operacemi, které představují součást ozbrojeného konfliktu, a těch, které jsou svou povahou vynucováním práva na vlastním území státu.[45]

2.3. Kybernetický útok

Definice útoku je z pohledu MHP velice důležitým krokem k naplňování jeho smyslu a účelu. Při pohledu na Dodatkový protokol I zjistíme, že mnoho stěžejních pravidel vedení boje, jako je například zákaz útoků na civilní obyvatelstvo (čl. 51 odst. 2) a civilní cíle (čl. 52 odst. 1) nebo preventivní opatření při útoku (čl. 57), s tímto pojmem pracuje. Ne jinak tomu bude v kybernetickém prostoru, avšak zřetelně zde bude vystupovat problematičnost přenesení standardů reálného světa do toho kybernetického.

Jak již bylo uvedeno výše, kybernetické útoky jsou podmnožinou kybernetických operací. Jejich specifikem je, že při nich dochází k užití násilí. Definice kybernetického útoku vychází z článku 49 odst. 1 DP I, kde se za útoky považují *„násilné činy proti protivníkovi, a to jak útočné, tak i obranné povahy.“* Tallinnský manuál však místo „násilných činů“ přichází s konkrétnějším určením podoby operací – jedná se o takové kybernetické operace, u kterých *„lze rozumně předpokládat, že způsobí zranění či smrt osobě, nebo škodu či zničení objektu“*.[46] Slovo „způsobí“ bude v tomto ohledu vykládáno jako rozumně předpokládaný následek kybernetického útoku v reálném světě, nikoli jen jako důsledek pro cílový kybernetický systém.[47]

Pro ilustraci můžeme uvažovat o situaci, kdy by byla kybernetické operaci podrobena čistička vod, která jako jediná zásobuje pitnou vodou civilní obyvatelstvo přilehlé oblasti. Pro

[45] Ibid. s. 377.
[46] „*A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.*“ SCHMITT M. *Tallinn Manual 2.0. op. cit.* Pravidlo 92.
[47] Ibid. s. 415.

počítačový systém by tato operace neměla žádné destruktivní následky, ale znehodnocení vody by mohlo mít fatální důsledky pro civilní obyvatelstvo, a jednalo by se tak o zakázaný útok dle čl. 54 odst. 2 DP I.

Většina odborníků, kteří se podíleli na tvorbě Tallinnského manuálu, se shodla, že za útok bude považována i taková kybernetická operace, která způsobí fyzické poškození technického zařízení (tedy část fyzické vrstvy kybernetického prostoru) vyžadující fyzickou opravu či výměnu, nebo pokud způsobí ztrátu funkčnosti některého z komponentů.[48]

Velká část kybernetických operací však vůbec nemusí vyústit v tak závažné situace. Velmi často budou dosahovat pouze určité míry nepříjemnosti a obtíží, jež však nedosahuje takové úrovně, aby byla operace považována za kybernetický útok.[49] Příkladem může být blokace poskytovatele e-mailových schránek, čímž by došlo k nemožnosti e-mailové komunikace mezi postiženými. Avšak vyřazení bankovního systému z činnosti už by dle některých[50] naplnilo kritéria útoku, nikoli pouhé nepříjemnosti. Jak je vidět, neexistuje všeobecná shoda na přesném určení míry nepříjemnosti, která ještě nespadá do kategorie útoku a která už ano. Také rychlý vývoj technologií, sofistikovanosti a četnosti kybernetických operací přispívá k tomu, že se chápání tohoto kritéria neustále proměňuje.

3. Aplikovatelnost základních zásad MHP v kybernetickém prostoru

Základní zásady či principy MHP jsou obecně uznávány jako vůdčí ideje systému MHP. Jejich důležitost nespočívá pouze v tom, že poskytují základy pro vznik jednotlivých pravidel MHP, ale také v jejich přímé aplikovatelnosti, kdy vyjadřují základní podstatu a význam konkrétních pravidel MHP.[51] Jsou nadány určitou mírou abstraktnosti, díky které mohou flexibilně reagovat na vývoj práva, a zároveň i specifickým právním významem, jenž poskytuje MHP alespoň minimum právní jistoty.[52] Minimum, které je pro toto odvětví práva stěžejní a bez kterého by jen těžko mohlo docházet k jeho adekvátní aplikaci. Římský statut Mezinárodního trestního soudu z roku 1998 v článku 21 odst. 1 pís. b) stanovuje, že *„Soud*

[48] Ibid. s. 417.
[49] Ibid. s. 418.
[50] DROEGE, Cordula. *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians*. International Review of the Red Cross. Vol. 94. Number 886. 2012. s. 560.
[51] SASSÒLI, Marco, Antoine A. BOUVIER a Anne QUINTIN. *How does law protect in war?: cases, documents, and teaching materials on contemporary practice in international humanitarian law* [online]. Third, expanded and updated edition. Geneva: International Committee of the Red Cross, 2011 [cit. 2019-11-17]. Military legal resources. https://casebook.icrc.org/law/fundamentals-ihl#d_iii_2_c
[52] KOLB, Robert. *Advanced Introduction to International Humanitarian Law.* Cheltenham, UK: Edward Elgar, 2014. Elgar Advanced Introductions. s. 75.

bude uplatňovat: /.../ aplikovatelné smlouvy a zásady a pravidla mezinárodního práva, včetně uznávaných zásad mezinárodního práva ozbrojených konfliktů.“ Tímto je zdůrazněna důležitost těchto zásad nejen pro rozhodovací praxi Mezinárodního trestního soudu, ale logicky do určité míry i pro praxi aplikační.

Ačkoli mezi jednotlivými zásadami neexistuje hierarchie, můžeme zásady vojenské nutnosti a humanity označit za naprosto základní, neboť ty odrážejí podstatu MHP, a z jejich vzájemného vztahu jsou odvozovány další zásady, především zásada rozlišování, přiměřenosti a zákazu zbytečných útrap.[53]

V roce 2015 skupina expertů na poli informačních a telekomunikačních technologií vypracovala zprávu (dále jen „zpráva GGE“) pro Valné shromáždění OSN, ve které bylo vůbec poprvé uvedeno, že základní principy jako humanita, nezbytnost, proporcionalita a rozlišování, jsou aplikovatelné tam, kde je to nutné, tzn. za ozbrojeného konfliktu.[54] Rezolucí[55] přijatou Valným shromážděním byly následně státy vyzvány, aby se i v kybernetickém prostoru v případě ozbrojeného konfliktu chovaly v souladu se závěry výše uvedené zprávy GGE. Což tedy znamená, aby i v kyberprostoru byly aplikovány základní zásady MHP. Možnosti této aplikace tak budou předmětem zkoumání této kapitoly.

3.1. Zásada vojenské nutnosti

Vojenská nutnost je stěžejním pojmem vojenství a tedy řekněme prazákladem celého odvětví MHP, neboť bez nutnosti využít vojenských sil vůči protivníkovi by neexistovaly ozbrojené konflikty. V moderní historii se poprvé setkáváme s vyjádřením podstaty vojenské nutnosti v Lieberově kodexu z roku 1863, který vznikl jako vojenská příručka pro armádu severu v americké občanské válce.[56] Dle čl. 14 vojenská nutnost *„spočívá v nezbytnosti těch opatření, která jsou nepostradatelná pro zajištění cílů války a která jsou legální dle současných zákonů a obyčejů války“*.[57] Co se v definici zmíněných cílů války týče, pracuje

[53] Různí autoři konstruují systém základních zásad různě. Srov. SASSÒLI, Marco, Antoine A. BOUVIER a Anne QUINTIN. *How Does Law Protect In War? Cases, Documents and Teaching Materials on Contemporary Practice in International Humanitarian Law.* [online] *op. cit.* Dostupné z: https://casebook.icrc.org/law/fundamentals-ihl#d_iii_2_c

[54] UN Doc. A/70/174 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. *op. cit*. Bod 28, pís. b).

[55] UN Doc. A/RES/70/237 *Developments in the field of information and telecommunications in the context of international security.* 30 December 2015.

[56] ONDŘEJ J. et al. *Mezinárodní humanitární právo. op. cit.* s. 201.

[57] *„/.../consists in the necessity of those measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usage of war.“* Instructions for the Government of Armies of the United States in the Field (Lieberův kodex), 1863.

s tímto pojmem Petrohradská deklarace z roku 1868, když stanoví, *„že jediný legální cíl, jejž státy mají sledovat za války, je oslabení vojenských sil nepřítele, že k tomuto účelu stačí učinit nezpůsobilým k boji co možná největší počet lidí“*.[58] Pokud bychom tedy tato vyjádření spojili, můžeme říci, že vojenská nutnost je požadavek vojenského oslabení nepřítele, a to především vyřazením z boje co největšího počtu kombatantů, avšak zároveň musí být toto jednání v souladu s normami MHP.

Vojenskou nutnost můžeme chápat ve třech rovinách: materiální, normativní a soudní.[59] V normativním smyslu se jedná o základ pro vznik norem MHP, tedy prvopočátek, od něhož se odvíjejí další konkrétní normy a jsou s ním v souladu. Z hlediska kybernetického prostoru je „kybernetická“ vojenská nutnost rozhodně přítomna, neboť co jiného mohlo vést k militarizaci kybernetického prostoru, k užívání kybernetických operací k podpoře konvenčních prostředků pro vedení boje, či samostatných kybernetických útoků, než vojenská nutnost porazit nepřítele s co nejmenšími ztrátami. Proti tomuto chápání, že by rozšiřování bojiště o bojiště virtuální bylo způsobeno adekvátním prosazováním vojenské nutnosti, vystoupila například Čína, která tvrdila, že kybernetický prostor by neměl být militarizován, ale naopak chráněn před válečnými aktivitami.[60]

Vojenskou nezbytností v materiálním smyslu je praktická aplikace na bojišti, kdy se má činit pouze to, co je vojensky nutné, a už ne to, co nutné není – *„jakási amoralita, která odlišuje kompetentní a nekompetentní boj.“*[61] V tomto ohledu bychom mohli diskutovat, nakolik bylo nutné v případě kybernetických operací vedených proti Gruzii nejen zablokovat určité vládní webové stránky, ale umístit na ně fotografie prezidenta, na kterých je přirovnáván k Adolfu Hitlerovi.[62] Samozřejmě navazující otázkou je, zda se v tomto případě jedná o součást útoku, tudíž se na něj aplikuje princip vojenské nutnosti, nebo zda se jedná o pouhou nepříjemnost, která s ohledem na svoji bezvýznamnost nespadá vůbec do rámce hodnocení. Jak již bylo řečeno výše v části věnované kybernetickým operacím probíhajícím současně, názory ohledně aplikovatelnosti MHP se liší. Z dnešního pohledu bychom však možná mohli uvažovat o podřazení takových operací pod normy MHP, protože

[58] Petrohradská deklarace, 1868. In: ONDŘEJ, Jan a Miroslav POTOČNÝ. *Obecné mezinárodní právo v dokumentech*. 3., dopl. vyd. V Praze: C.H. Beck, 2010. Beckova skripta. s. 295.
[59] HAYASHI, Nobuo. *Military Necessity: The Art, Morality and Law of War*. Cambridge: Cambridge University Press, 2020. s. 4. Kniha bude publikována až po uzavření této práce a byla použita s laskavým svolením autora.
[60] DROEGE C. *Get off my cloud: cyberwarfare, international humanitarian law, and the protection of civilians*.*op. cit.* s. 537.
[61] *„/.../ an amoral notion that separates competent fighting from incompetent figting.“* HAYASHI N. *Military Necessity: The Art, Morality and Law of War*. *op. cit.* s. 10.
[62] BRUNER T. *K podmínkám způsobu aplikace mezinárodního humanitárního práva na kybernetické operace. op. cit.* s. 168.

v mezinárodně propojeném světě mají větší destrukční potenciál. Vyvěšení takové fotografie na napadenou webovou stránku by se tedy dalo považovat za součást útoku, a tudíž aplikovat vojenskou nezbytnost. Nicméně v tomto konkrétním případě by nejspíše převládl názor, že se sice jedná o akci, která není vojensky nezbytná, avšak není nositelem výrazného vojenského potenciálu.

Vyjádření vojenské nezbytnosti nalezneme ve velké míře v oblasti mezinárodního trestního práva, především v rozhodnutích ICTY.[63] Soud posuzoval především válečné zločiny týkající se rozsáhlé a svévolné devastace objektů neomluvitelné vojenskou nutností.[64] Možnost ničit a zabírat nepřátelský majetek, pokud si to žádá vojenská nutnost, je připuštěna čl. 23 pís. g) Úmluvy o zákonech a obyčejích války pozemní z roku 1899. V podstatě se tímto umožňuje výjimka, která by měla být obhajitelná vojenskou nutností, avšak pouze tehdy, je-li taková možnost výslovně v daném pravidle stanovena.[65] Obecně lze ale shrnout, že vojenská nezbytnost jako výjimka je vykládána velmi striktně.[66] V kybernetickém prostoru se ničení nepřátelského majetku stává jednodušší a bezbolestné, tudíž je třeba nastavit určité limity. Je však stejně jako v případě konvenčních bojů úlohou soudů, aby posoudily, do jaké míry je ničení nepřátelské kybernetické infrastruktury nezbytné pro dosažení vojenské výhody. V tomto ohledu je nicméně nezbytné zapojit preventivní opatření, a to adekvátní výcvik vojáků, resp. útočníků, a jejich velitelů, kteří jsou následně trestně odpovědni z pozice nadřízeného.[67]

3.2. Zásada humanity

Jak již bylo zmíněno v první kapitole této práce, myšlenka humanity, lidskosti, byla zásadní pro vznik ženevského práva, tedy té části MHP, která se věnuje ochraně civilistů a osob *hors de combat*. Prostupuje však i do oblasti práva haagského, kde je například základem pro zákaz užívání takových zbraní, jež by způsobovaly nadměrné utrpení.[68] Humanita stojí často v protikladu k zásadě vojenské nutnosti, a tak ji limituje. Pro výslovné vyjádření tohoto vztahu můžeme opět použít ustanovení Petrohradské deklarace z roku 1868,

[63] KOLB R. *Advanced Introduction to International Humanitarian Law*. *op. cit.* s. 91.
[64] ICTY, *Prosecutor v. Pavle Strugar*, Case No. IT-01-42-T, Trial Chamber II. Trial Judgment. 31 January 2005. para 297.
[65] FLECK D. *The Handbook of International Humanitarian Law*. *op. cit.* s. 37.
[66] KOLB R. *Advanced Introduction to International Humanitarian Law*. *op. cit.* s. 92.
[67] Čl. 28 pís. a) a b). Římský statut Mezinárodního trestního soudu. 17. července 1998. In: ONDŘEJ, Jan a Miroslav POTOČNÝ. *Obecné mezinárodní právo v dokumentech*. *op. cit.* s. 320.
[68] KOLB R. *Advanced Introduction to International Humanitarian Law*. *op. cit.* s. 78

podle kterého *„se potřeby války musí zastavit před požadavky humanity“*.[69] Úkolem MHP je udržovat tuto křehkou rovnováhu a vyrovnávat opačné zájmy těchto zásad.

Princip humanity je dle některých autorů[70] jasně vyjádřen v tzv. Martensově klauzuli, která původně vznikla jako část preambule k Haagské úmluvě o zákonech a obyčejích války pozemní z roku 1907 a která stanoví: *„Dokud by nemohl být sepsán úplnější válečný zákoník, pokládají Vysoké smluvní strany za prospěšné stanovit, že v případech, které nejsou pojaty v ustanoveních řádu jimi přijatého, obyvatelstvo a válčící zůstanou pod ochranou a vládou zásad mezinárodního práva, jak jsou patrny z existujících obyčejů mezi civilizovanými národy, ze zákonů lidskosti a z požadavků veřejného svědomí.“*[71] Prací[72] pojednávajících o významu Martensovy klauzule bylo napsáno nespočet, avšak pro potřeby této práce budeme pracovat s obecně přijímaným názorem, že účelem klauzule je upozornit na fakt, že je-li určitá problematika ve smlouvě opomenuta, neznamená to nutně, že by se mezinárodní právo v této oblasti snad neaplikovalo.[73] Příliš úzký výklad by totiž mohl k takovému závěru vést. Proti tomu klauzule staví požadavek posuzování jednání nejenom z hlediska smluvní úpravy, ale také obyčejového mezinárodního práva a požadavku lidskosti a veřejného svědomí. Ač byla formulována poprvé již v roce 1899, je Martensova klauzule instrumentem užívaným (ač omezeněji) dodnes.

Jako příklad aplikace Martensovy klauzule uveďme Poradní posudek Mezinárodního soudního dvora (dále jen „Soud“ či „MSD“) týkající se legality hrozby nebo použití jaderných zbraní z roku 1996. Při posuzování dané problematiky zdůraznil Soud důležitost klauzule jako *„efektivního prostředku reakce na rychlý vývoj vojenské technologie“*.[74] Při dalším rozboru se Soud vyjádřil k základním pravidlům MHP, které označil za „elementární ohledy lidskosti“[75] a které, ač vznikly dříve než jaderné zbraně, tudíž by snad mohl vyvstat argument, že nereflektují jejich zvláštnosti a nelze je na tyto zbraně vztáhnout, aplikovány budou. Soud uvedl, že tyto základní humanitární principy MHP mají být *„aplikovány na všechny formy*

[69] *Petrohradská deklarace o zákazu používání výbušných nábojů ve válce*. 11.12.1868. In: ONDŘEJ Jan a Miroslav POTOČNÝ. *Obecné mezinárodní právo v dokumentech. op. cit.* s. 295.
[70] Srov. KOLB R. *Advanced Introduction to International Humanitarian Law. op. cit.* s. 79.
[71] *Úmluva o zákonech a obyčejích války pozemní*. 18.11.1907. In: ONDŘEJ Jan a Miroslav POTOČNÝ. *Obecné mezinárodní právo v dokumentech. op. cit*. s. 296.
[72] Srov. SASSÒLI M. et. al. *How Does Law Protect In War?* [online] *op.cit.* Dostupné z: https://casebook.icrc.org/law/fundamentals-ihl#d_iii_2_c
[73] FLECK D. *The Handbook of International Humanitarian Law*. *op. cit.* s. 33.
[74] *„Martens Clause /.../ has proved to be an effective means of addressing the rapid evolution of military technology.“* ICJ. *Legality of the Threat or Use of Nuclear Weapons.* Advisory Opinion. 8 July 1996. I.C.J. Reports 1996. para 78.
[75] *„Elementary considerations of humanity“* ICJ. *The Corfu Channel Case.* Judgment. 9 April 1949. ICJ Reports 1949. s. 22.

válčení a všechny druhy zbraní; na ty minulé, současné i budoucí".[76] A samotná existence a aplikovatelnost Martensovy klauzule tento závěr pouze potvrzuje.[77]

Poradní posudek se sice vztahuje k jaderným zbraním, na druhou stranu však nelze nevidět podobnost s kybernetickým prostorem. Je nepochybné, že vedení bojů v kyberprostoru je realitou a jedná se tedy jednoduše o novou formu válčení. Počítačové kódy či protokoly, které jsou užity pro kybernetickou operaci naplňující kritéria ozbrojeného útoku, pak v podstatě mohou být v kontextu MHP nazývány kybernetickými zbraněmi.[78] A na ně by se dle stanoviska MSD vztahovaly základní principy MHP tvořící tzv. elementární ohledy lidskosti. Martensova klauzule připomíná, že v současné situaci, kdy neexistuje smluvní úprava pravidel kybernetického prostoru, není možné aplikovat zásadu, že co není zakázáno, je dovoleno. Ačkoli existující normy MHP byly vytvořeny pro potřeby pozemních, resp. námořních či leteckých vojenských operací, kybernetické operace nezůstávají v právním vakuu, ale jejich užití a způsob vedení musí neustále odpovídat standardům Martensovy klauzule.

Princip humanity je pro MHP natolik typický, že jej nalezneme v určité míře ve všech aspektech této oblasti práva.

3.3. Zásada rozlišování

Ze základní teze MHP, tedy snahy o humanizaci ozbrojených konfliktů, vyplývá slovy MSD *„kardinální princip"*[79] MHP – zásada rozlišování mezi civilisty a kombatanty a mezi civilními a vojenskými objekty. Vyjádření této zásady nalezneme v Dodatkovém protokolu I v čl. 48: *„K zajištění respektování a ochrany civilního obyvatelstva a objektů civilního rázu budou strany v konfliktu vždy činit rozdíly mezi civilním obyvatelstvem a kombatanty a mezi objekty civilního rázu a vojenskými objekty a v souladu s tím povedou své operace pouze proti vojenským objektům."* Třebaže se jedná o smluvní pravidlo, je všeobecně závazné, neboť získalo obyčejový charakter, jak potvrdil například výše zmíněný poradní posudek Soudu[80] či později studie Mezinárodního výboru Červeného kříže *Obyčejové mezinárodní humanitární právo* (dále jen „obyčejová studie MVČK") z roku 2005, která zásadu rozlišování řadí hned

[76] *„/.../ applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future."* ICJ. *Legality of the Threat or Use of Nuclear Weapons. op. cit.* para 86.
[77] Ibid. para 87.
[78] DROEGE C. *Get off my cloud: cyberwarfare, international humanitarian law, and the protection of civilians*.*op. cit.* s. 567
[79] *„cardinal principle"* ICJ. *Legality of the Threat or Use of Nuclear Weapons.* Advisory Opinion. *op. cit.* para 78.
[80] Ibid. para 84.

na první místo z celkem 161 identifikovaných obyčejových pravidel.[81] Je tedy obecně přípustné směřovat útoky pouze proti kombatantům a vojenským objektům, protože jedině vyřazením z boje co největšího počtu vojáků a zničením velkého počtu či kvalitativně významnějších vojenských objektů je možné dosáhnout vojenské výhody nad protivníkem.

3.3.1. Zásada rozlišování z hlediska osob

Rozlišení mezi kombatantem a civilistou stojí na samém začátku MHP. Pouze kombatantům náležejí určitá privilegia. Prvním z nich je, že jsou legálně oprávněni bojovat proti nepříteli a bez rizika trestního stíhání zabíjet protivníkovi bojovníky.[82] V případě, že padnou do zajetí protivníka, mají nárok na status válečného zajatce se všemi výhodami z toho plynoucími.[83] Civilisté jsou naproti tomu chráněni před destrukcí působenou vojenskými operacemi, a to tak, že nesmějí být předmětem útoku nebo se stát obětí útoku, jehož sice nejsou zamýšleným cílem, ale z důvodu nerozlišujícího charakteru tohoto útoku, není možné omezit jeho účinky pouze na vojenské cíle.[84] Tato ochrana však trvá pouze po dobu, kdy se civilisté nijak neúčastní vojenských operací, respektive, civilista obecně požívá ochrany normami MHP, avšak tato ochrana je přerušena po dobu, kdy se civilista sám a přímo účastní nepřátelských operací.[85]

Oba výše zmíněné fenomény, tedy zákaz nerozlišujících útoků a ztráta ochrany pro civilisty, kteří se přímo účastní nepřátelství, jsou jistě hodné hlubšího prozkoumání v kontextu kybernetického ozbrojeného konfliktu.

Zákaz nerozlišujících útoků je jednou částí naplňování zásady rozlišování mezi kombatanty a civilisty a mezi civilními a vojenskými objekty. Podstatou je, že vojenská síla musí být limitována tak, aby mířila pouze proti vojenskému objektu a aby výsledkem bylo zničení či poškození pouze vojenských cílů.[86] Tallinnský manuál sice v pravidle 105 potvrzuje zákaz užití prostředků a způsobů boje, které by měly nerozlišující účinky, avšak sám uznává, že v kyberprostoru jsou možné nerozlišující následky útoků vysoce pravděpodobné, když se například škodlivý malware sice zaměří na vojenský cíl, ale jakmile je jednou v síti, tedy v navzájem propojeném kybernetickém prostoru, může se volně šířit

[81] HENCKAERTS, Jean-Marie, Louise DOSWALD-BECK a Carolin ALVERMANN. *Customary international humanitarian law.* New York: Cambridge University Press, 2005. s. 3.
[82] KOLB R. *Advanced Introduction to International Humanitarian Law*. *op. cit.* s. 126.
[83] Ženevská úmluva o zacházení s válečnými zajatci (ŽÚ III)
[84] DP I. čl. 51 odst. 2 a 4.
[85] DP I. čl. 51 odst. 3.
[86] FLECK D. *The Handbook of International Humanitarian Law*. *op. cit.* s. 130.

a napadat také vojenské a civilní sítě bez rozdílu a bez možnosti útočníka jakkoli toto ovlivnit.[87] V závěru však autoři uzavírají, že nenalezli prostředky a způsoby vedení boje v kyberprostoru, jež by toto pravidlo ve smyslu možných nerozlišujících následků porušovaly, protože aby došlo k porušení pravidla, musela by škoda napáchaná v civilní infrastruktuře dosahovat určité minimální výše, a také by tento následek muselo být možné alespoň do určité míry předvídat před zahájením útoku.[88] Do protikladu k tomuto tvrzení můžeme postavit kybernetický útok provedený virem Stuxnet proti atomovým zařízením v Íránu, který nezpůsobil škody na civilních zařízeních, ale minimálně se mimo Írán dál replikoval.[89] S ohledem na rychlý technologický vývoj a snadnější dostupnost těchto technologií není dle názoru autorky vhodné možnost nerozlišujícího kybernetického útoku podceňovat. Právě naopak je třeba jí věnovat větší pozornost.

Přímá účast na nepřátelství je výjimkou z pravidla, že civilisté jsou jako jednotlivci i jako skupina chráněni před dopady ozbrojeného konfliktu. Pojem se objevuje v DP I v čl. 52 bez jakéhokoli bližšího vymezení, proto byla Mezinárodním výborem Červeného kříže vypracována výkladová směrnice,[90] jejímž úkolem bylo prakticky vyřešit nejasnosti, které pojem přímé účasti na nepřátelských akcích pochopitelně doprovázejí. Aby byla aktivita jedince či skupiny považována za přímou účast na nepřátelských akcích, a tím pádem došlo ke ztrátě ochrany, je nutné *„kumulativně splnit tři kritéria: a) hranici ohledně pravděpodobné výsledné škody; b) přímý příčinný vztah mezi aktivitou a očekávanou újmou; c) válečný nexus mezi aktivitou a nepřátelstvím probíhajícím mezi stranami konfliktu“*.[91] Tallinnský manuál tato kritéria reflektuje a upravuje přímou účast na nepřátelských kybernetických operacích v souladu s nimi.[92]

V oblasti kybernetického prostoru nabývá toto pravidlo závažnějších rozměrů, protože armády pro činnosti spojené s kybernetickými operacemi stále častěji a ve větší míře zapojují

[87] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 456.
[88] Ibid. s. 457.
[89] DROEGE C. *Get off my cloud: cyberwarfare, international humanitarian law, and the protection of civilians*.*op. cit.* s. 570.
[90] ICRC. *Interpretative Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*. Geneva: International Committee of the Red Cross, 2009.
[91] *„/.../ meet three cumulative requirements: (1) a threshold regarding the harm likely to result from the act, (2) a relationship of direct causation between the act and expected harm, and (3) a belligerent nexus between the act and the hostilities conducted between the parties to an armed conflict.“* ICRC. *Interpretative Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*. *op. cit.* s. 46.
[92] SCHMITT M. *Tallinn Manual 2.0. op. cit.* Pravidlo 97.

odborníky, kteří nejsou příslušníky ozbrojených sil.[93] Posouzení, kdy se i oni stávají legitimním vojenským cílem je tedy na místě a bude shodné s pravidly stanovenými pro konvenční boj. Problematické se v tomto ohledu může jevit časové hledisko, neboť následky kybernetické operace se nemusí projevit okamžitě, ba naopak. Je také nutné zvolit takový přístup, který bude funkční, protože pokud by byl zvolený význam přímé účasti na nepřátelství příliš široký, docházelo by ke ztrátě ochrany civilistů, která je pro MHP typická. Autoři Tallinnského manuálu se ve většině shodli na tom, že přímá účast na nepřátelství probíhá po dobu, která počíná první účastí na plánování aktivity a trvá do chvíle, než osoba ukončí svoji aktivní roli v takové aktivitě, třebaže její očekávaný následek může nastat až se značným časovým zpožděním.[94] To s sebou přináší praktické problémy pro protivníka, protože v okamžiku, kdy se kybernetická operace projeví, nemůže už proti útočníkovi legálně provést protiopatření. Důsledkem takové situace by pak mohlo být porušení norem MHP tím, že by protivník útočil na jednotlivce, kteří již však opět nabyli ochrany před vojenskými operacemi. Dle názoru autorky je důraz na kumulativní splnění podmínek pro přímou účast na nepřátelství dostatečným limitem, jenž by měl vyloučit neadekvátní postihování civilistů v konfliktu.

3.3.2. Zásada rozlišování z hlediska objektů

Z pohledu aplikace rozlišování v kybernetickém prostoru je důležitý pojem vojenského objektu a jeho definice. Ta se nachází v čl. 52 odst. 2 DP I: *„Útoky musí být přísně omezeny na vojenské objekty. Pokud jde o objekty, omezují se vojenské 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.“* Aby tedy mohl být určitý objekt nazván objektem vojenským, a mohl se tak stát cílem vojenské operace, je nutné, aby přispíval k bojovým schopnostem protivníka svojí povahou, umístěním, účelem nebo použitím. U některých objektů, jako je například sídlo generálního štábu armády protivníka, není pochyb o jejich vojenské povaze, nehledě na účel či použití. U jiných bude záležet na aktuální situaci, neboť naplněním kritérií

[93] BANNELIER-CHRISTAKIS, Karine. *Is the principle of distinction still relevant in cyberwarfare?* In TSAGOURIAS, Nikolas a Russell BUCHAN. *Research handbook on international law and cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 2017. s. 362.
[94] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 431.

stanovených v čl. 52 odst. 2 DP I se v praxi téměř každý objekt může stát vojenským objektem, a být tak legálním cílem vojenské operace.[95]

Základní teze o rozlišování mezi civilními a vojenskými objekty je sice v praxi podrobována různým pochybnostem a interpretačním odchylkám, stále však poskytuje základní vodítko. Co narušuje toto striktní rozlišení na vojenské a civilní objekty je koncept tzv. dvojího užití určitých objektů. Tedy takového užití, kdy objekty slouží zároveň jak civilistům, tak kombatantům, například jaderná elektrárna zásobuje elektřinou nejen domácnosti civilistů, ale i sklady vojenské techniky či továrny na výrobu zbraní pro armádu. Tím, že naplňují kritérium čl. 52 odst. 2 DP I, se tyto objekty stávají legitimními vojenskými objekty.[96] Pokud bychom toto kritérium aplikovali v kybernetickém prostoru, dostali bychom se do svízelné situace, kdy by v podstatě veškeré vybavení mezinárodní kybernetické infrastruktury bylo označeno za vojenské objekty. A to proto, že vojenská komunikace a kybernetická technika není oddělena od civilní, když využívá stejná zařízení, jako jsou satelity či podmořské kabely.[97] Dle Tallinnského manuálu však v současném stavu práva není jiné chápání možné – jeden objekt nemůže mít zároveň status civilního i vojenského objektu.[98] Naskýtá se tedy otázka, zda je vůbec možné princip rozlišování v kybernetickém prostoru reálně aplikovat, tedy zda jeho aplikací bude dostatečně zajištěna civilních objektů. Na základě výše uvedeného rozboru však musíme konstatovat, že v kybernetickém prostoru ztrácí princip rozlišování svoji sílu – škodlivé malware vypuštěné do sítě se mohou volně šířit a napadat další cíle bez schopnosti rozlišovat jejich povahu a provázanost vojenské a civilní kybernetické infrastruktury činí drtivou většinu kybernetické infrastruktury vojenským cílem, nikoli civilním objektem hodným ochrany MHP. Bylo by tedy z pohledu ochrany civilních struktur vhodné zaměřit se spíše na princip přiměřenosti.[99]

3.4. Zásada přiměřenosti

Další důležitou zásadou z hlediska vedení bojových operací, která je vyjádřením neustálého vyvažování vojenské nutnosti a humanity, je zásada přiměřenosti. Její podstatou je, že na vojenský objekt je možné zaútočit vždy, avšak málokdy se takováto operace obejde

[95] SASSÒLI M. et al. *How Does Law Protect In War.* [online] *op.cit.* https://casebook.icrc.org/law/fundamentals-ihl#d_iii_2_c
[96] DROEGE C. *Get off my cloud: cyberwarfare, international humanitarian law, and the protection of civilians*. *op. cit.* s. 562.
[97] Ibid. s. 563.
[98] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 445.
[99] DROEGE C. *Get off my cloud: cyberwarfare, international humanitarian law, and the protection of civilians*. *op. cit.* s. 566.

bez možných ztrát na civilních osobách či majetku. Přesto je možné takovou operaci považovat z hlediska MHP za přiměřenou, pokud tyto tzv. kolaterální ztráty nepřevyšují výhodu, která byla útokem zamýšlena. Je dozajista zajímavé, že smluvní vyjádření této důležité zásady postrádá kompaktní vyjádření, ale je rozeseto do několika ustanovení, z nichž ani jedno neobsahuje slovo proporcionální či přiměřený.[100] Přesto však není pochyb o obsahu této zásady a jejím obyčejovém charakteru. Pravidlo 14 obyčejové studie MVČK tak zní: *„zahájení útoku, u kterého je možné očekávat, že způsobí případné ztráty na životech civilistů, jejich zranění, škody na civilních objektech nebo jejich kombinaci, která by byla excesivní ve vztahu k předpokládané konkrétní a přímé vojenské výhodě, je zakázáno.“*[101] V oficiálním českém překladu DP I, kde se zásada proporcionality nachází v čl. 51 odst. 5 pís. a) a také v čl. 57 odst. 2 pís. a) a b), je místo přídavného jména „excesivní“ používáno sloveso „převyšovat“, proto bude nadále používáno tohoto překladu.

Přiměřený je tedy takový útok, ve kterém ztráty na straně civilního obyvatelstva a jeho majetku nepřevyšují konkrétní a přímou vojenskou výhodu. Tento poměr mezi ztrátami a výhodami se však může za různých situací měnit.[102] Typický uváděným příkladem je útok na most, který očividně slouží vojenským účelům. Řekněme, že je to jediná přímá cesta mezi kasárnami a městem, které je nepřítelem obsazeno, a navíc je za jeho přechod účtován civilistům poplatek, který vybírá a dále používá armáda. Jeho zničení by jistě přineslo vojenskou výhodu, avšak je rozdíl, zda k takovému útoku dojde za dne, kdy je plný civilistů, či v noci, kdy je jejich počet na mostě minimální. Neustále musíme mít na paměti, že se jedná o poměřování dvou protichůdných hodnot, u kterého není stanoven žádný objektivní standard.[103] Často pak v praxi dochází k tomu, že je výsledek *ex post* podrobován kritice a zkoumání ohledně dodržení principu proporcionality.

Obyčejovou definici přebírá Tallinnský manuál v pravidle 113 téměř doslova.[104] Specifika kybernetického prostoru však přidávají definici přiměřenosti další interpretační a aplikační problémy. Autoři Tallinnského manuálu poukazují na to, že kybernetické operace často působí nepříjemnosti či strach, ale nelze je označit za kolaterální škody, protože nedochází ke smrti či zranění civilistů či škodám na jejich majetku.[105] Avšak za určitých okolností lze pod

[100] ONDŘEJ J. et al. *Mezinárodní humanitární právo. op. cit.* s. 231.
[101] *„Launching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited.“* HENCKAERTS J. et al. *Customary international humanitarian law. op. cit.* s. 46.
[102] KOLB R. *Advanced Introduction to International Humanitarian Law. op. cit.* s. 81.
[103] ONDŘEJ J. et al. *Mezinárodní humanitární právo. op. cit.* s. 237.
[104] Srov. HENCKAERTS J. et al. *Customary international humanitarian law. op. cit.* s. 46.
[105] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 472.

výše uvedené podřadit ztrátu funkčnosti určitého zařízení.[106] Na druhou stranu, v dnešním mezinárodně propojeném světě závislém do určité míry na technologiích je možná až neadekvátní neposuzovat například širokou nedostupnost internetového bankovnictví jako relevantní vedlejší ztráty, zatímco zničení automobilu či autobusu by sice nebylo podstatné, avšak z hlediska MHP alespoň relevantní kolaterální škodou.[107] Další výzvou z hlediska specifik kybernetického prostoru je posouzení „očekávaných" vedlejších škod, které není možné odhadovat s takovou jistotou jako v kinetickém boji.[108] Není to dáno pouze relativní novostí kybernetického prostoru, a tudíž i nedostatkem zkušeností s kybernetickými útoky, ale také proto, že vypuštěním škodlivého kódu do kybernetického prostoru se otevírají další možné způsoby páchání škod. Dle Tallinského manuálu je třeba zahrnovat do poměřování nejen následky přímé, ale i nepřímé druhotné či další v pořadí, avšak pouze takové, které lze nebo by mělo být možno očekávat.[109] Co je a co není očekávatelným následkem kybernetického útoku, je otázkou, na kterou by kromě odborníků mohly hledat odpovědi také mezinárodní soudy, jako například v případě užití jaderných zbraní.

Zásada proporcionality se v Tallinnském manuálu stejně jako v DP I promítá i do oblasti preventivních opatření.[110] I v kybernetickém prostoru je třeba posuzovat, jaké vojenské výhody a jakých možných škod by bylo možné určitým útokem dosáhnout, ještě před tím, než je předmětný kybernetický útok zahájen. Toto pravidlo zdůrazňuje, jaké nároky ohledně posouzení možných důsledků kybernetického útoku jsou kladeny na vojenské velitele, kteří rozhodují o tom, zda k útoku dojde či nikoli.[111] Další oblastí, kde se uplatní princip proporcionality, je povinnost odvolat či pozastavit útok v okamžiku, kdy se ukáže, že kolaterální škody by přesáhly předpokládanou vojenskou výhodu. U některých kybernetických operací je však těžké sledovat jejich průběh a případně je tak odvolat či pozastavit, což klade o to větší důraz na správné posouzení před započetím takové operace.[112]

Nezbývá než uzavřít, že hledisko přiměřenosti útoku je kritické v oblasti kybernetického prostoru, a to jak z důvodu oslabení možnosti aplikace principu rozlišení, tak z důvodu celosvětového propojení vojenských a civilních kybernetických infrastruktur. Posouzení možných dopadů kybernetického útoku je do značné míry mnohem komplexnější a zároveň

[106] Ibid. s. 472.
[107] DROEGE C. *Get off my cloud: cyberwarfare, international humanitarian law, and the protection of civilians*. *op. cit.* s. 572.
[108] Ibid. s. 573.
[109] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 473.
[110] Srov. SCHMITT M. *Tallinn Manual 2.0. op. cit. Pravidlo 117 a 119. a DP I čl. 57 odst. 2 pís. a) a b).*
[111] DROEGE C. *Get off my cloud: cyberwarfare, international humanitarian law, and the protection of civilians*. *op. cit.* s. 573.
[112] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 484.

ještě důležitější, aby mohlo dojít k posouzení splnění parametrů přiměřenosti útoku v souladu s realitou. To nicméně nemění nic na tom, že zásada proporcionality je aplikovatelná na kybernetické útoky ve stejné míře jako na útoky konvenční.[113]

3.5. Zásada zákazu zbytečných útrap

Poslední ze zásad, která bude podrobena zkoumání, je zásada zákazu zbytečných útrap. Od předchozích se liší tím, že není zmíněna ve zprávě GGE jako zásada, která se aplikuje v kyberprostoru za ozbrojeného konfliktu.[114] Podíváme-li se znovu na poradní posudek MSD ohledně hrozby a použití atomových zbraní, zjistíme, že je princip zákazu zbytečných útrap považován vedle zásady rozlišování za kardinální princip MHP.[115] Oba dva jsou jednoduchým vyjádřením podstaty humánního zacházení za ozbrojeného konfliktu. Princip rozlišování chrání civilisty tak, že je odlišuje od kombatantů, kteří jsou legitimním cílem vojenských operací. Princip zákazu zbytečných útrap pak chrání kombatanty před tím, aby se stali oběťmi útoků takových zbraní, které by jim způsobily nadměrné útrapy. Několikrát zmiňovaná Petrohradská deklarace z roku 1868 formulovala tezi, že cílem války je oslabit bojové schopnosti protivníka, a to vyřazením z boje co největšího množství bojovníků. K vyřazení z boje je adekvátní kombatanta zabít, zranit či zajmout. Avšak z hlediska vojenské nutnosti již není pro dosažení vojenské výhody třeba podrobovat vojáky *„utrpení více než nezbytnému“*[116] způsobenému například tříštivými střelami[117] (tzv. dumdum střely), které v lidském těle jednoduše mění tvar, a tak způsobují četná vnitřní zranění.

Obyčejový charakter této zásady je neoddiskutovatelný,[118] ve smluvním vyjádření ji najdeme v čl. 35 odst. 2 DP I, a to jako logické upřesnění pravidla z odst. 1, které říká, že strany nemají volnost v oblasti výběru způsobů a prostředků vedení ozbrojeného konfliktu.[119] V podstatě se stejným vyjádřením přichází Tallinnský manuál, když nejprve v pravidle 103 definuje, co se myslí pod pojmy způsoby a prostředky kybernetického válčení, a poté v pravidle 104 zakazuje takové, které by mohly způsobit nadměrné zranění či zbytečné

[113] GILL Terry D. *International humanitarian law applied to cyber-warfare: Precautions, proportionality and the notion of 'attack' under humanitarian law of armed conflict.* In: TSAGOURIAS, Nikolas a Russell BUCHAN. *Research handbook on international law and cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 2017. s. 378.
[114] Srov. UN Doc. A/70/174 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*.. Bod 28 pís. b).
[115] ICJ. *Legality of the Threat or Use of Nuclear Weapons.* Advisory Opinion. *op. cit.* para 78.
[116] *„/.../ a harm greater than unavoidable /.../“* Ibid. para 78.
[117] Deklarace o zákazu užívání střel, které se lehce v lidském těle rozšiřují nebo zplošťují. 29. července 1899.
[118] Srov. HENCKAERTS J. et al. *Customary international humanitarian law. op. cit.* s. 237.
[119] ONDŘEJ J. et al. *Mezinárodní humanitární právo. op. cit.* s. 243.

útrapy. Již v odůvodnění tohoto pravidla je však vyjádřena pochybnost o tom, že by kybernetické operace mohly toto pravidlo porušit, respektive že by k takovému porušení mohlo dojít pouze v ojedinělých případech.[120] Za současného stavu technologického vývoje není možné, aby byla kybernetická operace namířena proti lidské bytosti jako takové, proti jejímu životu, zdraví, ale spíše proti technologiím, které ji obklopují.[121]

Je samozřejmě možné si představit případ, kdy by se kybernetická operace posuzovala z hlediska porušení tohoto principu. Jako příklad uvádí Tallinnský manuál nepříliš pravděpodobnou situaci, kdy by bylo kybernetickou operací pozměněno nastavení defibrilátoru tak, že by zastavoval a zase obnovoval činnost srdce kombatanta několikrát před tím, než by ho s konečností zabil.[122] Skutečnost, že je takový případ nepravděpodobný, neznamená, že je nemožný, protože technologický vývoj jde neustále kupředu.

Stejný argument technologického vývoje, ač v diametrálně odlišném pojetí, by se dal použít na posouzení, zda by kybernetické zbraně nemohly být vhodnější a humánnější alternativou ke zbraním využívaným dnes za konvenčního způsobu vedení ozbrojeného konfliktu. Zbytečné utrpení je totiž výsledkem situace, kdy újma způsobená danou zbraní je větší než předpokládaná vojenská výhoda.[123] Pokud tedy porovnáme konvenční zbraně a kybernetické, můžeme vyhodnotit, že neutralizace či zničení objektu kybernetickým útokem přináší menší množství ztrát.[124] Na příkladu virusu Stuxnet můžeme tento rozdíl velmi dobře vidět. Pro zničení íránských zařízení zabývajících se obohacováním uranu (tedy pro výrobu jaderných zbraní) by v konvenčním boji bylo možné užít letecké bombardování, třebaže škody by byly s ohledem na přítomnost radioaktivních látek dozajista devastující. Virus Stuxnet však dosáhl poškozování tohoto zařízení jinak – jím napadaný ovládací systém roztáčel centrifugy určené k výrobě obohaceného uranu do takových rychlostí, že byly neovladatelné a zničené.[125] Tímto dosahoval v podstatě totožných výsledků, avšak za mnohem menších ztrát.

Pro princip zákazu zbytečných útrap je relevantní míra rizika pro kombatanty, která, jak vyplynulo z posouzení, je v současném stavu technologického pokroku minimální. Kybernetické útoky mohou být dobře použity proti předmětům, avšak nikoli proti lidským

[120] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 455.
[121] HARRISON DINNISS, Heather. *Cyber warfare and the laws of war*. New York: Cambridge University Press, 2012. s. 254.
[122] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 455.
[123] FLECK D. *The Handbook of International Humanitarian Law*. *op. cit.* s. 125.
[124] HARRISON DINNISS H. *Cyber warfare and the laws of war*. *op. cit.* s. 255.
[125] BEAUMONT, Peter a Nick HOPKINS. *US was 'key player in cyber-attacks on Iran's nuclear programme'*. The Guardian. 1.6.2012. Citováno dne: 18.11.2019. Dostupné z: https://www.theguardian.com/world/2012/jun/01/obama-sped-up-cyberattack-iran

bytostem. Aplikace této zásady se tak ukázala být z hlediska kybernetického prostoru nejméně relevantní.

4. Vybrané problematické aspekty aplikace MHP na kybernetické vedení boje

Účelem této kapitoly je upozornit na vybrané zásadní aspekty MHP, které se v kybernetickém prostoru mohou jevit jako těžce aplikovatelné či dokonce neaplikovatelné. MHP je dlouho se vyvíjejícím systémem norem, jejichž přijetí mnohdy naráželo na nevoli v rámci mezinárodního společenství. A v době vzniku většiny z nich nebyl ještě kybernetický prostor ani vzdálenou představou natož realitou, jaké v současnosti MHP čelí. Přestože je obecně přijímáno, že se MHP v kybernetickém prostoru aplikuje, je nepochybně důležité podrobit alespoň vybrané instituty, které jsou buď pro MHP stěžejním důvodem existence, tedy ochrana civilistů a poskytování pomoci civilistům a raněným, nebo jsou natolik typické pro tradiční způsob vedení ozbrojeného konfliktu, že přirozeně prostupují celým odvětvím, avšak v kyberprostoru narážejí na absenci nezbytných předpokladů pro jejich existenci. Do této kategorie spadá otázka autorství útoku a teritoriální limitace. Tyto kritické aspekty a jejich samotná aplikace budou v souladu s Tallinnským manuálem podrobeny obecnému přezkumu.

4.1. Autorství kybernetické operace

Základní charakteristikou kybernetického prostoru, která je zároveň jeho největším problémem z hlediska aplikovatelnosti nejen MHP, ale i mezinárodního práva obecně, je jeho anonymita. Dokud není možné určit s dostatečnou jistotou útočníka, není ani možné zjistit, zda se jedná o aktivitu státu či nestátního aktéra, a následně tak odpovědět na otázku, kdo je za takové jednání odpovědný. A od toho se odvíjí další souvislosti, které budou popsány níže.

Ačkoli se jedná spíše o nedostatek faktický, nabízí se možnost využít právní domněnky, že za kybernetickou operaci je odpovědný stát, z jehož infrastruktury byla vypuštěna.[126] Z příkladů z praxe je však očividné, že škodlivá operace nemusí putovat z bodu A do bodu B přímo, ale že útočník za účelem svého vlastního krytí může využít různých zástupných serverů, které vytvářejí zdání, že útok vychází odtud, nebo „zotročí“ množství jiných zařízení,

[126] DROEGE C. *Get off my cloud: cyberwarfare, international humanitarian law, and the protection of civilians*. *op. cit.* s. 543.

která ke spáchání útoku využije.[127] Podíváme-li se opět na již několikrát citovaný případ DDoS útoku na Estonsko z roku 2007, zjistíme, že takto zotročená zařízení, která v souhrnu podnikala útok, se nacházela po celém světě, například ve Spojených státech amerických, Kanadě či Vietnamu.[128] Tyto skutečnosti, které jsou spíše pravidlem než výjimkou, ještě více komplikují určení autorství daného útoku.

Tallinnský manuál problém identifikace útočníka, ale také samotnou existenci kybernetické operace uznává, avšak ihned dodává, že tato faktická otázka nemá vliv na aplikaci MHP.[129] Tomuto lze dozajista přisvědčit, nicméně zůstává otázkou, nakolik je fakticky možné aplikovat MHP, pokud neznáme identitu útočníka ani jeho příslušnost či motivaci. Co se týče domněnky odpovědnosti státu za aktivity vedené z jeho kybernetické infrastruktury zmíněné výše, lze o tomto samozřejmě uvažovat, i v kontextu pravidla 6 Tallinnského manuálu, které stanoví, že stát *„nesmí umožnit, aby byly jeho území nebo kybernetická infrastruktura pod jeho vládní kontrolou použity ke kybernetické operaci, která by /.../ měla vážné následky pro jiné státy“*.[130] V případě, že stát o takovém využití svojí kybernetické infrastruktury ví, je nepochybně jeho povinností tuto aktivitu ukončit. Nicméně takových situací bude minimum, protože je vysoce nepravděpodobné, že by „tranzitní státy“ měly povědomí o tom, že je jejich infrastruktura využívána ke škodlivému útoku na jiný stát.[131] Tato domněnka by tedy byla ve svém výsledku nespravedlivá a těžko obhajitelná před jednotlivými státy.[132]

Původ útoku je tak nutno hledat jinými prostředky. S ohledem na vlastnosti kybernetického prostoru se jeví jako vhodné, aby byly aplikovány liberálnější standardy ohledně důkazů k prokázání identity útočníka.[133] V úvahu přicházejí nejen závěry expertů na kybernetickou bezpečnost, ale například i práce médií, která často o kybernetických útocích veřejně informují, či poznatky whistleblowerů.[134] Jako příklad mohou opět sloužit DDoS útoky v Estonsku, kde je obecně přijímáno, že za útoky stála Ruská federace, a to hned z několika

[127] ROSCINI, Marco. *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations.* In: OHLIN, Jens David, Kevin GOVERN a Claire FINKELSTEIN. *Cyberwar: law and ethics for virtual conflicts*. Oxford: Oxford University Press, 2015. s. 215.
[128] Ibid. s. 227.
[129] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 377.
[130] *„A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that /.../ produce serious adverse consequences for, other States.“* SCHMITT M. *Tallinn Manual 2.0. op. cit.* Pravidlo 6.
[131] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 34.
[132] DROEGE C. *Get off my cloud: cyberwarfare, international humanitarian law, and the protection of civilians*. *op. cit.* s. 544.
[133] ANTONOPOULOS, Constantine. *State responsibility in cyberspace.* In: TSAGOURIAS, Nikolas a Russell BUCHAN. *Research handbook on international law and cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 2017. Research handbooks in international law. s. 64.
[134] Ibid. s. 64.

důvodů. V první řadě je to skutečnost, že k útokům došlo poté, co bylo rozhodnuto o přemístění památníku sovětského osvobození z centra města Tallinn. Další útoky následovaly i o významných dnech – 8. a 9. května, kdy si Evropa připomíná osvobození od nacismu, na čemž měla taktéž podíl sovětská armáda. Z technického hlediska vyšlo najevo, že nástroje užité ke spáchání útoků pocházely z ruských serverů a že alespoň určitá část útoků pocházela přímo z Ruska, dokonce z IP adres ruských státních institucí.[135] Nicméně se stále jedná o určitou míru pravděpodobnosti, protože skutečného původce se vypátrat nepodařilo, navíc Ruská federace svoji vinu popírá.[136]

Nutno podotknout, že obvinění určitého státu z kybernetických operací souvisí také s politickou situací. Pokud mezi určitými státy existuje ozbrojený konflikt a z kybernetické infrastruktury jednoho byly vypuštěny kybernetické operace na druhý, je do určité míry oprávněné se domnívat, že je tento stát také útočníkem. Avšak ani znalost IP adresy, a tedy určení místa původu, nemusí být dostačující. Jak je výstižně podotknuto v Tallinnském manuálu, vyvratitelnou domněnku toho, že určitá zařízení primárně náležejí státu (příkladem uveďme tanky), nelze do kybernetického prostoru převést.[137] Výjimečné není ani zmást nepřítele tak, že pravý útočník předstírá jinou identitu. K tomu je využíván tzv. spoofing, tedy metoda, kde se jedná o *„podvržení zdrojové IP adresy u zařízení (počítače), které iniciuje spojení (s příjemcem) za účelem zatajení skutečného odesilatele“*.[138] Sofistikovanost kybernetických operací se neustále zvyšuje a tím se zvyšuje i sofistikovanost operací majících za úkol zatajit identitu útočníka.

Navíc, abychom mohli kybernetickou operaci přičíst určitému státu, nestačí pouze zjistit zařízení, ze kterého útok pocházel, ale určit také osobu, jež jej způsobila, a její vztah ke státním složkám, popř. k ozbrojené skupině, pokud bychom uvažovali v intencích vnitrostátního ozbrojeného konfliktu.[139] Pokud se podaří určit všechny tyto náležitosti, jsou pak už pravidla pro přičitatelnost určitého jednání státu stejná jako v nevirtuálním světě. Z výše uvedeného rozboru však jasně vyplývá, proč je otázka autorství kybernetické operace tak často diskutovaným a kritickým tématem v oblasti aplikace mezinárodního práva v kybernetickém prostoru.

[135] ROSCINI, Marco. *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. op. cit.* s. 216.
[136] TRAYNOR, I. *Russia accused of unleashing cyberwar to disable Estonia. op. cit.*
[137] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 91.
[138] JIRÁSEK P. et al. *Výkladový slovník kybernetické bezpečnosti. op. cit.* s. 87.
[139] ROSCINI, Marco. *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. op. cit.* s. 220.

4.2. Teritoriální limitace

Kybernetický prostor umožnil lidstvu nejvyšší míru spojení v dějinách. Nikdy předtím nebyly státy tak propojené a vzájemně na sobě závislé v různých oblastech lidských aktivit jako dnes. Ovšem tato virtuální propojenost s sebou přináší z pohledu mezinárodního práva jednu podstatnou nevýhodu, a to je ztráta hranic. Význam teritoriality a teritoriální suverenity ztrácí v kybernetickém prostoru výrazně na síle.[140] Tím se odlišuje od dalších domén určených k válčení, kde lze do velké míry přesně určovat hranice. Ty v kyberprostoru prakticky neexistují, a pojí se tak s tím nejeden problematický element. Sám Tallinnský manuál upozorňuje na problematičnost aplikovat jakákoli územní omezení v kybernetickém prostoru. V pravidle 81 stanovuje, že *„kybernetické operace jsou předmětem územních limitů, které jsou stanoveny odpovídajícími ustanoveními mezinárodního práva aplikovatelného během ozbrojeného konfliktu“*.[141] V praxi však neexistuje žádné pravidlo, jež by zapovídalo možnost přenosu dat přes území jiných států, kde ozbrojený konflikt neprobíhá, tudíž jakákoli omezení kybernetických operací založená na územním principu by byla velice obtížně dodržována.[142]

Otázka teritoriality vystupuje jako jeden z prvků definice vnitrostátního ozbrojeného konfliktu. Ten je v čl. 1 odst. 1 DP II totiž vyjádřen nejen jako konflikt mezi státem a ozbrojenými silami, či mezi ozbrojenými skupinami navzájem, ale také jako konflikt probíhající *„na území Vysoké smluvní strany“*. Společný článek 3 ŽÚ, který je minimálním humanitárním standardem pro vnitrostátní ozbrojené konflikty, jež nenaplňují kritéria pro aplikaci DP II, dokonce uvádí, že by se takový konflikt měl odehrávat *„na území některé z Vysokých smluvních stran“*. Autoři Tallinnského manuálu tak polemizují nad tím, jaká je důležitost teritoriálního určení vnitrostátního ozbrojeného konfliktu, a to nejen z pohledu kyberprostoru. Většina dochází k závěru, že pro vnitrostátní ozbrojený konflikt je nutné, aby se odehrával na území státu, jež je stranou Ženevských úmluv, tedy jakéhokoli státu, nikoli pouze toho, na jehož území operuje i protistrana.[143] Nabízí se otázka, zda je tato dedukce vhodná.

---

[140] TURNS, David. *Cyber war and the law of neutrality.* In: TSAGOURIAS, Nikolas a Russell BUCHAN. *Research handbook on international law and cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 2017. Research handbooks in international law. s. 381.

[141] *„Cyber operations are subject to geographical limitations imposed by the relevant provisions of international law applicable during an armed conflict.“* SCHMITT M. *Tallinn Manual 2.0. op. cit.* Pravidlo 81.

[142] Ibid. s. 378.

[143] Ibid. s. 386.

Obecně je možné říct, že se v kybernetickém prostoru mnohem více setkáváme s možností přeshraničních útoků nestátních skupin, jako jsou různé skupiny hackerů, ale i samostatní jedinci. Nestátní skupiny jsou tradičně spojeny s výrazně menšími možnostmi válčení na větší vzdálenost, kdy takové zbraně jsou v drtivé většině případů ve vlastnictví států. Nicméně kybernetický prostor v tomto otevírá nové možnosti, protože i nestátní aktéři dokáží provádět kybernetické útoky nezanedbatelného rozsahu. Je obecně známo, že mnohdy jsou mezi členy takových skupin lidé expertních znalostí v oblasti moderních technologií. Tímto vším se podstatně rozšiřuje dosah možných destruktivních následků ozbrojených konfliktů, které byly původně spjaty s mezistátními ozbrojenými konflikty. Vrátíme-li se tedy k výše uvedenému závěru autorů Tallinnského manuálu, musíme konstatovat, že taková situace bude kvalifikována jako vnitrostátní ozbrojený konflikt. To znamená aplikovatelnost pouhých 28 článků DP II či pouze jediného společného článku 3 ŽÚ. Možná by se nabízela otázka, zda taková míra škodlivosti již nezasahuje do sféry mezinárodního ozbrojeného konfliktu, neboť rozdíly mezi protistranami se v kybernetickém prostoru na rozdíl od konvenčního boje smazávají. Obě strany totiž v podstatě disponují stejnými prostředky k páchání kybernetických útoků (odhlédneme-li od finančních zdrojů, jež jsou bezpochyby v mnohem větší míře přítomny na straně státu) a vliv na mezinárodní vztahy je bezpochyby vysoce destruktivní.

Tradiční MHP již od svého počátku, resp. po celou dobu existence válečných aktivit, pracuje s teritoriální limitací ozbrojených konfliktů, s čímž do značné míry souvisí institut neutrality. Autoři Tallinnského manuálu se jednoznačně vyjádřili tak, že se právo neutrality na kybernetické operace aplikuje.[144] Účel neutrality, tedy ochrana států, jež si přejí zůstat neutrální, a jejich obyvatel před škodlivými dopady ozbrojených konfliktů, stejně jako ochrana bojujících států před tím, aby jeden z protivníků byl podporován dalším aktérem, musí být zachován také v případě vedení ozbrojeného konfliktu kybernetickými prostředky.[145] Jak z tradičního pojetí neutrality, tak z pravidel Tallinnského manuálu v části věnující se neutralitě[146] vyplývá, že základním předpokladem pro zachování neutrality je uplatňování územní teritoriality, resp. v kybernetickém prostoru uplatňování teritoriality nad kybernetickou infrastrukturou. Jak již bylo zmíněno výše, státy mají v kybernetickém prostoru dodržovat *due diligence*, tedy neumožnit jiným, aby užívali jejich kybernetickou

[144] Ibid. s. 553.
[145] Ibid. s. 553.
[146] Ibid. Pravidla 150 – 154.

infrastrukturu k páchání škodlivých kybernetických operací.[147] Toto pravidlo je vyjádřením dlouhodobě uznávaného principu, který byl stanoven již v rozhodnutí MSD ve věci Korfského průlivu (Corfu Channel), a sice že je *„povinností každého státu vědomě neumožnit užití svého území k jednáním, jež by směřovala proti právům jiných států“*.[148] Avšak ani v reálném světě založeného na hmatatelných skutečnostech nelze pouze z toho důvodu, že daný stát vykonává nad územím kontrolu, vyvozovat, že by stát věděl o nepřátelských skutcích páchaných vůči jinému státu z tohoto území, či že by snad znal totožnost pachatelů.[149] V prostředí kybernetického prostoru se možnost kontroly státu nad infrastrukturou umístěnou na jeho území ještě více zužuje, a je tedy nutné jakékoli závěry o porušení neutrality v kyberprostoru vynášet pouze po důkladném zvážení.[150]

Někteří autoři[151] poukazují na možnost analogického použití haagských pravidel ohledně kontroly bezdrátového telegrafování v dobách války a leteckého válčení z roku 1923, přestože netvoří právně závazný dokument. Do určité míry je třeba ocenit snahu navázat pravidla týkající se technologického pokroku doby před téměř sto lety na moderní technologie doby dnešní. Avšak až na pár očividných analogií (například že rádiové stanice můžeme v dnešní době připodobnit k domácím počítačům[152]) je dle názoru autorky velice obtížné haagská pravidla aplikovat v natolik specifickém prostředí, jako je kybernetický prostor. V čem ale můžeme spatřovat důležitou indicii, je fakt, že jakékoli nové technologie nezůstávají v právním vakuu, ale jsou podřazovány pod existující pravidla. Tedy je zde očividná snaha existující obecná pravidla uplatňovat i ve velmi specifických podmínkách.

Zajistit uplatňování neutrality je také vysoce žádoucí, neboť v dnešním propojeném světě lze kybernetickými operacemi jednoduše zasáhnout do veřejně i soukromě vlastněné kybernetické infrastruktury různých států.[153] Nicméně aby bylo možné neutralitu adekvátně aplikovat a vynucovat její dodržování, bylo by vhodné stanovit jiný limit, než je teritorialita, která je v kybernetickém prostoru velmi omezeně, jestli vůbec, aplikovatelná. Jako možná vhodnější alternativa se nabízí princip personality.[154] A to i přesto, že v kybernetickém prostoru naráží na své vlastní limity popsané výše. Teritoriální limitace bojových operací se v kybernetickém prostoru ztrácí, kyberprostor nabízí možnosti boje na vzdálenost a rozsah,

[147] Ibid. Pravidla 6 a 7.
[148] *„/.../ every State´s obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.“* ICJ. *The Corfu Channel Case. op. cit.* s. 22.
[149] Ibid. s. 18.
[150] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 554.
[151] Například TURNS D. *Cyber war and the law of neutrality. op. cit.* s. 386.
[152] TURNS D. *Cyber war and the law of neutrality. op. cit.* s. 397.
[153] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 554.
[154] TURNS D. *Cyber war and the law of neutrality. op. cit.* s. 398.

která je tradičními způsoby téměř nedosažitelná. To s sebou nese však i negativní důsledky pro strany, jež se konfliktu neúčastní, protože se, ať už úmyslně či nikoli, mohou stát taktéž obětí kybernetických útoků. Koncept teritoriality je tedy pro kybernetický prostor prakticky nepoužitelný.

4.3. Účast civilistů

Dalším problematickým aspektem kybernetického prostoru, jak již vyplynulo v předcházející kapitole, je přítomnost civilistů a obtížnost jejich odlišení od kombatantů. Navíc se civilisté v čím dál větší míře účastní kybernetických operací, ať už v kontextu ozbrojeného konfliktu nebo vyloženě kriminální činnosti[155] spojené s peněžitou odměnou. Konvenční způsob boje, nebo v širším hledisku celá struktura stojící za úspěšným vedením ozbrojeného konfliktu, je spojen s profesionální armádou a její striktní hierarchizací. S nástupem nestátních aktérů se toto začalo mírně proměňovat, třebaže i nadále bylo třeba prokazovat organizovanost ozbrojených skupin, aby bylo možné kvalifikovat situaci jako vnitrostátní ozbrojený konflikt, nikoli jen jako vnitřní nepokoje.[156]

Na kybernetických útocích mohou být, a ve velké míře také jsou, účastni jednotlivci či malé skupiny hackerů, které se navíc mohou formovat pouze online a komunikovat virtuálními prostředky, aniž by reálně došlo k jejich osobnímu kontaktu. Skupina expertů Tallinnského manuálu se vyjádřila i k této možnosti a konstatovala, že pouhý „nedostatek" v tom, že by se členové této skupiny nikdy neviděli tváří v tvář, neznamená, že by skupina nesplnila požadavky na dostatečnou organizaci, pokud další kritéria naplněna jsou.[157] Je však jen těžko představitelné, že by členové takové skupiny byli podrobeni nějakému efektivnímu systému disciplíny či respektu k MHP.[158] V takovém případě, kdybychom byli schopni takovou skupinu identifikovat, nebude možné za současné situace MHP aplikovat. Je důležité si uvědomit, že dopad aktivit hackerů může být dalekosáhlý a vysoce ničivý. A příčinou toho může být do určité míry samotná podstata kybernetického prostoru – virtualita. Útočníci jsou

[155] Pro tuto oblast je relevantní Rada Evropy. *Úmluva o počítačové kriminalitě.* 23. listopadu 2001. ETS No. 185. (tzv. Budapešťská úmluva)
[156] Srov. ICTY, *Prosecutor v. Ljube Boškoski a Johan Tarčulovski*, Case No. IT-04-82-T, Trial Chamber II. Trial Judgment. 10 July 2008. para 195 – 206.
[157] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 390.
[158] DROEGE C. *Get off my cloud: cyberwarfare, international humanitarian law, and the protection of civilians*. *op. cit.* s. 550.

skryti za počítačem a uniká jim skutečný kontext jejich aktivit.[159] Páchané kybernetické útoky tudíž mohou být jen těžko podrobovány stejně silnému morálnímu hodnocení jako útoky v tradičním způsobu válčení, neboť pro samotné útočníky zůstávají jejich aktivity pouhým programováním.[160]

Hackeři jsou osoby s velice dobrou znalostí kybernetického prostoru, a proto mohou být najímáni jak soukromými osobami, tak také do služeb států jako tzv. kybernetičtí žoldnéři.[161] Žoldnéř je definován v čl. 47 DP I, kde mezi jeho základní charakteristiky patří, že je najat k tomu, aby bojoval v ozbrojeném konfliktu a skutečně tak činí, tato jeho účast je motivována vidinou osobního zisku, který mu je skutečně přislíben a který podstatně převyšuje obvyklou odměnu kombatantů, není vyslán jiným státem k plnění oficiálních úkolů a není ani příslušníkem ozbrojených sil strany v konfliktu ani jejím občanem. Taková osoba nemá status kombatanta, a tudíž ani nárok na status válečného zajatce. To, že by si státy najímaly vysoce profesionální hackery z jiných států, není rozhodně nepředstavitelné. Obzvlášť pokud vezmeme do úvahy, jak jednoduše by taková spolupráce mohla fungovat – kybernetický žoldnéř by mohl provádět kybernetické útoky pro určitý stát sám, z místa dalece vzdáleného od bojiště (pokud by se samozřejmě ozbrojený konflikt neodehrával pouze kybernetickými prostředky).[162] V obecném MHP je pojem žoldnéř prakticky nepoužitelný, protože je definován striktními podmínkami, které musí být naplněny kumulativně.[163] V kybernetickém prostoru si však lze tuto aktivitu představit podstatně jednodušeji, navíc jsou hackeři často motivováni vidinou finanční odměny, tudíž bychom v tomto ohledu mohli očekávat nárůst kybernetických žoldnéřů.

Dalším zajímavým promítnutím zvýšené účasti civilistů, resp. skupin, které nedosahují takového stupně organizovanosti, aby bylo možno na ně aplikovat MHP, je existence konceptu války proti terorismu, který vznikl po teroristických útocích na Světové obchodní centrum z 11. září 2001.[164] Terorismus a asymetrie válčení podstatně proměnily chápání bojových akcí a též aplikaci MHP, jak již bylo podrobněji popsáno ve druhé kapitole. A celosvětový dosah teroristických útoků takový vývoj dále podpořil. Bez zabíhání do podrobností ohledně tohoto komplikovaného fenoménu lze dozajista tvrdit, že pokud by se koncept války proti teroru přesunul také do kybernetického prostoru, nebo pokud by státy

[159] BUSSOLATI, Nicolò. *The Rise of Non-State Actors in Cyberwarfare.* In: OHLIN, Jens David, Kevin GOVERN a Claire FINKELSTEIN. *Cyberwar: law and ethics for virtual conflicts*. Oxford: Oxford University Press, 2015. s. 115.
[160] Ibid. s. 115.
[161] Ibid. s. 108.
[162] SCHMITT M. *Tallinn Manual 2.0. op. cit.* s. 413.
[163] HENCKAERTS J. et al. *Customary international humanitarian law. op. cit.* s. 392.
[164] ONDŘEJ J. et al. *Mezinárodní humanitární právo. op. cit.* s. 57.

začaly hodnotit kybernetické útoky páchané proti nim jako teroristické útoky a reagovaly na ně v souladu s doktrínou války proti teroru, mohlo by potenciálně dojít k celosvětovému rozšíření škodlivých aktivit, ať už pozemních či kybernetických.

4.4. Ochranné možnosti MHP

Ozbrojený konflikt s sebou obecně přináší mnohé nepříjemnosti. V tradičním pojetí ozbrojeného konfliktu, což v kontextu této práce znamená konvenční boj bez užití kybernetických prostředků, jsou ozbrojenými konflikty postiženi jak civilisté, tak kombatanti, kteří čelí útokům na svůj život a zdraví. Tyto škodlivé následky jsou do určité míry eliminovány díky lékařské pomoci, mnohdy poskytované nestrannými humanitárními organizacemi, jako je MVČK či Lékaři bez hranic. Jejich činnost stejně jako jejich ochrana jsou určovány normami MHP. Nicméně byli jsme již svědky kybernetických útoků na tato zařízení – jmenujme alespoň ty nejznámější jako ransomware[165] WannaCry a wiper[166] NotPetya. Oba v roce 2017 ovlivnily činnost lékařských zařízení, a třebaže se bavíme o kybernetickou operaci podniknuté v době míru, nelze pominout potenciální hrozbu, která vyvstává pro případ takového útoku za probíhajícího ozbrojeného konfliktu. A nutno dodat, že takové útoky jsou na vzestupu.[167]

MVČK si je velmi dobře vědom možných důsledků, jež by pro nejen jejich lékařská zařízení mohly takové útoky mít. Proto byla i tato hrozba zahrnuta do obsahu zprávy ze setkání expertů pod záštitou MVČK z roku 2018, jež se zabývalo možnými lidskými oběťmi kybernetických operací.[168] Nemocniční zařízení jsou pro útočníky výhodnými cíli, protože jsou často vybavena pouze velice slabou kybernetickou ochranou a navíc pracují i z finančních důvodů se systémy, jejichž softwary nejsou aktualizovány a třeba ani již nejsou podporovány výrobcem.[169] S ohledem na specifičnost nemocničních zařízení a systémů se

[165] *„Program, který zašifruje data a nabízí jejich rozšifrování po zaplacení výkupného.“* JIRÁSEK P. et al. *Výkladový slovník kybernetické bezpečnosti. op. cit.* s. 97.
[166] Přestože se NotPetya původně jevila jako ransoware, jedná se o wiper, neboť zašifrovaná data nelze ani zaplacením výkupného obnovit, jsou trvale zničena. IVANOV, Anton a Orkhan MAMEDOV. *ExPetr/Petya/NotPetya is a Wiper, Not Ransomware.* AO Kaspersky Lab. Securelist. 28.6.2017. [cit. 26.11.2019] Dostupné z: https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/
[167] Dle zprávy společnosti MalwareBytes, která se specializuje na kybernetickou bezpečnost a především na vývoj programů pro ochranu počítačů před škodlivými programy (malware), je sektor zdravotnictví sedmým nejvíce napadaným odvětvím a počet kybernetických hrozeb vzrostl jen mezi druhým a třetím čtvrtletím roku 2019 o 45 procent. Viz. MalwareBytes. *Cybercrime Tactics and Techniques: the 2019 state of healthcare*. *CTNT Report* [online]. November 2019. s. 4.
[168] ICRC. *The Potential Human Cost of Cyber Operations. ICRC Expert Meeting, 14 – 16 November 2018, Geneva.* Editor Laurent GISEL, Lukasz OLEJNIK. ICRC, May 2019. s. 3 a 6.
[169] Ibid. s. 61.

ukazuje, že i sekundární následky takového útoku, čímž máme na mysli znovuobnovení činnosti zařízení a systémů, by byly značného rozsahu, a to z toho důvodu, že v případě napadení více nemocnic či jiných lékařských zařízení by dodavatelům těchto specifických systémů trvalo podstatně delší dobu škodlivé následky napravit.[170] Podíváme-li se na dopady útoku ransomware WannaCry, zjistíme, že postihl jen ve Velké Británii asi třetinu nemocničních zařízení spadajících pod National Health Systém a náklady na odstranění dopadů tohoto útoku se vyšplhaly na přibližně 92 milionů liber.[171] Nemocnice byly vybaveny zastaralým systémem Windows XP, kvůli čemuž bylo možno jejich počítače v tak velké míře napadnout.[172] Co je však důležité z hlediska plnění základních úkolů lékařských zařízení, útokem WannaCry bylo přibližně 19 tisícům pacientů zrušen termín lékařské prohlídky, z čehož dle dostupných informací celkem 139 pacientů vyžadovalo okamžitou péči.[173]

Ačkoli se v těchto případech jednalo pouze o ztrátu určitých dat, třebaže důležitých, není následek útoku WannaCry natolik destruktivní. Nejsou to však jen počítače, které mohou být v lékařském zařízení napadeny z důvodu jejich napojení na počítačové systémy, ale i samotné lékařské přístroje sloužící k vyšetřování pacientů či operování, jako například rentgenový přístroj.[174] Z technického hlediska se zdá být možné, aby k takovému kybernetickému útoku úspěšně došlo. Jako příklad uveďme zařízení, jež pacientovi dávkuje a přímo aplikuje léky. Toto zařízení může být napadeno tak, že se změní dávkování či je podáván jiný lék, což by mohlo být pro pacienta v krajním případě smrtelné.[175] Za ozbrojeného konfliktu jsou nemocniční zařízení a transporty pod ochranou MHP, čemuž přisvědčuje i Tallinnský manuál, který jejich ochranu před kybernetickými operacemi taktéž upravuje.[176] Pozornost si zaslouží především pravidlo 132, ve kterém je tato tradiční ochrana rozšířena o *„počítače, počítačová data a data, která tvoří základní součást funkce a administrace zdravotnických jednotek a ransportů a které musí být respektovány a chráněny a především nesmějí být předmětem útoku“*.[177] Typicky by se mohlo jednat o data pacientů či rozvrhy naplánovaných operací.[178]

---

[170] Ibid. s. 21.
[171] FIELD, Matthew. *WannaCry cyber attack cost the NHS £92 as 19,000 appointments were cancelled.* The Telegraph. 11.10.2018. [cit. 26.11.2019]. Dostupné z: https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/
[172] Ibid.
[173] National Audit Office. Department of Health. *Investigation: WannaCry cyber attack and the NHS. Report by the Controller and Auditor General.* 24.10.2017. s. 14.
[174] ICRC. *The Potential Human Cost of Cyber Operations. op. cit.* s. 60.
[175] Ibid. s. 61.
[176] SCHMITT M. *Tallinn Manual 2.0. op. cit.* Pravidla 131 – 134.
[177] *„Computers, computer networks, and data that form an integral part of the operations or administration of medical units and transports must be respected and protected, and in particular may not be made the object of attack.“* SCHMITT M. *Tallinn Manual 2.0. op. cit.* Pravidlo 132.

Ustanovení Tallinnského manuálu reflektuje důležitost taková data lékařských zařízení chránit před kybernetickými útoky nepřítele, neboť jejich ztráta či zveřejnění protivníkem by mohly mít ve svém důsledku pro pacienta fatální následky. A taktéž reflektuje očividnou tendenci útočníků vybírat si za cíl slabě chráněná zdravotnická zařízení.

Problematičnost tohoto aspektu MHP v kybernetickém prostoru nespočívá v tak velké míře na nemožnosti či neochotě stran ozbrojeného konfliktu respektovat a chránit lékařská zařízení, třebaže jak již bylo uvedeno ve třetí kapitole, i nemocniční zařízení se mohou stát obětí nerozlišovacích útoků, či se projeví faktická nemožnost rozlišení nemocničních dat od dat vojenských. Jako problematická a potenciálně škodlivá se v tomto případě jeví skutečnost, že k útokům na nemocniční zařízení již v nedávné minulosti došlo, tyto útoky byly do určité míry úspěšné a bohužel je nutné konstatovat, že sofistikovanější útoky by za ozbrojeného konfliktu mohly skutečně vést ke ztrátám na životech jak kombatantů, tak civilistů.

[178] ICRC. *The Potential Human Cost of Cyber Operations. op. cit.* s. 60.

Závěr

Cílem této diplomové práce s názvem *Aplikace mezinárodního humanitárního práva na kybernetické vedení boje* bylo představit stále ještě relativně nový, přesto široce rozšířený fenomén využívání kybernetického prostoru jako domény pro vedení válečných aktivit mezi nepřáteli, čímž nemáme na mysli pouze státy, ale v čím dál větší míře také nestátní aktéry, ať už jednotlivce či malé nepříliš organizované skupiny. A dále tento fenomén podrobit kritickému zkoumání se snahou nalézt odpověď na výzkumnou otázku, kterou si autorka položila v úvodu této diplomové práce: *Zda je možné na válečné aktivity prováděné prostředky moderních technologií aplikovat existující mezinárodní humanitární právo, a pokud ano, pak do jaké míry.*

Pravidla regulující vedení ozbrojených konfliktů provázejí lidstvo od prvopočátku, neboť války jsou stejně staré jako lidstvo samo. Vezmeme-li do úvahy pouze moderní vývoj mezinárodního humanitárního práva spojeného se jménem Henryho Dunanta a vznikem Mezinárodního výboru Červeného kříže, můžeme konstatovat, že celé toto odvětví bylo nuceno reagovat na mnohé výzvy spojené mimo jiné z velké části také s technologickým vývojem. Kybernetické vedení boje tak není ničím jiným než dalším stupněm vývoje tohoto odvětví mezinárodního práva. Přináší však s sebou velkou řadu nových a do té doby obtížně představitelných elementů. Záměrem autorky bylo představit v této diplomové práci možnosti aplikace mezinárodního humanitárního práva v kybernetickém prostoru, a to z také z toho důvodu, že neexistuje všeobecné a závazné vyjádření ohledně takové aplikovatelnosti. Obecně v mezinárodním společenství převažuje názor, že se v kybernetickém prostoru aplikuje mezinárodní humanitární právo stejně jako v případě konvenčního způsobu vedení ozbrojeného konfliktu. Zásadní obtíže spojené s uvedením této teze do praxe byly v této diplomové práci popsány.

V první řadě byla zkoumána aplikovatelnost základních principů mezinárodního humanitárního práva na vedení ozbrojeného konfliktu prostřednictvím kybernetických operací. Z tohoto rozboru vyplynulo, že zásada vojenské nutnosti, kterou můžeme označit za prvopočátek militarizace kybernetického prostoru, a zásada humanity, jež je pro odvětví mezinárodního humanitárního práva typická, jsou na kybernetický způsob boje bez obtíží aplikovatelné. Zásada rozlišování, jejímž účelem je chránit civilní obyvatelstvo a civilní objekty před dopady ozbrojených konfliktů, se ukázala být jako velice obtížně aplikovatelná. Hlavními důvody tohoto nesouladu byly především reálná možnost toho, že i cílený kybernetický útok by se po vypuštění do kybernetického prostoru mohlo chovat

nerozlišujícím způsobem, a také skutečnost, že drtivá většina kybernetické infrastruktury je tzv. dvojího užití, tedy jsou tato zařízení využívána jak pro civilní účely, tak pro účely vojenské. Z tohoto důvodu je v souladu se současným mezinárodním humanitárním právem třeba konstatovat, že taková zařízení nemohou být chráněna jako civilní, ale stávají se legitimním cílem útoku. Zásada přiměřenosti se tak jeví jako vhodný instrument k eliminování nedostatků, které v kybernetickém prostoru prokazuje princip rozlišování. Za současného stavu technologického vývoje se zásada zákazu zbytečných útrap ukázala být nejméně aplikovatelnou, třebaže není nemožné si představit příklady důsledků kybernetických útoků, jež by tuto zásadu porušovaly.

Dále byly rozboru z hlediska aplikovatelnosti mezinárodního humanitárního práva podrobeny vybrané problematické aspekty, které byly autorkou identifikovány v rámci zkoumání aplikovatelnosti základních zásad mezinárodního humanitárního práva. Z důvodu rozsahu této diplomové práce byly vybrány a stručně popsány pouze zásadní problematické aspekty, a to autorství kybernetické operace, teritoriální limitace kybernetických operací, účast civilistů na kybernetickém vedení boje a problematičnost adekvátní aplikace ochranných možností mezinárodního humanitárního práva v kybernetickém prostoru. Určení původce útoku a vymezení teritoria jsou instituty, jež v kybernetickém prostoru do velké míry selhávají. Zvýšená účast civilistů na bojových operacích je fenomén známý i z tradičního způsobu vedení ozbrojeného konfliktu, nicméně problémy s tímto související získávají v kybernetickém prostoru nových obrysů. Problematičnost aplikace ochranných možností mezinárodního humanitárního práva v kybernetickém prostoru spočívá pro účely této diplomové práce v tom, že nemocniční zařízení, jež jsou předmětem této ochrany, jsou cílem nikoli zanedbatelného počtu a rozsahu kybernetických operací. A tyto operace by skutečně mohly mít svědomí ztráty lidských životů. Závěrem lze říci, že mezinárodní humanitární právo se v kybernetickém prostoru aplikuje, nicméně pro jeho adekvátní užití je třeba, aby došlo v určitých ohledech, které jsou naznačená ve čtvrté kapitole této práce, k zaplnění „mezer“, ať už interpretací či vznikem norem nových.

Protože je kybernetický prostor velice specifickou oblastí, bylo cílem autorky uvádět praktické příklady pro jednodušší a názornější představu tvrzených skutečností. Často byly užívány příklady proběhnuvších kybernetických operací, aby bylo dostatečně demonstrováno, že kybernetické operace a vůbec využívání kybernetického prostoru pro válečné aktivity je realitou dnešního světa.

Je přáním autorky, aby tato diplomová práce přispěla alespoň v prostředí České republiky k rozpoutání debaty o možnostech a limitacích aplikace nejen mezinárodního humanitárního práva, ale obecně celého odvětví mezinárodního práva v kybernetickém prostoru.

Seznam zkratek

Zkratka	**Český význam /*význam v původním jazyce***
CCD COE	*Cooperative Cyber Defence Centre of Excellence*
DP I	Dodatkový protokol k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí mezinárodních ozbrojených konfliktů
DP II	Dodatkový protokol k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí ozbrojených konfliktů nemajících mezinárodní charakter
DDoS	Rozdělené odepření služby / *Distributed Denial of Service*
ICTY	Mezinárodní trestní tribunál pro bývalou Jugoslávii / *International Criminal Tribunal for the Former Yugoslavia*
MHP	Mezinárodní humanitární právo
MSD	Mezinárodní soudní dvůr / *International Court of Justice*
MTS	Mezinárodní trestní soud / *International Criminal Court*
MVČK / *ICRC*	Mezinárodní výbor Červeného kříže / *International Committee of the Red Cross*
NATO	Severoatlantická aliance / *North Atlantic Organization*
OSN	Organizace spojených národů
ŽÚ I	Ženevská úmluva o zlepšení osudu raněných a nemocných příslušníků ozbrojených sil v poli ze dne 12. srpna 1949
ŽÚ II	Ženevská úmluva o zlepšení osudu raněných, nemocných a trosečníků ozbrojených sil na moři ze dne 12. srpna 1949
ŽÚ III	Ženevská úmluva o zacházení s válečnými zajatci ze dne 12. srpna 1949
ŽÚ IV	Ženevská úmluva o ochraně civilních osob za války ze dne 12. srpna 1949

Seznam použitých zdrojů

1. Mezinárodní smlouvy

1.1. Jednotlivé mezinárodní smlouvy

- *Charta Organizace spojených národů a Statut Mezinárodního soudního dvora.* 26. června 1945. Dostupné z: https://www.osn.cz/wp-content/uploads/2015/03/charta-organizace-spojenych-narodu-a-statut-mezinarodniho-soudniho-dvora.pdf
- *Ženevské úmluvy o ochraně obětí ozbrojených konfliktů z 12. srpna 1949 a Dodatkové protokoly z 8. června 1977.* Dostupné z: https://www.cervenykriz.eu/cz/mhp_knihovna/zenevske_umluvy.pdf
- Rada Evropy. *Úmluva o počítačové kriminalitě.* 23. listopadu 2001. ETS No. 185. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
- *Deklarace o zákazu užívání střel, které se lehce v lidském těle rozšiřují nebo zplošťují.* 29. července 1899. Dostupné z: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=F5FF4D9CA7E41925C12563CD0051616B

1.2. Soubory mezinárodních smluv

- ONDŘEJ, Jan a Miroslav POTOČNÝ. *Obecné mezinárodní právo v dokumentech.* 3., dopl. vyd. Praha: C.H. Beck, 2010. 341 s. ISBN 978-80-7400-330-1.

2. Historické dokumenty

- *Instructions for the Government of Armies of the United States in the Field* (Lieberův kodex). 24. dubna 1863. Dostupné z: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=A25AA5871A04919BC12563CD002D65C5&action=openDocument

3. Rozhodnutí soudních orgánů

3.1. Rozhodnutí Mezinárodního soudního dvora

- ICJ. *Legality of the Threat or Use of Nuclear Weapons.* Advisory Opinion. 8 July 1996. ICJ Reports 1996. Dostupné z: https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

- ICJ. *The Corfu Channel Case*. Judgment. 9 April 1949. ICJ Reports 1949. Dostupné z: https://www.icj-cij.org/files/case-related/1/001-19490409-JUD-01-00-EN.pdf

3.2. Rozhodnutí Mezinárodního trestního tribunálu pro bývalou Jugoslávii

- ICTY, *Prosecutor v. Duško Tadić*. Case No. IT-94-1-A, Appeals Chamber, Appeal, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995. Dostupné z: http://www.icty.org/x/cases/tadic/acdec/en/51002.htm
- ICTY, *Prosecutor v. Pavle Strugar*. Case No. IT-01-42-T, Trial Chamber II. Trial Judgment. 31 January 2005. Dostupné z: https://www.icty.org/x/cases/strugar/tjug/en/str-tj050131e.pdf
- ICTY, *Prosecutor v. Ljube Boškoski a Johan Tarčulovski*. Case No. IT-04-82-T, Trial Chamber II. Trial Judgment. 10 July 2008. Dostupné z: https://www.icty.org/x/cases/boskoski_tarculovski/tjug/en/080710.pdf

4. Dokumenty mezinárodních organizací

4.1. Dokumenty Organizace spojených národů

- UN Doc. A/RES/70/237 *Developments in the field of information and telecommunications in the context of international security*. 30 December 2015. Dostupné z: https://undocs.org/A/RES/70/237
- UN Doc. A/70/174 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. 22 July 2015. Dostupné z: https://undocs.org/A/70/174

4.2. Dokumenty Severoatlantické aliance

- *Warsaw Summit Communiqué*. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July, 2016. [online] [cit. 28.10.2019] Dostupné z: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

4.3. Dokumenty Mezinárodního výboru Červeného kříže

- HENCKAERTS, Jean-Marie, Louise DOSWALD-BECK a Carolin ALVERMANN. *Customary international humanitarian law*. New York: Cambridge University Press, 2005. 621 s. ISBN 05-218-0899-5.

- ICRC. *How is the Term „Armed Conflict" Defined in International Humanitarian Law?* [online] Opinion Paper. March 2008. 5 s. [cit. 26.11.2018] Dostupné z: https://www.icrc.org/en/doc/assets/files/other/opinion-paper-armed-conflict.pdf
- ICRC. *Interpretative Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*. Geneva: International Committee of the Red Cross, 2009. 85 s. ISBN 9782940396047.
- ICRC. *Mezinárodní humanitární právo: odpovědi na vaše otázky.* [online] Editor Veronika BÍLKOVÁ, Marek JUKL. Praha: Český červený kříž, 2009. 42 s. [cit. 26.11.2018] Dostupné z: https://www.cervenykriz.eu/cz/edicehnuti/MHP_odpovedi_na_vase_otazky.pdf
- ICRC. *The Potential Human Cost of Cyber Operations. ICRC Expert Meeting, 14 – 16 November 2018, Geneva.* [online] Editor Laurent GISEL, Lukasz OLEJNIK. ICRC, May 2019. 77 s. [cit. 26.11.2019] Dostupné z: https://www.icrc.org/en/document/potential-human-cost-cyber-operations
- SASSÒLI, Marco, Antoine A. BOUVIER a Anne QUINTIN. *How does law protect in war?: cases, documents, and teaching materials on contemporary practice in international humanitarian law* [online]. Third, expanded and updated edition. Geneva: International Committee of the Red Cross, 2011 [cit. 17.11.2019]. Military legal resources. ISBN 978-294-0396-122. Dostupné z: https://casebook.icrc.org/

5. Knižní publikace

5.1. Monografie

- ABBOTT, Daniel H. *The Handbook of Fifth-Generation Warfare (5GW).* Nimble Books LLC, 2010. 274 s. ISBN 9781934840177.
- FLECK, Dieter. *The Handbook of International Humanitarian Law.* Third edition. Oxford: Oxford University Press, 2013. 714 s. ISBN 978-0-19-872928-0.
- HARRISON DINNISS, Heather. *Cyber warfare and the laws of war*. [online] New York: Cambridge University Press, 2012. ISBN 978-1-107-01108-3.
- HAYASHI, Nobuo. *Military Necessity: The Art, Morality and Law of War*. Cambridge: Cambridge University Press, 2020. Kniha bude publikována na jaře 2020.
- KOLB, Robert. *Advanced Introduction to International Humanitarian Law*. Cheltenham, UK: Edward Elgar, 2014. Elgar Advanced Introductions. 216 s. ISBN 978-1-78347-753-1.

- KOLOUCH, Jan, Pavel BAŠTA, Andrea KROPÁČKOVÁ a Martin KUNC. *CyberSecurity*. 1. vyd. Praha: CZ.NIC, 2019. 556 s. ISBN 978-80-88168-31-7.
- ONDŘEJ, Jan, Pavel ŠTURMA, Veronika BÍLKOVÁ a Dalibor JÍLEK. *Mezinárodní humanitární právo.* 1. vydání. Praha: C.H. Beck, 2010. 559 s. ISBN 978-80-7400-185-7.
- SCHMITT, Michael N. a Liis VIHUL. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. [online] General editor Michael N. Schmitt; Managing editor Liis Vihul. Second edition. New York, NY, USA: Cambridge University Press, 2017. [cit. 30.1.2019] ISBN 9781107177222.
- TIKK, Eneken, Kadri KASKA a Liis VIHUL. *International Cyber Incidents: Legal Considerations.* [online] Tallinn: Cooperative Cyber Defence Cente of Excellence (CCD COE), 2010. s. 130. ISBN 978-9949-9040-0-6. Dostupné z: https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf

5.2. Dílčí kapitoly knižních publikací

- ANTONOPOULOS, Constantine. *State responsibility in cyberspace*. In: TSAGOURIAS, Nikolas a Russell BUCHAN. *Research handbook on international law and cyberspace.* Cheltenham, UK: Edward Elgar Publishing, 2017. Research handbooks in international law. s. 55 – 71. ISBN 978-1-78254-738-9.
- BANNELIER-CHRISTAKIS, Karine. *Is the principle of distinction still relevant in cyberwarfare?* In: TSAGOURIAS, Nikolas a Russell BUCHAN. *Research handbook on international law and cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 2017. Research handbooks in international law. s. 343 – 365. ISBN 978-1-78254-738-9.
- BRUNER, Tomáš. *K podmínkám způsobu aplikace mezinárodního humanitárního práva na kybernetické operace*. In: *Mezinárodní humanitární právo: vznik, vývoj a nové výzvy*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2015. s.159 – 171. ISBN 978-80-87975-35-0.
- BUSSOLATI, Nicolò. *The Rise of Non-State Actors in Cyberwarfare*. In: OHLIN, Jens David, Kevin GOVERN a Claire FINKELSTEIN. *Cyberwar: law and ethics for virtual conflicts.* Oxford: Oxford University Press, 2015. s. 102 – 126. ISBN 978-0-19-871749-2.

- FOLTÝN, Otakar. *Vojenské aspekty vývoje mezinárodního humanitárního práva na pozadí 4 generací moderních ozbrojených konfliktů*. In: *Mezinárodní humanitární právo: vznik, vývoj a nové výzvy*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2015. s. 27 – 33. ISBN 978-80-87975-35-0.
- GILL, Terry D. *International humanitarian law applied in cyber-warfare: Precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict.* In: TSAGOURIAS, Nikolas a Russell BUCHAN. *Research handbook on international law and cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 2017. Research handbooks in international law. s. 55 – 71. ISBN 978-1-78254-738-9.
- ROSCINI, Marco. *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations*. In: OHLIN, Jens David, Kevin GOVERN a Claire FINKELSTEIN. *Cyberwar: law and ethics for virtual conflicts*. Oxford: Oxford University Press, 2015. s. 215 – 248. ISBN 978-0-19-871749-2.
- TURNS, David. *Cyber war and the law of neutrality*. In: TSAGOURIAS, Nikolas a Russell BUCHAN. *Research handbook on international law and cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 2017. Research handbooks in international law. s. 380 - 401. ISBN 978-1-78254-738-9.

5.3. Slovníky

- JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online] 3. aktualiz. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2015. s. 240. [cit. 28.10.2019] Dostupné z: https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf

6. Články v odborných časopisech

- BASTL, Martin a Zuzana GRUBEROVÁ. *Kyberprostor jako „pátá doména"?* [online] Vojenské rozhledy 4/2013. s. 10 – 21. [cit. 28.10.2019] Dostupné z: http://www.vojenskerozhledy.cz/images/archiv_voj_rozhl/cele_cisla/rozhledy2013-4.pdf
- DROEGE, Cordula. *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians*. [online] International Review of the Red Cross. Vol. 94. Number 886. 2012. s. 533 – 578. [cit. 26.11.2019] Dostupné z:

https://www.cambridge.org/core/product/identifier/S1816383113000246/type/journal_article

- HAMMES, Thomas X. *Fourth Generation Warfare Evolves, Fifth Emerges.* [online] Military Review, May/June 2007. s. 14 – 23. [cit. 26.11.2018] Dostupné z: https://www.armyupress.army.mil/Journals/Military-Review/
- LIND, William S. *Understanding Fourth Generation of War.* [online] Military Review, September/October 2004. s. 12 – 16. [cit. 26.11.2018] Dostupné z: https://www.armyupress.army.mil/Journals/Military-Review/

7. Kvalifikační práce

- BÍLKOVÁ, Veronika. *Úprava vnitrostátních ozbrojených konfliktů v mezinárodním humanitárním právu.* [online] 2006. Dostupné z: Doktorská disertační práce. Karlova univerzita, Právnická fakulta. Publikováno též knižně: Praha: Eva Rozkotová –IFEC, 2007. 333 s. ISBN 80-85889-82
- KNOPOVÁ, Eva. *New IHL Framework for Cyber Warfare* [online]. 2016. Diplomová práce. Karlova univerzita, Právnická fakulta. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/164693

8. Internetové zdroje

8.1. Články publikované na internetu

- BEAUMONT, Peter a Nick HOPKINS. *US was 'key player in cyber-attacks on Iran's nuclear programme'.* [online] The Guardian. 1.6.2012. [cit. 18.11.2019] Dostupné z: https://www.theguardian.com/world/2012/jun/01/obama-sped-up-cyberattack-iran
- FIELD, Matthew. *WannaCry cyber attack cost the NHS £92 as 19,000 appointments were cancelled.* [online] The Telegraph. 11.10.2018. [cit. 26.11.2019]. Dostupné z: https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/
- IVANOV, Anton a Orkhan MAMEDOV. *ExPetr/Petya/NotPetya is a Wiper, Not Ransomware.* [online] AO Kaspersky Lab. Securelist. 28.6.2017. [cit. 26.11.2019] Dostupné z: https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

- LIND, William S. *On War. Fifth Generation Warfare?* [online] 4.2.2004. [cit. 26.11.2018] Dostupné z: https://www.lewrockwell.com/2004/02/william-s-lind/fifth-generation-warfare/
- TRAYNOR, I. *Russia accused of unleashing cyberwar to disable Estonia.* [online] The Guardian. 17.5.2007. [cit. 28.10.2019]. Dostupné z: https://www.theguardian.com/world/2007/may/17/topstories3.russia

8.2. Dokumenty publikované na internetu

- National Audit Office. Department of Health. Investigation: WannaCry cyber attack and the NHS. *Report by the Controller and Auditor General.* [online] 24.10.2017. 31 s. ISBN 978-1-78604-147-0. [cit. 29.11.2019] Dostupné z: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf
- MalwareBytes. *Cybercrime Tactics and Techniques: the 2019 state of healthcare*. CTNT Report [online]. November 2019. 36 s. [cit. 29.11.2019]. Dostupné z: https://resources.malwarebytes.com/files/2019/11/191028-MWB-CTNT_2019_Healthcare_FINAL.pdf

8.3. Nejčastěji využívané internetové stránky

- Databáze smluv ICRC: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/
- How Does Law Protect In War: https://casebook.icrc.org/
- Mezinárodní trestní tribunál pro bývalou Jugoslávii: https://icty.org/

Abstrakt

Aplikace mezinárodního práva na kybernetické vedení boje

Předmětem zájmu této diplomové práce s názvem *Aplikace mezinárodního humanitárního práva na kybernetické vedení boje* je kritické posouzení možností aplikovatelnosti současných norem mezinárodního humanitárního práva v kybernetickém prostoru. Válečné aktivity v kybernetickém prostoru jsou bohužel realitou dnešní doby, tudíž je více než žádoucí podrobit tezi o aplikovatelnosti mezinárodního humanitárního práva, kterou zastává většina mezinárodního společenství, reálnému rozboru. Výzkumnou otázkou tedy není pouze, zda je mezinárodní humanitární právo aplikovatelné na kybernetické vedení boje, ale také do jaké míry.

Diplomová práce se kromě úvodu a závěru skládá ze čtyř kapitol. První kapitola se věnuje základní charakteristice mezinárodního humanitárního práva a stručnému vývoji, se zaměřením na vývoj válečnictví jako předpokladu pro militarizace kybernetického prostoru. Následující kapitola definuje pojmy spojené s kybernetickým prostorem, aby byly dále v souladu s těmito definicemi používány. Stěžejní část diplomové práce tvoří rozbor aplikovatelnosti základních principů mezinárodního humanitárního práva na kybernetické vedení boje a upozornění na vybrané problematické aspekty přenosu existujících norem mezinárodního humanitárního práva do kybernetického prostoru. Základními zásadami, jež jsou aplikovány na kybernetické operace, jsou zásada vojenské nutnosti, humanity, rozlišování, přiměřenosti a zákazu zbytečných útrap. Ukázalo se, že zásady rozlišování a zákazu zbytečných útrap jsou do kybernetického prostoru za současného stavu technologií jen těžko přenositelné. Poslední kapitola se zaměřuje na vybrané problematické okruhy aplikovatelnosti mezinárodního humanitárního práva, a to určení autorství kybernetické operace, teritoriální limitace těchto operací, zvýšení účasti civilistů a jejich podílu na kybernetických operacích a v neposlední řadě možné zmenšení ochranných možností mezinárodního humanitárního práva v kybernetickém prostoru, především ve vztahu k nemocničním zařízením.

Jako příklady jsou užívány proběhnuvší kybernetické operace, jako například DDoS útok na Estonsko v roce 2007, kybernetická operace vůči Gruzii z roku 2008 či útok ransomware WannaCry v roce 2017. Přestože dosud nebylo mezinárodní humanitární právo na kybernetické operace aplikováno, je nepochybné, že takové aktivity jsou realitou dnešního světa.

Abstract

Application of international humanitarian law on cyber military engagement

The subject of interest of this master thesis with the name *Application of international humanitarian law on cyber military engagement* is a critical assessment of possible applicability of the contemporary norms of international humanitarian law in cyber space. War-like activities in cyber space are unfortunately nowadays reality, therefore it is more than desirable to subject this thesis about the applicability of the international humanitarian law, which is hold by the majority of the international community, to the real analysis. The research question is not only whether international humanitarian law is applicable on cyber military engagement but also into what extent.

The master thesis consists, except for introduction and conclusion, of four chapters. The first chapter is focused on fundamental characterization of international humanitarian law and brief development with a special focus on the development of warfare as a prerequisite to the militarization of cyber space. The following chapter defines concepts connected with cyber space in order to be further used in accordance with those definitions. The main part of this master thesis is the analysis of the applicability of the fundamental principles of international humanitarian law on cyber military engagement and the notice concerning selected problematic aspects of the transfer of existing norms of international humanitarian law into cyber space. The fundamental principles, which are applied on cyber operations, are the principle of necessity, humanity, distinction, proportionality and prohibition of unnecessary suffering. It appeared that principles of distinction and prohibition of unnecessary suffering are in today´s state of technologies translated into cyber space with great difficulties. The last chapter focuses on selected problematic issues of applicability of international humanitarian law which is the vocation of authorship of cyber operation, territorial limitation of these operations, increased participation of civilians and its contribution to cyber operations and last but not least the possible decrease of protective possibilities of international humanitarian law in cyber space especially in relation to health-care providers.

Past cyber operations serve as examples, such as DDoS attack against Estonia in 2007, cyber operation against Georgia in 2008 or attack of ransomware WannaCry in 2017. Although international humanitarian law was not as of now applied in practice on cyber operations it is without doubts that such activities are the reality of today´s world.

Klíčová slova

mezinárodní humanitární právo
kybernetické vedení boje
kybernetická operace

Key words

international humanitarian law
cyber military engagement
cyber operation