

Budoucnost nekonvenčních forem boje

Autor: Martin Bastl
Email: bastl@fss.muni.cz

This text is a research about the character of cyberwarfare and potential connection between cyberwarfare and the terrorism. Both forms of warfare have similarly attributes. Cyber attack can be violation of international law of war as well as terrorist action.

V posledních letech a v souvislosti s proměnou a částečnou transformací vojenství, založenou zejména na masivním nasazování informačních a komunikačních technologií, se vede debata i o chápání tzv. nových forem vedení boje. Zdá se, že valná část této diskuse vychází z předpokladu, že jde o zcela a snad i kvalitativně novou formu vedení boje, která má unikátní charakteristiky a vyžaduje zcela nový přístup. Někteří s diskutujících otevřeně připouštějí, že pravidla pro vedení těchto nových forem boje bude třeba teprve najít.

Tento text má upozornit na paralely mezi formami vedení boje s velmi dlouho tradicí a těmito takzvanými novými formami. Vychází z předpokladu, že se sice posunulo těžiště v oblasti technik a taktiky a větší roli než v minulosti hrají taktiky označované jako nekonvenční, nejde však o žádný zásadní a kvalitativní posun. Jde o přirozenou evoluci, podmíněnou hledáním neefektivnějšího způsobu poškození či porážky protivníka. Spolu s tím však, jak roste význam, dopad a frekvence užívání nekonvenčních forem boje, roste i tlak na modifikaci vojenské doktríny a následně či v souvislosti s tím i pravidel vedení války. Jako ilustraci pro toto srovnání byl zvolen kybernetický boj jako relativně nová forma vedení boje a terorismus jako případ formy psychologické války, která má naopak tradici velmi dlouhou. Význam obou dvou těchto forem vedení boje v posledních letech výrazně stoupá, zejména proto, že jsou efektivními způsoby válčení proti technologicky vyspělým protivníkům s masivní vojenskou převahou, jimž nelze čelit konvenčně. Konvenčnost, potažmo konvence, jsou při jejich opisu klíčovými termíny. Konvence nejsou nic, než přijaté a všeobecně (či dostatečně významným počtu případů) uznávané normy upravující způsob vedení boje. Konvence, které platí po určité období, nejsou a nemohou být nadčasové. Nadto - konvence, které jsou přijímány nejsilnějšími aktéry, což v případě konvencí upravujících pravidla pro vedení války bezpochyby platí, mohou být vynucovány, stěží však budou akceptovány a chápány jako legitimní slabšími aktéry, jimž nevyhovují. Ba dokonce - v případě změny situace - mohou být konvence

odvrhnuty i aktéry silnými, kterým náhle znemožní rozvinutí, posílení či multiplikaci vojenského potenciálu. Může se ovšem objevit politická (mocenská) poptávka a tlak na legalizaci takových nekonvenčních forem vedení boje, které posílí vojenské schopnosti silných aktérů, na druhou stranu formy boje, které by profit silným aktérům nepřinášely, mohou být udržovány mimo konvence či v ilegalitě. To může být i případ kybernetického boje na jedné straně a terorismu na straně druhé. Do jaké míry mají tyto formy boje shodné rysy bude nastíněno v následujícím textu. Zároveň bude naznačen možný budoucí vývoj v oblasti rozšíření, vnímání a posuzování těchto forem vedení boje. Vojenství a vedení války bylo dlouho určitým způsobem omezováno, zahájení a vedení boje jako organizovaného násilí bylo svázáno s určitými normami. Klíčové byly úpravy toho, za jakých podmínek, kvůli čemu lze vést válku, tedy důvod k vedení války, a – zejména – jakým způsobem má boj probíhat (Roberts 2007: 328-351). Současná pravidla pro rozlišování války, chápané jako legální vedení boje, a zločinu včetně zločinů válečných, tedy nelegálních forem a metod vedení boje, je do značné míry výsledkem vývoje následujícího po uzavření Vestfálského míru v říjnu 1648.

Nejvýraznějšími momenty kodifikace pravidel bylo zřejmě přijetí Haagských a Ženevských úmluv a vypracování a ustavení mezinárodního válečného a humanitárního práva. Snaha kodifikovat pravidla vedení boje se ovšem po celou dobu střetávala s mezními případy, rozdílnými zájmy významných aktérů (mezinárodního práva), rozdílnými kulturními přístupy k vedení boje a v neposlední řadě s technologickým vývojem, který samozřejmě ovlivňoval i oblast vojenství¹. Po změnách, které s sebou do vojenství přinesly zbraně hromadného ničení a jmenovitě zbraně nukleární, se vývoj koncem minulého století začal ubírat jiným směrem. Technologické změny, tedy zejména rychlý rozvoj a stále širší uplatnění informačních a komunikačních technologií, které umožnily krom jiného tzv. Revoluci ve vojenství (RMA), výrazně posílily schopnost bohatých a technologicky vyspělých států vést válku. Jejich protivníci, chudší a technologicky méně vyspělé státy, povstalci, nestátní a nadstátní uskupení a sítě fakticky nemohou v konvenčně vedené válce proti silným aktérům zvítězit. To sice na jedné straně bylo cílem a důvodem probíhající transformace např. americké armády, na druhou stranu tím RMA částečně anuluje sebe samu, protože motivuje protivníky hledat způsoby a formy boje, které kompenzují konvenční převahu velmocí. Chápání jus ad bellum a jus in bello je závislé na kontextu tradičního chápání války jako masivního ozbrojeného střetu mezi státy (Eichler 2006) či přinejmenším a zejména v případech občanských válek masového střetnutí organizovaných stran, kde přinejmenším jednou ze stran je stát (Mareš 2004). Je zcela evidentní, že masové střetnutí organizovaných stran je krajně nepravděpodobné v případě, že pro většinu protivníků technologicky vyspělých států by se taková forma boje stala sebevražednou, předem odsouzenou k neúspěchu. V takovém případě se nabízí využití nekonvenčních taktik a zbraní. Nejdiskutovanější je v posledních letech bezpochyby terorismus. I však v případě, že by protivníci technologicky vyspělých států nesáhli přímo k terorismu, ale využili jiných forem boje, guerillové kampaně, sabotáží atd., překročili by s největší pravděpodobností omezení daná konvencemi. Nejinak je tomu i v případě, že by se pokusili využít nových forem boje, jako je např. kybernetický boj.

Jaké jsou charakteristiky kybernetického boje? Podstatou kybernetického boje je vymístění operací do kybernetického prostoru. Kybernetický boj je veden v elektronickém prostoru, prostřednictvím elektronických dat a elektronická data jsou také cílem operací. Ba dokonce by bylo možné jít ještě dále, aby došlo k jasnému odlišení elektronického boje (electronic warfare) a kybernetického boje, specifikovat operační prostor jako oblast dat v počítačích a počítačových sítích. Názor, že kybernetický boj lze vést i ve fyzickém světě, včetně užití konvenčních zbraní, například fyzickou

destrukcí hardware, který nese elektronická data, je diskutabilní, zvažování této možnosti do značné míry paralyzuje snahu o analýzu kybernetického boje – fyzická destrukce by měla být uvažována jako v nejlepším případě pomocná, podpůrná taktika nespádající do oblasti kybernetického boje per se. Stejně tak by užití EMP2 spadalo spíše do oblasti boje elektronického než kybernetického. Z terminologického hlediska je v kontextu této diskuse možné se odkázat na termín Computer Network Operations (CNO). CNO jsou chápány jako „akce vedené prostřednictvím (užití) počítačových sítí k narušení, zamítnutí (přístupu k), snížení hodnoty (poškození) nebo zničení informací nacházejících se v počítačích a počítačových sítích nebo počítačů a počítačových sítí samotných“ (U.S. Army War College: 2004). Přestože v definici tohoto termínu je zmíněna komponenta „vedení akcí prostřednictvím počítačů a počítačových sítí“, druhá část definice, tedy ničení počítačů a počítačových sítí samotných, odkazuje přinejmenším sekundárně k fyzické destrukci. Jakkoliv však, zúžení analyzované oblasti na boj v kybernetickém prostoru umožní uchopit a zdůraznit jeho klíčové charakteristiky.

Kybernetický prostor je ve své rozhodující části³ spojitý. Propojeny jsou jak „národní“ kybernetické prostory, tak privátní a veřejné a vojenské a civilní. Přechody, hranice mezi nimi, jsou často nezřetelné. Akce mohou probíhat rychlostí limitovanou pouze výkonem procesoru a kapacitou infrastruktury, tedy mnohem rychleji než operace ve fyzickém světě. Zejména mizení hranic (teritoriální, sociálních atd.) je typické i pro jiné typy bojových operací, nese s sebou však i popření minulých několika staletí vývoje, který směřoval právě k narýsování ostrých kontur války a míru, vojenského a civilního, legálního a zločinného, na kterých je vystavěno současné válečné a humanitární právo.

Kybernetický boj může být obranný i útočný. Součástí obrany je kontinuální ochrana, výstavba robustních a velmi dobře chráněných počítačových sítí, zřizování týmů monitorujících kybernetický prostor, schopných rychle reagovat, odhalit a zastavit kybernetický útok a napravit škody atd. Problém spočívá v útočném kybernetickém boji. Útočný kybernetický boj předpokládá krom přímé podpory jednotek na bojišti také útoky na nepřátelskou infrastrukturu. V duchu široké definice, která byla představena úvodem, jsou terčem operací data v počítačích a počítačových sítích, přičemž tato data se nemusejí ani zdaleka nacházet pouze ve vojenských počítačích a sítích, ba naopak – řada scénářů (strategické informační války, neomezené kybernetické války atd.) předpokládá právě využití slabin protivníkovy infrastruktury k realizaci plošných útoků, které mají ochromit ekonomiku, vyvolat strach, způsobit fyzické škody či obecně – ve svém důsledku vést k morálnímu rozvratu protivníka a zlomení jeho vůle pokračovat v odporu. Cílem kybernetického boje z podstaty věci není a nemůže být fyzické zničení (vojenských sil) protivníka.

Útočný kybernetický boj svojí podstatou popírá a překračuje hranice mezi vojenskou a civilní sférou. V obecné rovině je diskutováno vedení boje v kontextu principů rozlišování, přiměřenosti, zákonnosti, nezbytnosti, lidskosti a neutrality. Princip rozlišování, který je jedním z klíčových (srv. např. Jukl), odkazuje na striktní rozlišování mezi vojenskými a civilními cíli, aby byla výzbroj a taktika zákonná, nesmí působit ani nepřímé škody civilnímu sektoru a ne-kombatantům, pokud nejsou nezbytné. Princip přiměřenosti stanoví, že užití zbraně a taktika musejí být přiměřené vojenským cílům, což má předcházet neodůvodněné masivnímu použití síly, neadekvátnímu sledovaným cílům. Princip zákonnosti odkazuje na mezinárodní úmluvy či dvou- a vícestranné smlouvy a dohody – použitá výzbroj a způsob jejího nasazení nesmí odporovat takovýmto smlouvám. Princip nezbytnosti vychází z předpokladu, že použité zbraně a taktiky musí být odůvodnitelně nezbytné k dosažení vojenských cílů. Princip lidskosti spočívá v zákazu užití zbraní a způsobu jejich nasazení, který by způsobil obětem zbytečné utrpení a kalkuloval s šířením strachu. Podle principu neutrality by nasazené zbraně, ani způsob jejich použití neměly vést k poškození zdraví či smrti lidí v neutrálních zemích,

poškození jejich majetku nebo životního prostředí. V případě útočné kybernetické války není možné těmto principům vyhovět. Princip rozlišování je neuplatnitelný v případě strategické informační války nebo neomezené kybernetické války jednak proto, že vojenská a civilní infrastruktura jsou provázány, protože armády využívají i komerční (civilní) infrastrukturu, zvláště komunikační (srv. např. Greenberg, Goodman, Soo Hoo: 1998), ale i proto, že aby měl kybernetický boj skutečně účinný dosah, je často počítáno s útoky na kritické infrastruktury, které ovlivňují život celé populace, a to zcela úmyslně. Princip přiměřenosti není v případě kybernetického boje uplatnitelný v případech, kdy kybernetické operace nemají žádné přímé vojenské cíle, přičemž zjevně tento fakt hraje roli i v případě principu nezbytnosti. Princip zákonnosti by sice byl dodržen v tom ohledu, že kybernetické zbraně nejsou zakázány, na druhou stranu jejich využití porušuje celou řadu jiných smluv a úmluv, počínaje ochranou komunikací a pošty. Princip lidskosti předpokládající zamezení vyvolávání strachu je obtížně uplatnitelný v případech, kdy cílem kybernetického boje zcela naopak je či má být narušení morálky nepřátelské populace a strach by byl jednou z klíčových komponent takové operace. Ve spojitém kyberprostoru naprosto není možné zaručit dodržení principu neutrality – nejen, že může být nezbytné využít komunikačních tras neutrálních států a jejich kybernetického prostoru, což nemusí být ani úmyslné, ale může to být vlastností bojiště, ale navíc dopad kybernetického útoku nelze přesně alokovat (Darton: 2006).

Nedosti však na tom, že útočný kybernetický boj by byl diskutabilní formou boje, byl-li by užít slabšími protivníky technologicky vyspělých států k tomu, aby byla kompenzována jejich konvenční převaha. Kybernetický boj patří mezi oblasti válečnictví, které se zejména v poslední dekádě těší značné pozornosti, protože mohou posloužit k posílení či multiplikaci vojenského potenciálu těchto vyspělých zemí samotných. Není překvapivé, že největší zájem tato oblast přitáhla v USA, zemi patřící k technologicky nejpokročilejším, s nepochybně největšími investicemi do vojenství. Doktríny, které byly rozpracovány v dalších zemích NATO (např. Velké Británii), Ruské federaci či Číně zdaleka nedosahují takového stupně komplexnosti jako teoretické či doktrinální materiály americké armády (a U.S. Department of Defense). Americké studie jsou – i pro ostatní zmiňované země – referenčními.

V USA sílí v posledních letech pozice zastánců názoru, že obranná kybernetická válka je v horším případě odsouzena k neúspěchu, v lepším by byla neúměrně nákladná a náročná. Během více než 10 let, od cvičení Eligible Receiver 97 (viz GlobalSecurity.org) přes cvičení Blue Cascades a Blue Cascades II, Black Ice, Purple Crescent, Purple Crescent II4 atd. se opakovaně ukázalo, že infrastruktury jsou zranitelné kybernetickými útoky, které mohou způsobit nebo násobit významné škody i ztráty na lidských životech. Obrana proti kybernetickým útokům je ovšem nesmírně obtížná. Jedním z důvodů je zásadní podíl komerční či privátní infrastruktury⁵. Komerční infrastruktury jsou a byly budovány z pohledu cost/benefit jako takové, které při co nejmenších nákladech budou generovat co nejvyšší zisk. V průběhu desetiletí byla na internet či do kybernetického prostoru převedena řada aktivit, které dříve byly ošetřeny mechanicky anebo kontrolovány lidskými supervizory, což – zcela v duchu informační společnosti – šetří náklady na pracovní sílu, prostory, čas atd. Na druhou stranu se tyto aktivity staly zranitelnějšími. Komerční infrastruktury nebyly budovány primárně s ohledem na bezpečnost. Škody působené útoky či selháními mohou být nižší, než by byly náklady na zvýšené zabezpečení. U privátních segmentů informační infrastruktury může být situace ještě výrazně horší s ohledem na fakt, že značný podíl uživatelů ICT nedisponuje ani zdaleka dostatečnými znalostmi a zkušenostmi, aby i v případě zájmu dokázali zabezpečit infrastrukturu ve svém vlastnictví. Příkladem hrozby založené na privátních zdrojích mohou být obrovské botnety, které se opírají zejména o tisíce osobních pracovních stanic⁶. Zabezpečení komerční a privátní infrastruktury by si vyžádalo značné finanční náklady, úpravu legislativy či dohody mezi privátním a veřejným sektorem a zcela jistě by ani v nejlepším případě nemohlo být stoprocentní. Přestože se

situace v oblasti ochrany počítačů a počítačových sítí výrazně zlepšuje, sílí hlasy, že armády technologicky vyspělých států potřebují útočnou doktrínu kybernetického boje. To, co je nevýhodou při obranné kybernetické válce, je v případě ofenzivního kybernetického boje výhodou. A tak se objevuje doktrína ofenzivního kybernetického boje. Na rozdíl od defenzivního, kdy si lze představit dodržování konvencí, je ofenzivní boj nekonvenční. V tomto okamžiku se sbíhá několik tendencí. V případě slabších aktérů je to, jak bylo naznačeno, snaha kompenzovat převahu protivníka. V případě silných aktérů snaha využít potenciálu, který je jim vlastní, tedy kapacit k vedení útočného kybernetického boje a nízká efektivita obranného kybernetického boje. Výsledkem je všestranné nerespektování konvencí.

Vzhledem k tomu, že diskuse o mezinárodně-právním postavením útočného kybernetického boje jsou nápadně podobné diskusím o postavení terorismu (Roberts: 2002), nabízí se otázka, zda se ve vztahu k válečným konvencím nejedná o tentýž problém a tutéž otázku.

Terorismus jako takový nebyl dosud uspokojivě definován. Existuje celá řada více či méně obsáhlých definic (srv. např. Prudíková 2004) teroristického násilí, od definice vypracované už v 70. letech minulého století P. Wilkinsonem, který terorismus definoval jako "donucovací zastrašování, systematicky užívané vraždění a ničení nebo hrozba vraždění a ničení k terorizování jednotlivců, skupin, komunit či vlád s cílem dosáhnout uznání politických požadavků teroristů" až po syntetickou definici vycházející z textu A. P. Schmidta (Schmid 2001) pocházející z konce 80. let 20. století, která terorismus chápe jako „metodu vzbuzování strachu prostřednictvím opakovaných násilných aktů, vykonávaných tajnými nebo polo-tajnými jednotlivci, skupinami či státními orgány z idiosynkratických, kriminálních nebo politických důvodů, přičemž na rozdíl od atentátů nejsou přímé oběti násilí pravým terčem teroru. Okamžité lidské oběti násilných aktů jsou obvykle buď vybrány náhodně (příležitostné terče) z cílové veřejnosti, nebo záměrně (reprezentativní neboli symbolický terč) a slouží k předání zprávy. Komunikační procesy mezi teroristy (organizací), (ohroženou) obětí a hlavním terčem, založené na násilí a šíření strachu, jsou využívány k manipulaci hlavního terče (veřejnosti) tím, že se z nich stávají terče teroru, požadavků nebo upoutání pozornosti v závislosti na tom, zda jde o zastrašování, násilné donucování nebo šíření propagandy". Empirické definice, méně závislé na kulturním a politickém prostředí, se pokoušejí o extrakci podstatných rysů, kterými se terorismus liší od jiných forem nekonvenčního násilí. Obvykle odkazují na fakt, že v případě terorismu jde o specifickou formu psychologického boje, který využívá násilí s cílem vyvolat určitou - psychologickou - reakci u širšího počtu recipientů než jsou přímé oběti (Strmiska 2001). V paralele s kybernetickým bojem můžeme konstatovat, že ani cílem terorismu není a nemůže být fyzické zničení vojenských sil protivníka, ale ochromení jeho morálky. Ambiciózní pokus vypracování podrobného katalogu rysů či vlastností terorismu podnikl A. Merari (Merari 1993, Mareš 2004), který srovnával válku, guerillu a terorismus. Podle jeho názoru se terorismus a válka liší téměř ve všech ze sledovaných kritérií. Vojenská operace má zahrnovat či zahrnuje akce velkých uskupení, na kterých se podílí široké spektrum vojenské techniky, jde o kombinované operace, jejichž cílem jsou většinou vojenské jednotky protivníka, které mají být fyzicky ničeny. Cílem válečných akcí je kontrola teritoria, přičemž válečné zóny jsou geograficky rozeznatelné, vojáci nosí uniformy či jasné identifikační znaky. To zakládá legalitu vojenských operací. Teroristé oproti tomu operují v malých skupinách, používají specializované zbraně a zvláštní taktiku, jejich cílem nejsou vojenské síly protivníka, ale političtí oponenti, symboly a veřejnost, zamýšleným účinkem je psychologický nátlak, nikoliv tedy zničení protivníka. Teroristé ani neaspirují na kontrolu teritoria, nenosí uniformy, nelze je tedy identifikovat, boje probíhají v geograficky nerozeznatelných zónách. Teroristické akce také postrádají legalitu.

To co může sloužit jako ilustrace změny charakteru vojenství na případu útočného kybernetického boje, je fakt, že kritéria, která Merari nabídl ve svém výzkumu, a vlastnosti, které přičítá terorismu a kterými se podle jeho soudu terorismus odlišuje od války, vcelku přesně opisují i rozdíl mezi konvenční válkou a kybernetickým bojem. Ofenzivní kybernetický boj, zdá se, v mnoha svých ohledech odpovídá spíše terorismu než válečné akci tak, jak byla chápána v minulosti.

Kybernetický boj ve své podstatě vykazuje znaky značně odlišné od konvenčního válčení. Tyto znaky jsou společné mnoha jiných formám boje ve či proti vyspělé společnosti a vymykají se normám, podle kterých je v současné době posuzována oprávněnost akce a její legalita. Snaha předkládat kybernetický boj jako zcela novou, unikátní a kvalitativně odlišnou formu vedení boje, může být založena jak na nepochopení podstaty jeho nekonvenčnosti, tak politicky – vědomě či nevědomě – snahou o kodifikaci pravidel vyhovujících zejména silným hráčům s dostatečným politickým vlivem. Je však pravděpodobné, že nejde o speciální a unikátní případ vedení boje – jsou i jiné, dlouhodobě existující formy vedení boje, které vykazují podobné charakteristiky. Mnohem pravděpodobnější se zdá, že i s ohledem na fakt, že význam všech těchto nekonvenčních forem vedení boje stále roste v závislosti na posilování konvenčních kapacit některých silných hráčů, jde symptom obecného vývoje v oblasti vojenství. Společným rysem všech změn je přesun těžiště bojových operací. Namísto vojenské porážky protivníka se cílem operací stává morálka protivníka, ekonomika, vůle bojovat a klást odpor. Zároveň slabší aktéři nemohou čelit silným otevřeně, na bitevním poli. Nejenže nemají důvod, ale nemají ani příliš možností dodržovat konvence. Silní hráči souběžně zjišťují, že je pro ně nevýhodné konvenčním způsobem čelit nekonvenčním hrozbám. V některých případech je to téměř nemožné. Tento vývoj i tyto debaty lze ilustrovat stejně tak na příkladu terorismu, jako kybernetického boje. Možnosti, které se nabízejí, jsou pak v zásadě dvě: dojde k přehodnocení a modifikaci konvencí (dále viz např. Ellis 2001, Dahl 2004 aj.) a k modifikaci vojenské doktríny. Doktrína orientující se na porážku či fyzické zničení vojenských sil protivníka je nedostatečná v případě užití nekonvenčních forem boje a – jak bylo naznačeno – nekonvenční formy boje budou užívány stále častěji. Druhá možnost je, že problém zůstane neřešen a každý případ bude považován za unikátní svého druhu a poměřován a analyzován v rámci stávajících konvencí a politického vlivu konkrétních aktérů. Vojenská doktrína zůstane nezměněna a nekonvenční operace budou realizovány v rámci operací speciálních jako podpůrné a to do té doby, dokud se bude jednat o marginální oblast a komponentu válčení. To vposled s největší pravděpodobností povede k rozpadu systému konvencí jako takového a vzniku specializovaných institucí a organizací, které se budou podílet na boji, ale nebudou mít status armády. Vytvoří se tak přechod mezi civilní sférou a sférou vojenskou a dualita bude oslabena nebo zcela zmizí.

Poznámky:

1) Nabízí se koneckonců i srovnání s postojem velké části vojáků a teoretiků ve středověku k nasazení střelných zbraní. To bylo nejen považováno za nerytířské, ale v některých oblastech přímo za zločinné. To ovšem v žádném případě nezabránilo jejich masovému rozšíření. (Srv. Childs 2007)

2) Zbraně pracující na principu vytvoření elektromagnetického pulsu, který vyřadí nechráněnou elektroniku.

3) Existují samozřejmě separátní části, počítače nepřipojené k síti, izolované LAN (Local Area Network) nebo WAN (Wide Area Network), jako je např. The Secret Internet Protocol Network (SIPRNET).

4) Cvičení byla často zaměřena na kombinaci přírodní katastrofy a nebo fyzického a kybernetického útoku.

5) Tento podíl kolísá jak v čase, tak je třeba brát v úvahu podmínky jednotlivých národních států. V amerických podmínkách se uvádějí nejčastěji čísla mezi 80-95 procenty.

6) Za botnet je obvykle považována síť počítačů infikovaných bez vědomí majitele či autorizovaného uživatele programy umožňujícími jejich plnou či částečnou kontrolu útočníkem. Tyto sítě mohou být obrovské (desítky tisíc počítačů) vzhledem k tomu, že se k jejich získávání v posledních letech využívá automatizovaných nástrojů a jsou využívány jako infrastruktura, ze které jsou vedeny útoky (od rozesílání spamu, přes pronikání do dalších sítí, defraudace až po útoky zaměřené na odepření služby). Samo vytváření botnetů je v současnosti samostatným byznysem, útočníci s botnety nebo jejich částmi obchodují – prodávají je zájemcům na černém trhu, kteří je využívají k další nelegální činnosti (více např. Turek: 2008).

7) J. Langevin, prezident House Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, koncem září 2008 konstatoval, že nejlepší obranou je „dobrý útok“ a USA by se tudíž měly koncentrovat na rozvoj útočných schopností. (Viz. Waterman: 2008)

Literatura:

Dahl, E. Too Good to Be Legal? Network Centric Warfare and International Law. Journal of Public and International Affairs Volume 15/Spring 2004. Dostupné z WWW

<http://www.princeton.edu/~jpia/pdf2004/Chapter%203.pdf>, ověřeno k 8. 10. 2008.

Darton, G. Information Warfare and the Laws of War. In Cyberwar, Netwar and the Revolution in Military Affairs. New York : Palgrave Macmillan, 2006. ISBN 1-4039-8717-3.

Eichler, J. Mezinárodní bezpečnost na počátku 21. století. Praha: AVIS, 2006. ISBN 80-7278-326-2.

Ellis, B. W. The International Legal Implications and Limitations of Information Warfar. U.S. Army War College.

Dostupné z WWW http://www.iwar.org.uk/law/resources/iwlaw/Ellis_B_W_01.pdf, ověřeno k 7. 10.

2008.

Childs, J. Vojenská revoluce I. Přejchod k modernímu válečnictví. In Historie moderní války. Praha: Mladá fronta, 2007. ISBN 978-80-204-1540-0.

Greenberg L. T., Goodman S. E., Soo Hoo K. J. Information Warfare and International Law. National Defense University Press. Dostupné z WWW http://www.dodccrp.org/files/Greenberg_Law.pdf, ověřeno 8. 10. 2008.

Mareš, Miroslav. Vymezení pojmů terorismus, válka a guerilla v soudobé bezpečnostní terminologii Dostupné z WWW http://www.army.cz/mo/obrana_a_strategie/1-2004cz/mares.pdf, ověřeno k 8. 10. 2008.

Merari, A. Terrorism as a Strategy of Insurgency. Dostupné z WWW http://www.martinfrost.ws/htmlfiles/strategy_insurgency.html, ověřeno k 8. 10. 2008.

Prudíková, D. Násilí v rámci korsické otázky. Brno, 2004. Diplomová práce na FSS MU na katedře politologie. Vedoucí diplomové práce M. Mareš.

Roberts, A. Counter-terrorism, Armed Force and the Laws of War. Social Science Research Council. Dostupné z WWW <http://www.ssrc.org/sept11/essays/roberts.htm>, ověřeno 7. 10. 2008.

Roberts, A. Proti válce. In Historie moderní války. Praha: Mladá fronta, 2007. ISBN 978-80-204-1540-0. Red. Mají teroristé právo na status válečného zajatce? Vojenské rozhledy 2/2003. ISSN 1210-3292. Dostupné z WWW http://www.army.cz/avis/vojenske_rozhledy/022002.htm, ověřeno 10. 10. 2008.

Schmid, A.. Problémy s definováním terorismu. In. Encyklopedie světový terorismus. Od starověku až po útok na USA. Praha: Svojtka&CO, 2001. ISBN 80-7237-340-4.

Strmiska, M. Terorismus a demokracie. Brno: Masarykova univerzita, 2001. ISBN 80-210-2755-X.

Rexter | Časopis pro výzkum radikalismus, extremismu a terorismu

<http://www.rexter.cz/kategorie/02-2008/>

U.S. Army War College. Information Operations Primer. Fundamentals of Information Operations. Dostupné z WWW <http://www.csl.army.mil/usacsl/publications/IO-Primer-AY07.pdf>, ověřeno 4. 10. 2008.

Globalsecurity.org. Eligible receiver. Dostupné z WWW

<http://www.globalsecurity.org/military/ops/eligible-receiver.htm>, ověřeno k 10. 10. 2008..

Jukl, M. Obyčejové normy mezinárodního humanitárního práva. Český červený kříž. Dostupné z WWW

http://www.cck-cr.cz/docs/mhp/obycej_mhp.htm, ověřeno k 7. 10. 2008.

Turek, R. Bootnety. IT NEWS. ISSN 1336-3581. Dostupné z WWW

http://www.itnews.sk/buxus_dev/generate_page.php?page_id=53630, ověřeno k 9. 10. 2008.

Waterman, S. U.S. urged to develop offensive cyberwar capabilities. UPI. Dostupné z WWW

http://www.upi.com/Emerging_Threats/2008/09/29/US_urged_to_develop_offensive_cyberwar_capabilities/UPI-49311222720057/, ověřeno k 7. 10. 2008.