BEZPEČNOSTNÍ PROSTŘEDÍ

Mgr. Martin Bastl, Ph.D., Zuzana Gruberová

Kyberprostor jako „pátá doména“?

Vojenské rozhledy, 2013, roč. 22 (54), č. 4, s. 10–21, ISSN 1210-3292

Cyberspace as a “Fifth Domain”?

Abstrakt:

Cílem článku je představit aktuální diskuzi o kyberprostoru jako nové, páté válečné doméně. Čtenář je seznámen s konceptem kyberprostoru, jeho současným uchopením v především amerických doktrínách a vojenské teorii. Kontextuálně je zmíněna i funkce armády a specificky vymezení možností české armády. Diskutována je podoba kyberprostoru a jeho charakteristiky v kontextu vedení vojenských operací. Představeny jsou argumenty zastánců myšlenky kyberprostoru jako válečné domény i kritika tohoto pojetí. V závěru jsou argumenty obou stran shrnuty a zhodnoceny, a to i s přihlédnutím k roli a možnostem ozbrojených sil.

Abstract:

The aim of the article is to present an up-to-date discussion on cyberspace as a new, fifth domain of warfare. The reader is provided with the concept of cyberspace, its current interpretation, primarily in American doctrines and military theory. The army mission is contextually mentioned as well, explicitly the limits of Czech forces capacity. The paper deals with the form of cyberspace and its characteristics in the context of military operations. It advocates the idea of cyberspace as a war domain, which is presented together with the criticism to such approach. The article concludes with the summary and evaluation of both sides' arguments, taking into account the specific role and abilities of armed forces.

Klíčová slova:

Kyberprostor, informační a komunikační technologie, ICT, revoluce ve vojenství, RMA, informační válka, kyberválka, pátá válečná doména, sítí vedená bojová činnost, NCW, vojenské operace, role a možnosti ozbrojených sil.

Key words:

Cyberspace, information and communication technology, ICT, revolution in military affairs, RMA, information warfare, cyberwar, fifth domain of warfare, Network Centric Warfare, NCW, military operations, role and abilities of armed forces.

1. Úvod

Za poslední tři dekády se v souvislosti se šířením a stále intenzivnějším využíváním informačních a komunikačních technologií (ICT) hluboce a podle některých názorů i revolučně [1] proměnil charakter lidské společnosti, způsob života i fungování všech oblastí, od ekonomické a politické až po společenskou a – přirozeně – i vojenskou. Rychlost, se kterou k tomu dochází, v minulosti nemá obdoby. Kyberprostor, nová a uměle vytvořená sféra pronikající fyzickým světem, se stal novou složkou životního prostředí. Je provázán s existujícími prvky a ovlivňuje zásadním způsobem chod globálního ekonomického a politického systému. Jen počet uživatelů Internetu vzrostl za necelých 18 let z 16 milionů v prosinci 1995 na 2,75 miliardy v březnu 2013. [2]

S rostoucí vyspělostí společnosti roste závislost na ICT. Tato závislost ji činí zranitelnou v případě napadení informačních systémů a narušení kyberprostoru zvnějšku či zevnitř. Nové slabiny a zranitelná místa dávají prostor novým obavám, stejně jako novým strategickým úvahám. [3] V posledních dvaceti letech se tak vede diskuze jak mezi bezpečnostními experty, tak mezi vojenskými teoretiky o možnostech obrany i útoku založených na existenci informační infrastruktury a její role. V současnosti jsou kybernetické operace nedílnou součástí konfliktů, ať již jako samostatné akce nebo součást kombinovaných operací. Jako takové našly své místo i ve vojenských doktrínách. Od relativně vágních termínů jako „informace“, „informační sféra“, „informační doména“ používaných v 90. letech [4] postupně v doktrínách krystalizovala orientace na kyberprostor, chápaný jako nejvýraznější a – prozatím – nejkonkrétnější podoba nové složky operačního prostředí. To se otevřeně projevilo v roce 2006 uznáním kyberprostoru coby „válečné domény“ Ministerstvem obrany USA. [5]

Tento text se věnuje zásadní debatě, která ohledně celého konceptu v současnosti probíhá. Diskuze je reprezentována na jedné straně stále se vyvíjejícím pojetím kyberprostoru jako páté válečné domény, vedle souše, moře, vzduchu a vesmíru. Na druhé straně stojí kritici, reprezentovaní dvěma proudy. Jeden se orientuje na operační aspekty boje v kyberprostoru a autoři se jej prozatím rozhodli označit jako integrální. Ten nahlíží na kyberprostor coby sféru, která ostatními válečnými doménami prostupuje a tvoří jejich neoddělitelnou součást, nikoliv jako na svébytný celek či novou doménu. Považuje tedy doménový přístup za zbytečný, nekoncepční a neúčelně rozšiřující bojiště. Druhý kritický názor považuje za chybné opuštění konceptu informační domény. Zastává stanovisko, že samotný kyberprostor je pouze součástí informační domény a zaměření operací pouze na něj oslabí účinnost boje v informační doméně jako celku.

Cílem tohoto článku je diskuzi představit, porovnat a analyzovat vybrané argumenty doménového přístupu a jeho kritiků. Obecným metodologickým přístupem je hermeneutická analýza [6] následovaná komparací. Autoři přitom vycházejí především z odborné vojensko-teoretické literatury, přičemž hlavním pilířem jsou vojenské doktríny USA a odborná debata vedená v jejich kontextu. Tak je tomu i s ohledem na fakt, že USA jsou v současnosti dominující vojenskou silou a jejich vojenská teorie udává témata a určuje směr diskuze i ve vojenských kruzích dalších zemí.

Zařazení či nezařazení kyberprostoru mezi válečné domény není čistě teoretickou otázkou. Způsob, jakým věci pojmenujeme, předurčuje styl, jakým o nich přemýšlíme. To dále ovlivňuje způsob, jak s nimi nakládáme. Výsledek diskuze má a bude mít zcela praktické dopady nejen na to, jakými způsoby a prostředky bude veden boj

v kyberprostoru, ale také kým bude veden, v jakém rozsahu či s jakými omezeními. Pohled, jakým budeme na kyberprostor nahlížet, patrně ovlivní i to, jak budou strukturovány armády. Seznámit se s východisky a argumenty jednotlivých stran je tedy klíčové pro pochopení této nové, člověkem vytvořené vrstvy reality, i pro způsob, jakým bude včleněna do vojenské teorie a rozvoj dalších koncepcí kybernetického boje. Náš text je tedy příspěvkem do diskuze, která u nás probíhá jen ve velmi omezené míře. [7] A pokud tomu tak je, jde o diskuzi se zaměřením nikoliv na celkové koncepce a vojenskou teorii, ale na konkrétní otázky.

2. Terminologie a konceptualizace

Chceme-li se tázat po povaze jednotlivých prvků a jejich vzájemných vztahů, musíme si nejprve vymezit jejich podstatu, nalézt definici a účel. Pro naše potřeby je klíčový koncept kyberprostoru. Ve vztahu k němu pak úloha ozbrojených sil.

2.1 Kyberprostor

Koncept kyberprostoru v současnosti není ustálen a stále se vyvíjí. K řadě jeho charakteristik se nezbytně vrátíme ještě později. Sám pojem kyberprostor se v době, kdy se objevil, to jest v 80. letech, úzce vázal k vizi nefyzického, virtuálního prostředí generovaného počítači. To souznělo s jeho původem v jednom ze subžánrů vědeckofantastické literatury. V 90. letech, kdy začal být patrný rychlý a masivní nástup ICT, začal být kyberprostor chápán jako součást, podtřída informační sféry. [8] Současné definice jsou výsledkem více než třiceti let existence pojmu samotného a diskuze o roli informační infrastruktury. Mají již konkrétnější podobu, ale ani tak je nelze považovat za definitivní.

Za typické představitele definic posledních pěti let lze uvést tři příklady. Prvním je definice uváděná v *Joint Terminology for Cyberspace Operations*, kde je kyberprostor vymezen jako: „doména charakterizovaná užitím elektroniky a elektromagnetického spektra ke skladování, modifikaci a výměně dat skrze systémy spojené v sítích a přidruženou fyzickou infrastrukturu“. [9]

Druhá je definice TRADOC z roku 2010, kde je kyberprostor označen jako „globální doména uvnitř informačního prostředí sestávající se z propojených sítí informačních infrastruktur, včetně internetu, telekomunikačních sítí, počítačových systémů a včleněných procesorů a řídících jednotek”. [10] Třetí je definice D. Kuehla, který kyberprostor chápe jako „globální doménu uvnitř informačního prostředí, jejíž osobitý a unikátní charakter je zarámován užitím elektroniky a elektromagnetického spektra k vytváření, skladování, modifikaci, změnám a využívání informací skrze vzájemně závislé a provázané sítě užívající ICT“. [11]

Podobných příkladů by bylo jistě možné najít celou řadu. Společných rysů je přitom několik: jednak přenesení důrazu na fyzickou vrstvu jako podstatu kyberprostoru, kterou jsou přinejmenším systémy informační infrastruktury (hardware), v rozšířenější podobě ovšem i elektromagnetické spektrum jako takové. Další rozšířeně užívanou charakteristikou je funkce – zpracování informací – a struktura – vzájemně propojené systémy globálního dosahu.

Faktem je, že v současnosti dochází, na rozdíl od předchozích vágních vizí, k postupnému rozpracování konceptu kyberprostoru pro vojenské účely.

Obvykle je považován za systém sestávající se ze tří vrstev (viz tab.), rozdílní autoři je ovšem v současnosti stále charakterizují různě. Konstantou je přítomnost fyzické vrstvy, která je chápána buď jako a) hardware nebo b) hardware a elektromagnetické spektrum nebo c) elektrony. Druhou je logická vrstva. Ta je obvykle chápána jako a) aplikační vrstva (protokoly, software) nebo b) informace (software, data). Třetí vrstva je lidská či sociální, která je chápána jako a) kognitivní (poznávací) složka nebo za b) sociální složka sestávající se z osob a kyberosob, přičemž tyto dvě kategorie nejsou identické. [12]

Tab.: Vrstvy kyberprostoru

Fyzická vrstva	Logická vrstva	Lidská složka
hardware	aplikační vrstva	kognitivní vrstva
hardware a elektromagnetické spektrum	informační vrstva	sociální vrstva
elektrony		

Co můžeme v tomto okamžiku považovat za klíčové je skutečnost, že kyberprostor je nyní chápán jako konkrétní sféra zakotvená ve fyzickém světě, která nese logickou vrstvu (funkce, struktura) a interaguje (vzájemně působí) s lidským vnímáním, kognitivními schopnostmi a aktivitami stejně, jako je tomu u ostatních domén.

2.2 Úloha armády

Co se týče samotných ozbrojených sil, vymezení jejich vztahu ke kybernetickému prostoru je jednodušší otázkou. Není pochyb o tom, že role a postavení armády se historicky měnila. Mohla být společenským vzorem (Prusko 19. století), garantem určitého společenského uspořádání (kemalistické Turecko) či dokonce jeho strůjcem (Chile 70. let minulého století), plnit policejní či záchranářské úkoly v době nouze aj.

Samotným účelem armády však je a vždy bylo vedení války. Spolu s prudkým poklesem rizika rozsáhlého konvenčního konfliktu, k němuž došlo po zhroucení východního bloku, vzrostla také tendence využívat vojenské síly i v jiných typech operací, než jsou čistě válečné. [13] Tato tendence se nezvrátila. Lze však i přes širší spektrum možných protivníků, konfliktů a nástrojů vycházet z toho, že i nejaktuálnější vojenská teorie považuje za hlavní úlohu ozbrojených sil vedení vojenských operací proti organizovaným silám protivníka. [14] K tomu směřuje i činnost doktrinální.

Konkrétně v českém případě, pokud vyjdeme ze současného přístupu, zakotveného ve Vojenské strategii ČR a Doktríně Armády ČR, [15] který v podstatě určuje, že armáda může vojenské operace vést kdekoliv ve světě, bude-li k tomu vyzvána v rámci NATO, a proti jakémukoliv typu bezpečnostní hrozby. Pokud zároveň připustíme volný výklad zákona č. 219/1999 Sb., o ozbrojených silách ČR, zejména paragrafu 14, kde se hovoří i o převzetí úkolů Policie ČR v případě, že síly a prostředky ČR nebudou dostatečné k zajištění pořádku a bezpečnosti, případně odstranění jiného hrozícího nebezpečí za použití vojenské techniky, [16] můžeme konstatovat existenci extrémně

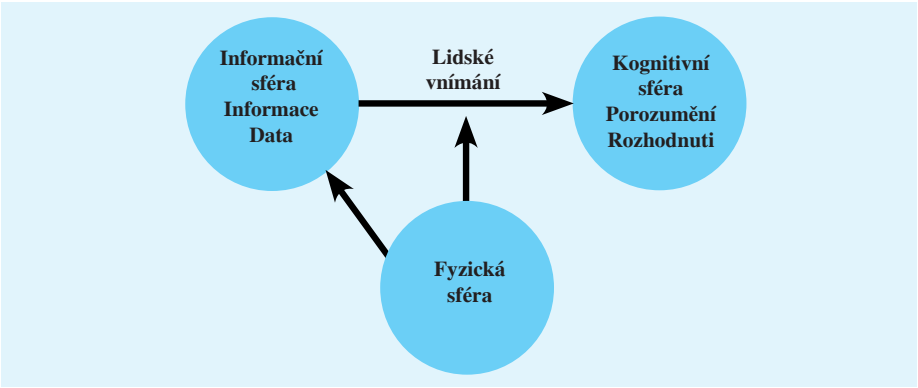
širokého spektra možných aktivit, na nichž se armáda může podílet, včetně aktivit v kybernetickém prostoru.

3. Kyberprostor jako válečná doména?

3.1 Pátá doména

Vývoj směřující k završení v podobě současného přijímání kyberprostoru coby páté válečné domény má kořeny v debatách 90. let o rostoucím významu ICT, potažmo informací jako takových. V první polovině 90. let měla idea války ve sféře informací minimálně dva zdroje. Jedním byla vlivná teorie manželů Tofflerových, kteří kromě jiného spolupracovali i na dlouhodobých koncepcích rozvoje americké armády. [17] Druhým byl již zmíněný pád východního bloku. Z toho vyplynulo zásadní snížení možnosti či hrozby rozsáhlého konvenčního konfliktu a zvyšující se důraz na řešení jiných než válečných hrozeb. Rozvinula se debata o revoluci ve vojenství (RMA). [18] Byl položen důraz na informace jako podstatnou, snad klíčovou složku pro získání převahy a rychlé dosažení vítězství.

Jako první se objevil koncept *informační převahy* (či dominance), k jejímuž dosažení má (ofenzivní i defenzivní) informační válka sloužit. Informační převaha má přispět především ke zvýšení efektivity vedení bojové činnosti ve fyzických doménách. [19] Druhým konceptem pak je informační sféra, v níž má být této dominance dosaženo.



Obr. 1: Koncept jednotlivých sfér bojiště [20]

Informační sféra zahrnovala nejen informace a data, ale i informační systémy, které byly samy o sobě infrastrukturou takzvaného kyberprostoru. Boji v oblasti informací se měly věnovat informační operace (IO), které zahrnovaly i boj v počítačových sítích (útok, obranu a vytěžování).

Důraz byl nejprve, koncem 90. let, položen na obranu počítačových sítí. S masivní expanzí ICT byla na prostředí počítačových sítí, potažmo kyberprostor, kladena stále větší váha. V prvních pěti letech 21. století sílily hlasy zdůrazňující roli informační infrastruktury a potřebu věnovat jí silnější pozornost, protože by mohla být strategickou slabinou USA. [21] Po několikaletém institucionálním rozvoji, kdy všechny složky

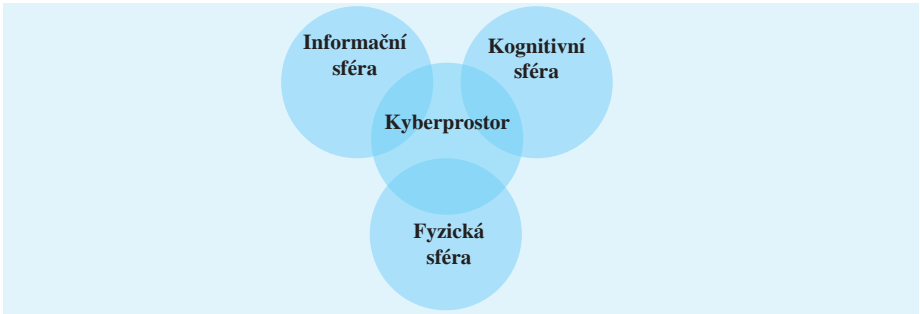
americké armády věnovaly kybernetickému boji zvyšující se pozornost, skutečně došlo k uznání kyberprostoru jako svébytné složky operačního prostředí. Národní strategie pro vojenské operace v kyberprostoru v roce 2006 uznala kyberprostor jako samostatnou doménu. Od té doby se o tomto kroku vede diskuze.

Jaké argumenty tedy předkládají zastánci vyčlenění kyberprostoru jako svébytné domény, stojící na úrovni fyzických domén jako je souš, moře, vzduch a vesmír?

Prvním argumentem je fakt, že je to efektivní, a to hned ve dvou ohledech. Jednak je to politicky výhodné, za druhé to umožní restrukturalizaci ozbrojených sil. Je to tedy to výhodné pro jednotky a struktury zaměřené na vedení kybernetického boje. Předpokládá, že posílení kybernetických jednotek, případně jejich osamostatnění povede ke zvýšení účinnosti operací v kyberprostoru. Uznáním kyberprostoru jako válečné domény se otevřel prostor pro artikulaci a prosazování amerických národních zájmů v kybernetickém prostoru ve velmi širokém ohledu – od vytvoření formálních mechanismů umožňujících v širokém rozsahu zpravodajskou činnost Národní bezpečnostní agentury (NSA), [22] až po investici půl miliardy dolarů do pokročilých vojenských systémů včetně systému pro boj v počítačových sítích. [23]

Přispělo to k uvedení *U.S. Cyber Command* do stavu plné operační schopnosti. Konečným cílem mají být změny, které umožní takovou organizaci, výcvik a vybavení v rámci kyberprostoru, s jakou se pracuje ve vzduchu, na souši, moři a vesmíru. [24] Jinak řečeno, označení kyberprostoru za doménu umožní širší manévrovací možnosti v politice, zvýší podporu investic do dané oblasti a otevře cestu k restrukturalizaci ozbrojených sil. Následný efekt bude spočívat v lepší činnosti vojenských jednotek a zpravodajských služeb, která směřuje či má směřovat k ovládnutí a kontrole této domény.

Další argument souvisí s prvním: kyberprostor má charakter teritoria, které je možné ovládnout a kontrolovat. Vykazuje tedy znak domény spadající do prostoru snahy o celospektrální dominanci. [25] Silným argumentem pro vyčlenění kyberprostoru, tedy i pro názor, že je samostatnou doménou, nikoliv jakousi podmnožinou informační sféry, je složení kyberprostoru tak, jak bylo zmiňováno v konceptu. Pokud kyberprostor zahrnuje fyzickou, logickou/informační a kognitivní/sociální vrstvu, zasahuje do všech sfér. V tomto ohledu má tedy stejné parametry jako ostatní válečné domény, souš, moře, vzduch a vesmír. Informace je jen složkou kyberprostoru – kyberprostor umožňuje informacím proudit, [26] není tomu obráceně.



Obr. 2: Složky kyberprostoru

Pokud odkážeme na charakteristiky ostatních domén, [27] což je závěrečný argument, kyberprostor je splňuje. Z podstaty jeho vrstev vyplývá, že jde o fyzikální oblast omezenou fyzikálními zákony, ať již v podobě infrastruktury nebo v podobě elektronů (elektromagnetického spektra). Platí v něm logika vojenských operací: útočných i obranných akcí [28] a vede se diskuze o manévrech specifických pro kyberprostor. [29] Vojenská uskupení mají stanoveny konkrétní úkoly a cíle. Pro operování v dané doméně jsou zapotřebí specializované zbraně a zbraňové systémy a vycvičený personál, což opět platí pro všechny domény. A nakonec – domény jsou navzájem závislé.

3.2 Kritika

Pokud se vyjádříme k argumentům zastánců vymezení kyberprostoru postupně, jako úvodní můžeme uchopit argument efektivity. Faktem totiž je, že tento argument je politický. Neříká nic o tom, jestli kyberprostor skutečně – *de facto* – je pátou válečnou doménou, tedy zda má smysl se ke kyberprostoru stavět stejně jako k ostatním doménám. Říká pouze, že bude efektivní ho takto chápat. To není argument, pouze předpoklad, který zastávají navrhovatelé vymezení kyberprostoru jako páté domény. Ano, pokud označíme kyberprostor za pátou válečnou doménu, povede to ke zvýšení investic a s největší pravděpodobností k rozšíření prostoru pro výcvik jednotek, možnosti osamostatnění struktur pro vedení kybernetického boje atd. To je praktický důsledek, není to ale důvod k tomu tak učinit. Kritici mohou naopak argumentovat tím, že je to neúčelné a efektivita tohoto kroku se ještě neprokázala a nemusí se prokázat, stejně jako tomu bylo u jiných transformačních kroků, které se na přelomu století orientovaly na sítí vedenou bojovou činnost (NCW), či v 80. letech investic do pokročilých zbraňových systémů určených pro konflikt se Sovětským svazem. Prostředky tím pádem budou vynaloženy neúčelně [30] a vytvoření potenciální samostatné vojenské struktury naopak oslabí účinnost boje, protože povede ke kompetenčním sporům, zvýší nároky na komunikaci a koordinaci, roztříští jednotu úsilí atd.

Proti vymezení kyberprostoru jako samostatné domény lze postavit perspektivu, která chápe kyberprostor jako sféru, která je transverzální – prostupuje všemi ostatními válečnými doménami, od nichž není možné ji oddělit. V případě armád technologicky vyspělých zemí v současnosti dokonce není možné bez využití kyberprostoru v kterékoliv z existujících domén operovat. [31]

Nejde o teritorium, spojitý prostor. Nelze v něm dosáhnout dominance. Tím je zpochybněn i druhý argument zastánců páté válečné domény, tedy předpoklad existence kyberprostoru jako teritoria, které lze ovládnout. Podle kritiků na rozdíl od čtyř známých domén – souše, moře, vzduchu a vesmíru – které je možné kontrolovat do takové míry, aby byl zajištěn svobodný přístup do každé z těchto sfér a zároveň dosaženo možnosti odepřít tento přístup protivníkovi, kyberprostor – jako globální elektronické médium – nemůže být kontrolován jediným státem [32] Kyberprostor nefunguje jako jednolitá sféra, ale jako vrstva sestávající z mnoha složek, z nichž každá je utvářena bez nutné závislosti na ostatních. [33] Kyberprostor, v kontrastu ke známým válečným doménám, je od základu vytvořen člověkem. Proto může být formován a utvářen způsobem, který je u jiných médií nemyslitelný.

Tím se dostáváme k argumentu shody či podobnosti s ostatními, fyzickými doménami. Tato shoda není úplná, ale pouze částečná. S největší pravděpodobností se týká

pouze jedné ze složek kyberprostoru, a to fyzické vrstvy. I v tom případě jde o nedokonalou shodu s ohledem na proměnlivost a nespojitost fyzické vrstvy. Kyberprostor nadto není proměnlivý nepředvídatelně, může být a je utvářen svými provozovateli v nebývalé míře a ve všech třech vrstvách. Je možné vytvářet nové sítě pro vojenské i jakékoliv další účely, izolované a vybavené maximálně bezpečným softwarem. Je možné prověřovat uživatele vojenských sítí a jednoznačně je identifikovat. Kyberprostor má zcela jiné charakteristiky než fyzické domény. Nahlížíme-li na něj jako na doménu, zavádí nás to k uvažování ve starých strategických intencích a k upřednostňování typu myšlení podobnému úvahám, ať taktickým či operačním, vycházejícím z analogického myšlení ve fyzických doménách. Namísto snahy o realizaci konkrétní akce s cílem dosažení konkrétního efektu (a zabránění téhož u protivníka) vede doménové myšlení k úvahám o kontrole, manévru, převaze.

Kyberprostor je konstruovaný a rekonstruovaný a všechny efekty v něm dosažené mají pouze dočasný charakter. Je možné skrze něj usnadnit fyzickou akci nebo zvýšit její účinnost, ale není možné v něm dosáhnout rozhodnutí. [34] Válka vedená prostřednictvím kyberprostoru by měla charakter války ekonomické a nikdo dosud nenavrhl označit ekonomiku za válečnou doménu. [35] Skrze kyberprostor lze způsobit ekonomické škody, ale nikoliv zastrašit, přinutit nebo porazit odhodlaného nepřítele. Jak rychle a snadno může být efektu dosaženo, tak rychle a snadno mohou být škody napraveny. Absence zastrašujícího či donucujícího efektu akcí v kyberprostoru souvisí s absencí přímého násilí – násilí je jedním z charakteristických znaků války a oddělení jednoho od druhého činí z války pouhou metaforu. [36]

Na jednu stranu je zapotřebí dodat, že slouží-li kybernetické operace jako podpora fyzických bojů, stává se tento argument bezobsažným. [37] Na druhou stranu lze tuto nutnost spojení s fyzickou (či kinetickou) akcí interpretovat i tak, že pokud bez tohoto spojení není kybernetický útok smrtící, je pouze integrální komponentou fyzického boje. Pokud kybernetické operace mohou usnadnit akce fyzické, ale musí jimi být provázeny nebo bezprostředně následovány, nelze v kyberprostoru jako takovém vést samostatně válku. [38] Není tedy samostatnou válečnou doménou. Zatímco válku ve fyzických doménách si bez kybernetické dimenze lze představit velice snadno, opačně to možné není.

A do řady odpůrců doménového přístupu, byť nikoliv zastánců toho integrálního, můžeme přidat také autory, kteří považují kyberprostor za vrstvu, která umožňuje skladování a přenos informací mezi aktéry. Podle jejich názoru jde tedy pouze o jednu ze složek informační sféry. Označením kyberprostoru za samostatnou válečnou doménu bychom se podle nich dopustili podobné chyby, jako kdybychom „za doménu moře chtěli označit pouze podmořské akce“. [39] Tito autoři prosazují koncept celé informační sféry jako válečné domény. Je to návrat zpět ke konceptu informační domény, který byl v průběhu posledních deseti let do značné míry opuštěn ve prospěch zdůraznění významu kyberprostoru.

4. Srovnání, vyhodnocení

V otázce zařazení či nezařazení kyberprostoru mezi válečné domény dosud nepanuje shoda a jak argumenty pro, tak argumenty proti, staví na logických základech. Nelze předpokládat, že by byla v dohledné době byla uzavřena ať již konsenzem nebo jasným

prosazením se jedné ze stran. To ovšem souvisí i s vývojem a dalším rozvojem kyberprostoru a ICT jako takových, stejně jako akcí a aktivit, které jsou v tomto prostředí vyvíjeny.

Patrně nejsilnějším argumentem zastánců doménového přístupu je potřeba efektivnější organizace ozbrojených sil pro operace v kyberprostoru. Ta je možná právě díky zařazení mezi domény a začlenění kybernetického boje za účelem získání převahy v kybernetickém prostoru do strategických vojenských doktrín. Není-li kyberprostor pokládán za doménu, nejsou ani možnosti plánování strategie obrany proti kybernetickým útokům tak široké. Funkce armády v rámci kyberprostoru je méně účinná.

Odpůrci naproti tomu varují před zastaralými představami o tom, že lze v kyberprostoru uplatňovat pravidla a postupy platné v jiných doménách. Odmítají myšlenku, že mu lze jednoznačně dominovat a že je tedy možné vytvářet za tímto účelem vojenské strategie tak jako v ostatních válečných doménách. Kromě toho poukazují na fakt, že kyberprostor prostupuje všemi ostatními doménami. Kyberválka podle jejich názoru není funkcí nezávislé domény, ale součástí boje vedeného ve fyzickém světě. [40]

Zastánci doménového přístupu kontrují konstatováním, že všechny domény jsou na sobě vzájemně závislé. Kyberprostor, ačkoliv vykazuje nesporně mnohé rozdíly oproti ostatním doménám, podléhá stejným fyzikálním zákonům jako ony, a je stejně tak vymezen fyzickým prostorem. S tím souvisí i teritoriální charakter kyberprostoru.

Na základě zkoumaných dokumentů lze rovněž vypozorovat, že zatímco doménový přístup volá po angažmá armády ve věci vedení kybernetických operací a následování určitého strategického rámce, odpůrci toto považují za kontraproduktivní. Otázky kybernetické bezpečnosti a ochrany kritické infrastruktury nepovažují za záležitost spadající do vojenských kompetencí. [41]

Přesto však k zařazení kyberprostoru mezi válečné domény již fakticky došlo. Přestože je nejen možné, ale hraničící s jistotou, že se doktríny budou dále vyvíjet, je třeba s tímto faktem pracovat. Prozatím nejnosnějším způsobem překonání rozporů mezi zastánci a odpůrci myšlenky páté válečné domény se jeví syntéza.

V tomto ohledu je možné přijmout definování kyberprostoru jako páté domény pragmaticky, jako koncept usnadňující přemýšlení, nicméně se silným omezením.

Velmi diskutabilní je užívání a hledání analogií mezi bojem v kybernetickém prostoru a ve fyzických doménách. Na taktické a operační úrovni vykazuje kyberprostor výrazně odlišné charakteristicky od fyzického světa, počínaje jeho tvárnosti a proměnlivostí a jeho nespojitostí konče.

Druhým problémem souvisejícím s chápáním kyberprostoru jako válečné domény je fakt, že samostatné akce v kyberprostoru jsou sice možné a představitelné, ale v dohledné budoucnosti nebudou mít zdaleka charakter a účinky srovnatelné s kinetickými operacemi ve fyzických doménách. Dosah kybernetických operací kolísá mezi zpravodajskou činností, sabotáží a ekonomickou válkou. Stejně rychle jako mohou být tyto škody působeny, mohou být i odstraněny. Mnohem větší potenciál má spojení akce v kyberprostoru s fyzickou akcí, kdy kybernetické akce doplňují tu fyzickou a zvyšují její účinnost. K takovýmto kombinovaným akcím již v minulosti došlo a byly úspěšné. Primární role kyberprostoru a akcí v něm je tedy zesilovat účinek akcí ve fyzickém světě. Z této perspektivy je nutné, aby byly aktivity jednotek činných v kyberprostoru úzce koordinovány s aktivitami jednotek působících v ostatních doménách. V tomto ohledu je třeba brát v potaz úlohy armády. Pokud americká armáda v souladu s americkou

národní strategií usiluje o světovou dominanci, je možná účelné budování samostatných struktur pro vedení kybernetického boje. Jinak se výhodnější cestou jeví cesta maximální integrace.

Diskutabilní je **role obrany v kyberprostoru.** Je jistě nutné zajistit ochranu vojenských sítí a instalací. Toho se, krom jiného, dá dosáhnout jejich vhodným návrhem, konstrukcí, izolací kritických systémů od vnějšího prostředí. Na druhou stranu je třeba přijmout fakt, že ani úspěšná obrana nemusí být dokonalá a stoprocentní. Postačí však, aby byla dostatečná na to, aby armádní složky působící ve fyzických doménách mohly plnit svoji funkci. Otázkou je samozřejmě, zda má armáda převzít odpovědnost i za ochranu vybraných civilních infrastruktur. Obecný závěr zní, že nikoliv, pokud jde o incidenty nízké intenzity, kriminalitu atd. Vstup armády má svoji logiku až v případě, kdy útoky přerostou svojí intenzitou, četností a nebezpečností hranici, za kterou je přestanou zvládat civilní struktury, hlavně týmy CERT (Computer Emergency Response Team) aj. Informační útoky se stanou přímou hrozbou národní bezpečnosti, případně budou spojeny s akcemi ve fyzickém světě, která budou válečného charakteru.

S ohledem na provázanost kyberprostoru s ostatními doménami dále nemá smysl, respektive je neúčelné a neefektivní uvažovat o vojenských operacích v kyberprostoru jako izolovaných aktech. Jejich význam by tak mohl být snadno přeceněn. Na rozdíl od kinetických akcí mohou být útoky v kyberprostoru jen stěží smrtící intenzity. Podle některých názorů [42] dokonce ani masové útoky, pokud se odehrávají pouze na kybernetické úrovni, nepředstavují skutečně životní nebezpečí.

Závěrem je nutno konstatovat, že koncept kyberprostoru jako páté válečné domény, přestože je v současnosti již běžně používán, se jeví prozatím jako nestabilní v otázkách teoretického rámce. Jeho funkce je zejména praktická. Vývoj v následujících letech může vést stejně tak k zakotvení i k redefinování, stejně jako tomu bylo u informační domény.

Tento příspěvek byl zpracován v rámci výzkumného projektu Metody predikce dlouhodobého geopolitického vývoje střední Evropy (VF20102015005), jehož poskytovatelem je Ministerstvo vnitra ČR.

Poznámky a literatura:

[1] Typicky jde o zastánce a pokračovatele práce manželů Tofflerových, jejich vize společnosti třetí vlny, společnosti informační. Viz TOFFLER, A. - TOFFLER. H. *The Third Wave.* 1. vyd., New York: Bantam, 1984, 560 s. ISBN: 978-05-532-4698-8; TOFFLER, A. - TOFFLEROVÁ, H. *Nová civilizace. Třetí vlna a její důsledky.* 1. vyd., Praha: Dokořán, 2001, 128 s. ISBN 80-86569-00-4 aj.

[2] MMG. *Internet Growth Statistics.* [online] 2013. [Cit. 2013-08-13] Dostupné z <http://www.internetworldstats.com/emarketing.htm>.

[3] Jedná se v případě závislosti na informační infrastruktuře o nové clausewitziánské těžiště, „centrum of gravity", dané společnosti? A s tím celá související debata o „strategické informační válce" (viz MOLANDER, R. - RIDDILE, A. - WILSON, P. *Strategic Information Warfare. A New Face of War.* RAND Corp. [online] 1996, 113 s. [Cit. 2013-07-25] Dostupné z <http://www.rand.org/pubs/monograph_reports/MR661.html>, ISBN 0-8330-2352-7; MOLANDER, R. - WILSON, A. - MUSSINGTON, D. - MESIC, R. *Strategic Information Warfare Rising.* RAND Corp. [online] 1998, 107 s. [Cit. 2013-07-25] Dostupné z <http://www.rand.org/pubs/monograph_reports/MR964.html>. ISBN 0-8330-2622-4; SIROLI, G. P. Strategic Information Warfare: An Introduction. In *Cyberwar, Netwar and Revolution in Military Affairs.* 1. vyd., NY: Palgrave Macmillan, 2006, 252 s. ISBN 987-1-4039-8717-4. S. 32–48 aj.) a „kritické infrastruktuře".

[4] Viz např. Joint Chiefs of Staff. *Joint Vision 2020: America's Military - Preparing for Tomorrow*, [online] 2000. [Cit. 2013-07-25] Dostupné z <http://www.fs.fed.us/fire/doctrine/genesis_and_evolution/source_materials/joint_vision_2020.pdf>; Joint Chiefs of Staff. *Joint Operations, JP 3-0*, [online] 2001. [Cit. 2013-08-11] Dostupné z <http://www.fs.fed.us/fire/doctrine/genesis_and_evolution/source_materials/dod_joint_ops_doctrine.pdf> aj.

[5] Joint Chiefs of Staff. *The National Military Strategy for Cyberspace Operations*, [online] 2006. [Cit. 2013-08-11] Dostupné z <http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf>.

[6] Existují tři druhy formální metodologie analýzy textů. Jsou to obsahová analýza, Glasser-Straussova metoda konstantního srovnávání a hermeneutická interpretace textu. Každá z těchto metodologií slouží k jinému účelu. Nejobvyklejší z nich je formální obsahová analýza, což je, jak známo, technika měření, která umožňuje testování teoreticky podložených hypotéz. Glaser-Straussova metoda je určena k tomu, aby se z psaných textů teorie vytvořila nebo vyvodila. Hermeneutická interpretace textu je přístup, který zdůrazňuje hluboké porozumění materiálu, který máme k dispozici. Klade důraz na uvědomování si vzájemného propojení „faktu" a „hodnoty" a na hledání významu uvnitř materiálu v kontextu, v němž vznikl. KRONICK, Jane, C. Alternativní metodologie pro analýzu kvalitativních dat. *Sociologický časopis,* 1997, roč. XXXIII, č. 1. Dostupné na <http://sreview.soc.cas.cz/uploads/d9ea8b94ec58c839306f61835d149215d1a90b3f_276_057KRONI.pdf >.

[7] Vzhledem k integraci do NATO je běžnější adaptace aliančních materiálů.

[8] Typicky publikace věnující se NCW, srv. ALBERTS, D.- GARSTKA, J.- STEIN, F. *Network Centric Warfare.* 2. vyd., Washington: CCRP, 2000, 284 s. ISBN 1-57906-019-6; ALBERTS, D.- GARSTKA, J. - HAYES, R. - SIGNORI, D. *Understanding Information Age Warfare.* 1. vyd., Washington: CCRP, 2001, 312 s. ISBN 1-893723-04-6 aj.

[9] Joint Chiefs of Staff. *Joint Terminology for Cyberspace Operations.* [online] 2010. 16 s. [Cit. 2013-07-28] Dostupné z <http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf>.

[10] TRADOC. *Cyberspace Operations: Concept Capability Plan 2016-2028.* [online] 2010, 80 s. [Cit. 2013-07-28] 16 s. Dostupné z <www.fas.org/irp/doddir/army/pam525-7-8.pdf?>.

[11] KUEHL, D. *From Cyberspace to Cyberpower: Defining the Problem.* [online] Information Resources Management College/National Defense University, 2009, 23 s. [Cit. 2013-07-28] 16 s. Dostupné z <http://www.carlisle.army.mil/DIME/documents/Cyber%20Chapter%20Kuehl%20Final.doc>.

[12] Viz např. TRADOC, 2010, VENTRE, D. Cyberconflict: Stakes of power. In *Cyberwar and Information Warfare.* 1. vyd. London: ISTE Ltd., 2011, 412 s. ISBN 978-1-84821-304-3. S. 113-244. Cit. s. 151.

[13] Přesto ovšem zůstávalo zachováno označení „vojenské operace", jak naznačoval akronym používaný v 90. letech pro mírové operace: „vojenské operace jiné než válka" (military operations other than war).

[14] Srv. GRAY, C. *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling.* [online] Strategic Studies Institute, 2013, [Cit. 2013-08-11] Dostupné z <http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1147>.

[15] *Vojenská strategie ČR.* [online] 2008. [Cit. 2013-08-11] Dostupné z <http://www.mocr.army.cz/images/id_8001_9000/8492/Vojensk__strategie__R-2008.pdf>; *Doktrína Armády ČR.* [online] 2010. [Cit. 2013-08-11] Dostupné z <http://www.unob.cz/fvz/struktura/k302/Documents/Doktrina_ACR.pdf>.

[16] *Zákon č. 219/1999 Sb.* [online] 2002. [Cit. 2013-08-11] Dostupné z <http://www.mocr.army.cz/images/id_0000_1000/172/219k.pdf>.

[17] TOFFLER, A. - TOFFLEROVÁ, H. *Válka a antiválka.* 1. vyd., Praha: Argo, 2002, 304 s. ISBN 80-86569-16-0.

[18] HUNDLEY, R. *Past Revolutions, Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us About Transforming the U.S. Military?* RAND Corp. [online] 1999, 124 s. [Cit. 2013-07-25] Dostupné z <http://www.rand.org/pubs/monograph_reports/MR1029>. ISBN: 0-8330-2709-3; BLANK, S. Preparing for the Next War: Reflections on the Revolution in Military Affairs. In *Athena's Camp.* RAND Corp. [online] 1997, 525 s. [Cit. 2013-07-25] Dostupné z <http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch3.pdf>. ISBN: 0-8330-2514-7. S. 61-77.

[19] Joint Chiefs of Staff. *Joint Vision 2010.* [online] 1996. [Cit. 2013-07-25] Dostupné z <www.dtic.mil/jv2010/jv2010.pdf?>.

[20] Na základě ALBERTS, D. - GARSTKA, J. - HAYES, R. - SIGNORI, D. 2001.

[21] K tomu přispívaly i hlasy ze zahraničí, např. čínská vojenská teorie, která jmenovitě informační infrastrukturu označila jako jeden z potenciálních cílů případné války s USA, viz LIANG, Q., XIANGSUI, W. *Unrestricted warfare.* [online] Peking: PLA Literature and Arts Publishing House, 1999, 228 s. [cit. 2013-07-26] Dostupné z <http://www.cryptome.org/cuw.htm>.

[22] PELLERIN, CH. *Lynn: Cyberspace is the New Domain of Warfare.* [online] DoD, 2010. [cit. 2013-08-15] Dostupné z <http://www.defense.gov/news/newsarticle.aspx?id=61310>.

[23] LYNN, William, J. III. The Pentagon's Cyberstrategy, One Year Later. *Foreign Affairs*. [online] Council of Foreign Relations, 2011. [cit. 2013-08-15] Dostupné z <http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later>.

[24] DoD. *Strategy for Operating in Cyberspace.* [online] 2011. 19 s. [cit. 2013-08-15] Dostupné z <http://www.defense.gov/news/d20110714cyber.pdf>.

[25] Např. DoD. *Joint Publication 1-02.* [online] 2010, 495 s. [cit. 2013-08-15] Dostupné z <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>.

[26] KELLEY, O. *Cyberspace Domain: A Warfighting Substantiated Operational. Environment Imperative.* [online] US Army War College, 2008, 37 s. [cit. 2013-08-15] Dostupné z <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA479775>.

[27] Ibidem.

[28] GRAY, C. 2013.

[29] Např. APPLEGATE, S. *The Principle of Maneuver in Cyber Operations.* [online] 2012, 13 s. [cit. 2013-08-15] Dostupné z <http://www.academia.edu/1436096/The_Principle_of_Maneuver_in_Cyber_Operations>.

[30] Podotkněme, že existují dokonce kritici, kteří upozorňují na to, že politická podpora vedoucí ke zdůraznění významu kyberprostoru souvisí s ekonomickými zájmy „kyberbezpečnostně-průmyslového komplexu", který má přímý zájem na profitu ze zvýšených investic, srv. např. BRITO, J. - WATKINS. T. *The Cybersecurity-Industrial Complex.* [online] 2011. [cit. 2013-08-18] Dostupné z <http://reason.com/archives/2011/07/25/the-cybersecurity-industrial-c>.

[31] RID, T. *What War in the Fifth Domain?* Kings of War. [online] 2012. [Cit. 2013-08-17] Dostupné z <http://kingsofwar.org.uk/2012/08/what-war-in-the-fifth-domain/>; VENTRE, D. 2012.

[32] CARR, J. *Inside Cyber Warfare.* Sebastopol, CA: O´Reilly Media, Inc. 2012, 294 s. ISBN 978-1-449-31004-2.

[33] LIBICKI, M. Cyberspace Is Not a Warfighting Domain. *A Journal of Law and Policy For Information Society* [online] 2012, Vol. 8:2, s. 321-336. [Cit. 2013-08-17] Dostupné z <http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf>.

[34] GRATZKE, E. *The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth.* [online] 2012. [cit. 2013-08-17] Dostupné z <http://dss.ucsd.edu/~egartzke/papers/cyberwar_12062012.pdf>.

[35] V tom se shodují autoři odmítající koncept páté válečné domény (E. Gartzke) i s některými jeho zastánci (C. Gray).

[36] RID, T. 2012.

[37] Např. J. Carr uvádí příklady útoků, které měly charakter kombinované operace – v kybernetickém a ve fyzickém světě a vedly k násilí či smrti, která by bez kybernetické komponenty nemohla být možná. Bylo by však velmi odvážné interpretovat tyto útoky jako smrtící kybernetické akce, viz CARR, J. *Clausewitz and Cyber War.* [online] 2011. [Cit. 2013-08-17] Dostupné z <http://jeffreycarr.blogspot.cz/2011/10/clausewitz-and-cyber-war.html>.

[38] Před zavádějícím pojmem kyberválka (cyberwar) varuje také jeden z tvůrců americké doktríny *Air-Land Battle* Huba Wass de Czege – směřuje totiž podle něj k představě analogií s tradičními formami války, které mohou být aplikovány v novém – kybernetickém – prostředí, viz de CZEGE, H. Winning in the Cyberelectropmagnetic Dimension of "Full Spectrum Operations". *Military Review* [online] 2010, Vol. 90:2 [cit. 2013-08-17] Dostupné z <http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20100430_art006.pdf>, ISSN 0026-4148. Tato debata o podstatě a charakteru kybernetické války ovšem již překračuje možnosti našeho textu.

[39] ALLEN, P. - GILBERT, D. The Information Sphere Domain. *The Virtual Battlefield: Perspectives of Cyber Warfare*. Amsterdam: IOS Press, 2009, s. 136. ISBN 978-1-60750-060-5.

[40] GRATZKE, E., 2012. Gratzke používá přímo termínu „pozemní boj".

[41] LIBICKI, M., 2012.

[42] GRAY, C., 2013.