 DOI: 10.3849/2336-2995.26.2017.04.035-054

Recenzovaný článek

Zajištění požadovaných schopností kybernetické obrany

Securing the Required Cyber Defence Capabilities

Miroslav Feix, Dalibor Procházka

Abstrakt: Článek se zabývá problematikou kybernetické bezpečnosti, kybernetické obrany a operací v kybernetickém prostoru s důrazem na rezort obrany. Článek navazuje na dříve provedenou analýzu úkolů, které stojí v oblasti kybernetické obrany a navrhuje rozdělení působností aktérů. Požadované schopnosti jsou odvozeny z úkolů stanovených právním řádem, vyplývajících z členství v NATO a EU a především staví na vytvořených strategických a operačních scénářích. Komparací požadovaných schopností a aktuálního stavu navrhuje řešení, umožňující uvedení do souladu obranu v kybernetickém prostoru s obranou České republiky, zajistit obranu kybernetického prostoru a integrovat kybernetické schopnosti do společného vedení operací.

Abstract: The paper deals with cyber security, cyber defence and operations in cyber space. It follows earlier performed analysis of cyber defence tasks and proposes distribution of competencies among key players. The required capabilities are derived from tasks determined by legislation, NATO and EU commitments and earlier developed strategic and operational scenarios. Comparing required capabilities and an actual state, a solution harmonizing defence in cyber space with defence of the Czech Republic and ensuring the cyber space defence and integration cyber capabilities into common operations conducting is proposed.

Klíčová slova: Kybernetický prostor; Kybernetická bezpečnost; kybernetická obrana; kybernetické operace.

Key words: Cyberspace; Cyber Security; Cyber Defence; Cyber Operations.

ÚVOD

Ohrožení České republiky, stejně jako ostatních států, v kybernetickém prostoru není hypotetickou hrozbou, ale aktuální skutečností. Včas porozumět, identifkovat a vhodně eliminovat ohrožení v době míru, či umět využít pro vedení operací i všechny operační domény v době vedení bojové činnosti je pro zajištění životních a strategických zájmů ČR klíčové. Článek je příspěvkem k diskuzi o kybernetickém prostoru, kybernetické obraně a o potřebných schopnostech rezortu MO. Navazuje na dříve provedenou identifikaci potřebných schopností rezortu MO v oblasti kybernetické obrany a zabývá se návrhem, jak rozdělit role rozdělit role, odpovědnosti a požadované schopnosti. Zodpovězením těchto otázek chce práce přispět k objasnění problematiky širší **vojenské operační komunitě** a nastínit možné cesty do budoucnosti.

VYMEZENÍ ZÁKLADNÍCH POJMŮ

Problematice kybernetického rozměru bezpečnostního prostředí je věnována stále větší pozornost. Je to dáno zejména tím, jak tento fenomén ovlivňuje čím dál více složky života naší společnosti. Podle Bezpečnostní strategie České republiky patří zajištění kybernetické bezpečnosti a obrany ČR mezi strategické zájmy.[1]

Kybernetika jako v nejširším smyslu je věda zabývající se řízením. Význam slova kybernetický se zejména s podstatným nástupem počítačů, počítačových sítí a internetu poněkud posunul a znamená „vztahující se nebo zahrnující počítače nebo počítačové sítě".[2]

Existuje řada definicí kybernetického prostoru. Z hlediska obsahového zpravidla zahrnují všechny entity, které jsou nebo potenciálně mohou být digitálně propojeny a mající vztah k ukládaným, zpracovávaným nebo přenášeným datům. Do **kybernetického prostoru** tedy patří všechna zařízení zpracovávající digitální data, která jsou nebo mohou být propojena. Jedná se o *„globální doménu uvnitř informačního prostředí, sestávající z nezávislých sítí a obsažených dat, včetně sítě Internet, telekomunikačních sítí, počítačových systémů a obsažených procesorů a řídicích prvků"*[3]. V kontextu článku chápeme kybernetický prostor jako globální fyzickou síť technologických infrastruktur, umožňující vznik, zpracování, ukládání, výměnu informací a lidské aktivity či virtuální život v něm.

Z hlediska struktury je kybernetický prostor chápán jako systém sestávající se z fyzické vrstvy, logické vrstvy a lidské složky.[4] Fyzická vrstva zpravidla zahrnuje technické prostředky, případně i elektromagnetické spektrum využívané k přenou informací, aplikační vrstva data a algoritmy jejich zpracování a lidská složka pak interakci s člověkem.

---

1 *Bezpečnostní strategie České republiky 2015*. Dostupné z: http://www.mocr.army.cz/images/id_40001_50000/46088/Bezpecnostni_strategie_2015.pdf.

2 http://www.merriam-webster.com/dictionary/cyber-

3 *Joint Publication 3-12 (R)* [online]. Dostupné z: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

4 Ibidem

Pod **kybernetickými operacemi** rozumíme nasazení kybernetických schopností, jejichž primárním účelem je dosažení cílů v nebo prostřednictvím kyberprostoru[5]. Důležité jsou vlastnosti kybernetického prostoru, které determinují, jakým způsobem a jakými cestami se kybernetické hrozby, případně kybernetické operace, mohou realizovat. Kybernetický prostor:

- Je stvořen, užíván a měněn lidmi.
- Je časově proměnný, nestabilní, nespojitý.
- Prostor pro kybernetické operace je dán zranitelností informačních systémů nebo entit, které jsou jejich součástí. Neexistuje-li zranitelnost, není možné do segmentu kyberprostoru proniknout, tudíž ani jakkoli v něm působit.
- Je tvárný a jeho tvárnost je pod kontrolou toho, kdo jej stvořil (připojení nebo odpojení k síti, vypnutí, administrativa, aplikace nebo změna bezpečnostních nastavení),
- Segmenty kyberprostoru mohou být vytvářeny, ale i ničeny.

Tyto vlastnosti kybernetický prostor odlišují od jiných válečných domén (země, voda, vzdušný prostor, kosmický prostor). Ačkoli polemika, zda je lepší kybernetický prostor považovat za pátou válečnou doménu[6], či jen jako integrální součást ostatních domén[7] se stále vede, podstatné je, že na summitu NATO ve Varšavě byla tato doména uznána. Toto rozhodnutí se promítne do organizační struktury sil, obranného plánovaní i plánování operací.

Odlišnosti kyberprostoru jsou zásadní pro chápání kybernetických operací, ať obranných nebo útočných. Z hlediska dopadů je nejzávažnější kybernetický útok, o jehož provádění nemá napadená strana povědomí. Jedná se o tzv. pokročilé kybernetické hrozby (Advanced Persistent Threads). Tento útok probíhá v následujících fázích, viz obrázek č. 1:[8]

- Průzkum. Protivník zkoumá, identifikuje a vybere své cíle.
- Vyzbrojení. Protivník spáruje malware se zjištěnými zranitelnostmi.
- Doručení. Protivník přenáší datové části zbraně k cíli, často prostřednictvím e-mailu, webových stránek nebo USB tokeny.
- Zneužití. Doručený škodlivý kód je spuštěn uživatelem, například otevřením přílohy e-mailu, návštěvou infikované webové stránky, připojením infikovaného média.
- Instalace. Malware infikuje systém uživatele. Zpravidla se provádějí kroky znesnadňující jeho detekci v tomto systému.
- Řízení a komunikace. Malware naváže spojení s řídícím serverem, zpravidla často prostřednictvím šifrovaných kanálů, které je těžké odhalit. Protivník pak může podnikat konkrétní akce, například skrytě získávat informace nebo připravit destrukci systém, případně po vytěžení zničit stopy po působení. V případě, že cílem je destrukce, není komunikace s řídicím systémem nutná.

---

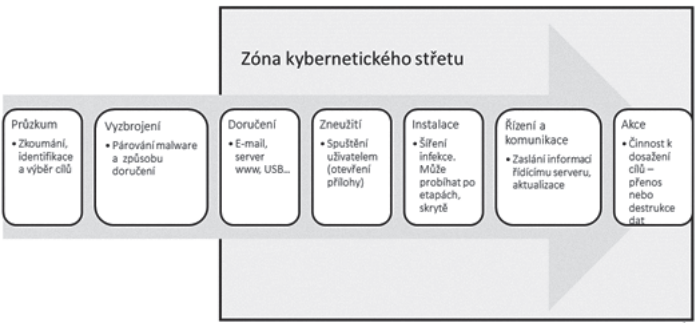
5 Ibidem

6 WELCH, Larry D. *Cyberspace – the Fifth Operational Domain.* Alexandria 2011, Institute of Defense Analyses.

7 LIBICKI, Martin. Cyberspace Is Not a Warfighting Domain.

8 LACHOW, Irving. Active Cyber Defense: A Framework for Policymakers.

- Akce. Malware provede činnosti, které plní cíle a záměry útočníka. Obvykle se jedná o získání dat, ale data mohou být také změněna nebo zničena.



Obrázek č. 1: Fáze kybernetického útoku.[9]

Zásadní odlišnosti od kinetického působení spočívají především v nezbytnosti průzkumu a zjištění zranitelnosti, dále ve vytvoření kybernetické zbraně využívající tyto specifické zranitelnosti a dále v nutnosti doručení kybernetické zbraně do cílového systému. Všechny tyto aktivity vyžadují přístup k cílovému systému, ať prostřednictvím přímého připojení, nebo prostřednictvím vědomě či nevědomě spolupracující osoby. V závislosti na důležitosti cíle a jeho aktiv pro útočníka se uplatňují různé metody, od prostého šíření necílené nevyžádané pošty po metody sociálního inženýrství.[10] Dalším aspektem je nepředvídatelnost účinků takového útoku, kdy může rozsah škod překročit záměr útočníka.

V minulosti se ukázalo zastrašování v oblasti nukleárních zbraní významným stabilizačním faktorem. Tento přístup je v kyberprostoru využitelný jen omezeně.[11] Vyplývá to především z toho, vůči jakým aktérům je aplikovatelný. Princip zastrašování může být účinný vůči státním aktérům, protože vůči nim lze nalézt adekvátní odpověď. Naopak proti nestátním aktérům, skupinám nebo jednotlivcům formulaci a prosazení adekvátní a účinné politiky zastrašování znesnadňuje obtížnost přiřazení, prokázání a fyzické zajištění původce kybernetického útoku. Obecně účinnost zastrašení v kyberprostoru souvisí se zranitelností aktiv prostřednictvím kybernetického útoku. Na druhé straně může kybernetický konflikt v závislosti na jeho dopadech eskalovat i do jiných domén.

Kybernetická doména je vojenské označení pro kybernetický prostor. Je to operační prostředí se svébytnými faktory a dostatečně odlišnými zákonitostmi, vyžadující specifický přístup při vedení bojové činnosti, prostředí, kde se plánují a vedou operace. Na summitu NATO ve Varšavě[12] byla uznána jako další doména. Kybernetická doména má zvláštní povahu, je doménou sama o sobě a zároveň propojuje vojenské platformy

9 Upraveno podle LACHOW, Irving. Active Cyber Defense: A Framework for Policymakers.

10 Sociálním inženýrstvím rozumíme způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace.

11 DENNING, Dorothy. *Rethinking the Cyber Domain and Deterrence.*

12 Warsaw Summit Communiqué. Dostupné z: 1url.cz/MtQEy.

působící v ostatních doménách a také vytváří virtuální informační prostor. Je to taková nervová síť operačních domén, avšak do těchto domén vnáší i specifické zranitelnosti.

Kybernetickou bezpečnost (KB) můžeme chápat jednak jako stav, kdy jsou na nejnižší míru eliminovány hrozby pro ČR působící z kybernetického prostoru, na druhé straně jako „souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru".[13]

Kybernetická obrana (KO) je v kontextu článku chápána jako obrana[14] v kybernetickém prostoru a jeho prostřednictvím.

VÝZKUMNÉ OTÁZKY A METODY ŘEŠENÍ

Autoři se zabývali následujícími výzkumnými otázkami:

1. Jakými schopnostmi by měl disponovat rezort obrany, aby zajistil požadované úkoly z hlediska kybernetické bezpečnosti a kybernetické obrany?
2. Jak rozdělit role, odpovědnosti a požadované schopnosti v tomto kontextu?

Při identifikaci požadovaných schopností byly použity metody analýzy legislativních, koncepčních a doktrinálních dokumenty ČR, Severoatlantické aliance i Spojených států amerických (USA), a dalších zdrojů a konzultací s vybranými odborníky v dané oblasti. Pro zpracování analýzy trendů byla využita faktorová analýza PESTLE[15], jejíž podstatou je analýza politické, ekonomické, sociální, technologické, právní a environmentální oblasti. Hlavním zdrojem informací o trendech a budoucím prostředí jsou analytické dokumentu NATO[16] a Spojených států amerických.[17] Jako další zdroj úkolů byly zpracovány čtyři scénáře[18] pokrývající některé možné situace působení v kybernetickém prostoru.

Syntézou úkolů byly dále stanoveny kvalitativní požadované schopnosti a navržena řešení na jednotlivých úrovních. Požadavky na schopnosti vyplývají ze scénářů, stanovených úkolů ať už v rámci ČR nebo vyplývající ze členství v NATO a EU. Požadavky jsou pro snazší porozumění seskupeny dle hlavních oblastí schopností (dále MCA – Main Capabilities Areas). Komparací požadovaných schopností a úkolů stanovených v zákonných, koncepčních a doktrinálních dokumentech byly zjištěny mezery a nedostatky a dále navržena systémová řešení problémů na jednotlivých úrovních a upozornění na sporná místa návrhu. Navrhovaná řešení byla prodiskutována s vybranými odborníky.

---

13 JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*.

14 V souladu s definicí v Zákoně 222/1999 Sb.

15 GRASSEOVÁ, Monika, Radek DUBEC a David ŘEHÁK. *Analýza podniku v rukou manažera*.

16 *Framework for Future Alliance Operations*. Norfolk, Virginia: North Atlantic Treaty Organisation, Supreme Allied Command Transformation, 2015.

17 *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World*. Joint Chiefs of Staff, 2014.

18 GRASSEOVÁ, Monika, Radek DUBEC a David ŘEHÁK. *Analýza podniku v rukou manažera*.

Výsledky vztahující se k první otázce byly již publikovány.[19] Následující část je věnována návrhu v souladu s druhou výzkumnou otázkou.

POŽADAVKY NA KYBERNETICKOU OBRANU PODLE HLAVNÍCH OBLASTÍ SCHOPNOSTÍ

Úkoly, identifikované analýzou, jsou shrnuty v tabulce č. 1. Dále jsou rozebrány požadované schopnosti seskupené do oblastí MCA.

Úkoly vyplývající z dokumentů NATO a EU	Úkoly vyplývající z legislativy **a koncepčních dokumentů**	**Oblasti úkolů vyplývající ze scénářů**
zodpovědnost za vlastní sítě,	ochrana vlastních neutajovaných sítí a kritické infrastruktury	odolnost a bezpečnost informací
odolnost a bezpečnost informací,	ochrana vlastních utajovaných sítí (zákon výslovně neřeší)	zabezpečování informací v kyberprostoru
interoperabilita sítí a kybernetické obrany,	kybernetická obrana*	Kkybernetické operace
sdílení informací,	systémy zařazené do významných informačních systémů a kritické infrastruktury musí splňovat stanovené standardy	informační působení v kyberprostoru
společné vzdělávání,	povinnost podávat a sdílet informace	koordinace a řízení
spolupráce s průmyslem,	provádět opatření k ochraně sítí a infrastruktury	
spolupráce s akademickou sférou,	systém koordinace	
začlenění Cyber Defence** do plánování a vedení operací		
začlenění Cyber Defence do vojenských cvičení		
jasná struktura velení a řízení v kybernetické oblasti		
schopnost tvorby společného obrazu o stavu vlastních sítí a kybernetického prostoru		

Tabulka č. 1: Identifikované úkoly kybernetické obrany podle zdrojů úkolů

* S vědomím faktu, že pojem kybernetická obrana není legislativně vymezen.
** Ve smyslu chápání pojmu podle NATO, tedy blíže k pojmu kybernetická bezpečnost.

19 FEIX, Miroslav a Dalibor PROCHÁZKA. Aktuální úkoly kybernetické obrany rezortu Ministerstva obrany.

Rozvoj, výstavba a příprava (Prepare).

Rezort obrany musí být schopen:

- vytvořit a rozvinout schopnosti pro vedení operací v kybernetickém prostoru,
- připravit bojovníka-specialistu pro vedení operací v kybernetickém prostoru,
- připravit vojáky na vedení operací v kybernetickém prostoru,
- vybrat a udržet vhodné vojáky pro vedení operací v kybernetickém prostoru,
- přizpůsobit systém přípravy tak, aby podporoval spolupráci, výzkum a inovace, flexibilitu a kritické myšlení.

Imperativem doby je vytvořit a rozvinout schopnosti pro vedení operací v kybernetickém prostoru a to koncepčně, doktrinálně a uvést do praxe. V současné době již není možné provádět operace v kyberprostoru jako přidruženou záležitost, vytvoření a rozvoj vlastní vojenské odbornosti je nezbytnou podmínkou. S tím souvisí tvorba vzdělávacích programů a studijních oborů na Univerzitě obrany a podpora této oblasti na vysokých školách. Specifika kyberprostoru přináší i nutnost výběru vhodného personálu pro vedení operací, často ne zcela odpovídajícího zažitým představám o příslušníku ozbrojených sil. Celý systém přípravy musí budoucího vojáka profesionála ve vysoké míře formovat ke spolupráci, inovacím, flexibilitě a kritickému myšlení. Jedinou jistotou budoucího prostředí je dynamika změn, a nutnost neustálé adaptace a hledání nových cest a řešení. V kybernetickém prostoru, jako lidmi vytvořené a tvarovatelné doméně, je pak rychlost změn ještě výraznější a pro vojáky-specialisty tak klíčová.

Budoucí operace budou společné, provázané a integrované úsilí všech sil, druhů vojsk, složek státu ve všech doménách a prostředích. Síly a prostředky pro operace v kybernetickém prostoru nesmí být budovány odděleně od ostatních. Vedení operací a využívání kyberprostoru se musí stát běžnou součástí přípravy a působení sil a kybernetická tématika součástí všech stupňů kariérního vzdělávání.

Základem všeho je však výchova a vzdělávání k bezpečnému chování v kyberprostoru v rámci celého školského vzdělávacího procesu. U vojáků pak specificky zaměřená na ochranu identity, operační bezpečnosti a bezpečnosti informací.

Nasazení (Project).

Rezort obrany musí z hlediska projekce síly a působení v kyberprostoru obsahovat:

- infrastrukturní schopnosti,
- nasaditelné schopnosti,
- reachback.[20]

Projekce síly v kybernetickém prostoru má svá specifika. Projekce jako fyzický přesun v mnoha případech ztrácí svou relevanci. Naopak v kybernetickém prostoru dochází k projekci síly bez nutnosti fyzické přítomnosti. Ve velké míře bude hrát svou roli působení na nepřítele silami a prostředky, které nebudou fyzicky nasazeny a bude se ve vysoké míře používat metod reachback.

Z hlediska místa je nezbytné vlastnit schopnosti umožňující zabezpečení funkčnosti vlastní infrastruktury a vedení operací na stacionárních sítích. K působení pak využívat vzájemnou propojenost kybernetického prostoru.

---

20 Využívání kapacit a schopností nenasazených přímo v operaci, ale působících ve prospěch operace.

I přes propojenost a velkou míru nezávislosti na místě v síti je nebytné vytvářet i nasaditelné schopnosti, schopné rychle se přesunout do prostoru operace, rychle rozvinout síly a prostředky, vytvořit bezpečné oblasti v rámci kybernetického prostoru a integrovat kybernetické síly a prostředky (ať už fyzicky přítomné, nebo vzdálené) do společného působení v rámci vedení operace.

Zasazení (Engage).

Rezort obrany musí být schopen působit v kybernetickém prostoru a vést následující operace:

- odolnost a bezpečnost informací,
- defenzivní kybernetické operace,
- ofenzivní kybernetické operace,
- strategická komunikace v kybernetickém prostoru,
- informační operace v kybernetickém prostoru.

První tři operace mají převážně technickou povahu a dopad do fyzického světa, poslední dvě naopak primárně míří do informačního prostředí. Není možné to ale takto striktně oddělit, operace se prolínají a vzájemně podporují.

Odolnost a **bezpečnost informací** je souhrn opatření k návrhu, výstavbě, konfiguraci, zabezpečení, řízení, údržbě a provozu komunikačních a informačních systémů s cílem udržet datovou dostupnost, integritu, důvěryhodnost, stejně jako autentičnost a nepopiratelnost.[21] Toto je základní a nezbytnou schopností, kterou musí disponovat každý provozovatel komunikačních a informačních sítí. Vychází jak z národních požadavků kybernetické bezpečnosti, kdy je někdy také tato schopnost takto označována, tak z požadavků a cílů schopností NATO. Jedná se o aktivity, které probíhají vždy v rámci vlastních sítí.

Defenzivní kybernetické operace jsou operace na ochranu a obranu vlastních, spřátelených a neutrálních sítí. Zajišťují svobodu přístupu a manévru v kybernetickém prostoru. Jsou souhrnem aktivních a pasivních opatření k přetváření vnitřní struktury a charakteru kyberprostoru a komunikačních kanálů v něm, například *„reestablish, resecure, reroute, reconstitute, or isolate degraded or compromised local networks"*.[22] Do defenzivních operací patří i aktivní vyhledávaní průniku do vlastních sítí a nepřátelských aktivit v nich, včetně vytváření léček a nástrah (Honeypot[23]).

Ofenzivní kybernetické operace jsou charakteristické aktivní aplikací síly v kybernetickém prostoru. Cílem je buď ničení infrastruktury, komunikačních tras, dat a informací, nebo poškození, manipulace a změny dat a informací. V druhém případě je vidět možná provázanost těchto operací s informačním působením a informačními operacemi.

Tabulka č. 2 ukazuje rozdělení částí operací v kybernetickém prostoru technické povahy, podle vlastnictví sítě a použití síly.

---

21 *Joint Publication 3-12 (R): Cyberspace Operations*. Washington, DC: Joint Chiefs of Staff, 2013. Dostupné také z: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

22 Ibid, s. II-2.

23 Proactive detection of security incidents II - Honeypots. Dostupné z: https://www.enisa.europa.eu/publications/proactive-detection-of-security-incidents-II-honeypots.

	Sítě			
Operace	Vlastní	Spřátelené a neutrální	Nepřátelské	Použití síly
Odolnost a bezpečnost informací	X			NE
Ofenzivní		X	X	ANO
Defenzivní	X	X		NE

Tabulka č. 2: Technické operace v kybernetickém prostoru

Strategická komunikace a **informační operace** v **kybernetickém prostoru.** Současné a budoucí operační prostředí bude charakteristické informační propojeností. Působení na informace a rozhodování protivníka a ochrana vlastních bude klíčovým prvkem úspěchu. *„To platí již* v *dnešním operačním prostředí,* a *proto ozbrojené síly ČR potřebují schopnost účinně informačně působit* a *bránit se proti takovému působení."*[24]

Kybernetický prostor je významnou součástí informačního prostředí s neustále rostoucím podílem vlivu. Ovládnutí metod a forem strategické komunikace a informačních operací v kybernetickém prostoru je tak nutností.

Udržení (Sustain).

Rezort obrany musí pro udržení nepřetržitého vedení vybudovat:

- vhodný akviziční systém,
- dostatečně robustní strukturu,
- aktivní zálohy.

Vhodný akviziční systém. Rozvoj technologií, metod a postupů v oblasti informačních technologií jde výrazně rychleji než v jiných relevantních oblastech nákupu materiálu a služeb pro potřeby obrany. Materiál se stává zastaralým a v mnoha případech i nepoužitelným již po velmi krátké době. Zatímco auto může mít životnost 20let, puška 10let, počítač 4 roky, životnost kybernetické softwarové zbraně, tj. malware, může být omezena identifikovanou zranitelností, které trvají omezenou dobu. Pro vývoj kybernetických zbraní je běžný akviziční proces nepoužitelný i z hlediska utajení požadavků.

Operace v kyberprostoru probíhají nepřetržitě i v době míru. Proto je nezbytné vybudovat **dostatečně robustní strukturu** sil a prostředků v požadované kvantitě a kvalitě, pro zajištění plnění úkolů. Výhodou a zároveň nevýhodou je částečný překryv vlastních činností s civilním sektorem. Jedná se především o IT specialisty v technické oblasti, kde se soutěží o vhodné pracovníky a ozbrojené síly často prohrávají, ať už kvůli finančnímu ohodnocení nebo nekompatibilitě organizačních kultur. V informačním působení je pak důležitá blízkost například s novináři nebo pracovníky reklamních společností. Zde se ale

24 ŘEHKA, Karel. *Strategická komunikace a informační operace v resortu MO ČR: Závěrečná práce v kurzu Generálního štábu. Univerzita Obrany, Centrum bezpečnostních a vojenskostrategických studií*. Brno, 2016, s. 19.

zase nabízí možnost využít institut **aktivních záloh** pro případ vedení dlouhodobé operace, nebo nutnosti jednorázové pomoci.

Konzultace, velení a řízení (Consult, Command and Control).

Rezort obrany musí být schopen:

- koordinace,
- jednotného řízení,
- mezinárodní spolupráce.

Tato oblast propojuje všechny ostatní oblasti schopností. Na dosažení stanovených cílů je nezbytná koordinace a spolupráce všech zainteresovaných aktérů, které představují soukromá sféra, vládní a nevládní organizace, zpravodajské služby a ozbrojené síly. Každý z aktérů má své zájmy a cíle často i dost rozdílné. Cílem je sjednotit úsilí, shodnout se na společném směru, a **koordinovat** postup. Prostředkem je vytvořit v mírovém stavu platformu pro koordinaci, sdílení informací, dekonflikci a mechanismus utváření shody. V rámci MO a ozbrojených sil pak **systém velení** a řízení, a odborného řízení integrovaný a plně kompatibilní se standardním systémem velení a řízení.

V neposlední řadě musí být nastavený systém schopen mezinárodní spolupráce, plnění závazků a vzájemné pomoci. Propojený kybernetický prostor s někdy velmi obtížně rozpoznatelnými hranicemi a vymezením rozsahu působností není možné zabezpečit bez vysoké míry mezinárodní spolupráce, interoperability a sdílení informací.

Ochrana (Protect).

Rezort obrany musí být schopen zabezpečit:

- ochranu jednotlivce v kybernetickém prostoru,
- operační bezpečnost,
- kontrarozvědnou ochranu,
- klamání v kybernetickém prostoru,
- bezpečnost dodavatelského řetězce.

Ochrana vojsk v kybernetickém prostoru začíná od **ochrany jednotlivce** a jeho identity, lokalizace a příslušnosti k ozbrojeným silám v průběhu plnění úkolu. Sdílení informací o sobě na sociálních sítích, vědomě či nevědomě lze využít k plánování a vedení operací a cílených kampaní. Všechna opatření a aktivity musí směřovat k zachování **operační bezpečnosti** a přispívat k plnění úkolů. Součástí zabezpečení je i **kontrarozvědná ochrana**. Digitální stopa nebo její absence, kterou jednotlivec či organizace zanechává, sebou nese mnoho operačně využitelných informací. „Radiový klid“ nemusí být nejlepším řešením, naopak lze kybernetický prostor využít pro **klamné operace** s cílem narušit vnímání a rozhodování protivníka a přinutit ho jednat v jeho neprospěch.

Dále je pro ochranu vojsk nezbytné zabezpečit **bezpečný dodavatelský řetězec**, s přihlédnutím k požadavkům na zajištění kybernetické bezpečnosti. Je třeba eliminovat rizika kompromitace nejen kybernetických nástrojů, ale i veškeré „připojitelné“ techniky a zařízení.

Informační zabezpečení (Inform).

Rezort obrany musí být schopen provádět:

- zpravodajské zabezpečení – operační a taktické,
- zpravodajské zabezpečení – strategické,
- sdílení informací.

Zpravodajské kybernetické operace zaměřené na sběr informací o kybernetickém prostoru nebo jeho prostřednictvím o fyzických doménách a informačním prostředí. Informace slouží k doplnění společného obrazu o situaci v rámci všezdrojové fúze a také samozřejmě pro vlastní činnost v rámci kybernetického prostoru.

Zpravodajské úkoly několika úrovní kopírují standardní rozdělení zpravodajských úkolů. Informace z kybernetického prostoru pro potřeby **strategického zpravodajství**, které poskytuje informace pro strategické rozhodování státu, dlouhodobé analýzy a trendy. **Operační zpravodajství** poskytující informace pro vedení operací na operačním stupni, především pro zpravodajskou přípravu operačního prostoru. Na nejnižším stupni pak vedení **taktického zpravodajství** poskytující informace pro vlastní plnění taktických úkolů a zpravodajskou přípravu bojiště. V kybernetickém prostoru se často činnosti spojené se ziskem informací budou značně prolínat, techniky používané v rámci taktické činnosti budou stejné jako pro případ strategické úrovně. Rozdíl je tedy v cíli a účelu sběru informací, ne v názvu a používaných metodách. Dostatečně robustní struktury a jejich integrace jsou nutné na všech úrovních.

Sdílení informací o hrozbách a postupech jejich řešení je zvláště v kybernetickém prostoru významnou součástí. Bez systému, který najde rovnováhu mezi bezpečností a nutností součinnosti bude docházet k duplicitám a mezerám v obraně.

NÁVRH ŘEŠENÍ

Úroveň České republiky – použití kybernetické obrany

Navrhované řešení představuje dotvoření systému řízení, koordinace a kontroly na úrovni státu v případě použití sil a prostředků kybernetické obrany. Řešení vychází ze standardního zákony vymezeného systému použití sil a prostředků ozbrojených sil, částečně modifikovaného pro potřeby čelit hybridním hrozbám a nutnosti zvýšit akceschopnost obranného systému.

V tabulce č. 3 je možné na levé straně vidět základní charakteristiky současného stavu a možností použít ozbrojené síly v rámci zajištění vnitřní a vnější bezpečnosti, na pravé straně pak navrhované začlenění jednotlivých typů operací v kybernetickém prostoru do současného stavu, možné řešení při nasazení mimo území ČR a také na území ČR bez vyhlašování jednotlivých stavů.

<table>
<tr><td colspan="4" rowspan="2">Současný stav</td><td colspan="2">Návrh</td></tr>
<tr><td>v rámci vyhlašovaných stavů</td><td>mimo území ČR, bez vyhlašování stavů</td></tr>
<tr><td>Právní předpis</td><td>Stav</td><td>Kdo rozhoduje</td><td>Ozbrojené síly z.219/1999</td><td>Kybernetické schopnosti</td><td>Kdo rozhoduje</td></tr>
<tr><td>Ústava ČR</td><td>Válečný</td><td>Parlament</td><td rowspan="2">Obrané úkoly</td><td rowspan="2">Ofenzivní kybernetické operace</td><td rowspan="2">Vláda rozhoduje, parlament může zrušit</td></tr>
<tr><td rowspan="2">ú.z. 110/1999</td><td>Ohrožení státu</td><td>Parlament na návrh vlády</td></tr>
<tr><td>Nouzový</td><td>Vláda</td><td rowspan="3">Plnění úkolů pro zajištění vnitřní bezpečnosti dle rozhodnutí vlády (odkaz)</td><td rowspan="2">Defenzivní kybernetické operace

Odolnost (Kybernetická bezpečnost)</td><td rowspan="2">Vláda</td></tr>
<tr><td>z. 240/2000
z. 181/2014

Právní řád</td><td>Nebezpečí

Běžný život</td><td>Hejtman

Ředitel NBÚ</td></tr>
</table>

Tabulka č. 3: Návrh použití kybernetické obrany a právní rámec

Navrhované řešení v **rámci vyhlašovaných stavů.** V běžném životě platí právní řád. V případě stupňujícího ohrožení v kybernetickém prostoru ředitel Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) vyhlašuje stav kybernetického nebezpečí.[25] Z rozhodnutí vlády je již v této fázi možné omezené vedení defenzivních kybernetických operací. Při eskalaci a rostoucí intenzitě nelze ohrožení odvrátit, a tak ředitel NÚKIB žádá vládu o vyhlášení nouzového stavu a nasazení prostředků obrany. Vláda vyhlašuje nouzový stav a v jeho rámci vydává i úkoly k vedení defenzivních kybernetických operací k obraně v kybernetickém prostoru. V případě vyhlášení stavu ohrožení státu a válečného stavu je pak již možno použít veškeré prostředky pro vedení obrany v kybernetickém prostoru.

25 *Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony*. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=38257.

Popis navrhovaného řešení při působení mimo území ČR a **na území ČR bez vyhlašování stavů.** Řešení je v duchu návrhu novelizace článku 43, Ústavy ČR, kde se uvažuje vládě svěřit pravomoc rozhodnout o použití sil a prostředků ozbrojených sil mimo území ČR do 60 dnů bez dalšího omezení[26], zůstává povinnost neprodleně informovat Parlament a dát Parlamentu právo toto rozhodnutí zrušit. Tento návrh je veden nutností zvýšit akceschopnost ozbrojených sil a možností ochrany národních zájmů. Obdobně lze použít i na působení v kybernetickém prostoru. Specifikem kybernetického prostoru jsou těžko rozeznatelné hranice států. Pokud bude hrozba nebo cíl zcela jasně mimo území,[27] je členění jednoduché a lze aplikovat článek 43. V současném znění však nebude možno využít plně možností, které působení v kybernetickém prostoru poskytuje.

Pro efektivní vedení kybernetických operací je nezbytně nutné svěřit vládě pravomoc rozhodnout o jejich použití. V případě defenzivních operací bez dalšího omezení. Pro ofenzivní operace je již nutností vytvořit kontrolní mechanismus. Operace, jejímž primárním cílem je aktivní aplikace síly, tedy ničení infrastruktury, komunikačních tras, dat a informací nebo poškození, manipulace a změny dat, již mohou představovat velmi silné porušení mezinárodního práva, nebo poškození práv občanů v České republice. Jedna možnost je řešení odpovídající článku 43, kdy kontrolující prvek je Parlament nebo jím ustavený permanentní prvek. Další možností je dát pravomoc prvku v rámci soudní moci, obdobně jako v jiných případech narušování práv občanů.

V obou případech je nutné dopracovat **systém řízení** a **koordinace mezi prvky kybernetické bezpečnosti** a **kybernetické obrany** v okamžiku zapojení obou složek do aktivní činnosti v rámci kybernetické prostoru v ČR. V rámci vyhlašování stavu nebezpečí a nouzového stavu vláda při rozhodnutí nasazení sil a prostředků kybernetické obrany musí také rozhodnout, kdo bude mít zodpovědnost za celkové řízení aktivit. Buď si tuto pravomoc ponechá, a v tomto případě je nutné mít prvek na úrovni vlády, který bude tyto aktivity řídit a koordinovat, nebo přenese pravomoc rozhodovat, řídit a koordinovat na jednu ze složek působících v kyberprostoru. Všechny tyto varianty by se měly analyzovat, procvičit a vyhodnotit a poté stanovit pomocná kritéria pro hodnocení vhodnosti využití modelu v různých situacích.

V případě stavu ohrožení státu nebo válečného stavu jsou prostředky kybernetické bezpečnosti podřízeny řízení obrany. Proto se musí v rámci kybernetické obrany vyvinout systém řízení a koordinace všech nástrojů v kybernetickém prostoru, nutný pro dosažení společných účinků při vedení obrany v kyberprostoru. Tento systém musí být samozřejmě provázaný s celým systémem velení a řízení v rámci obrany ČR.

---

26 *Ústavní zákon č. 1/1993 Sb., Ústava České republiky*. In: Praha: Poslanecká sněmovna parlamentu České republiky, 1993, ročník 1993, číslo 1. Dostupné také z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=40450&fulltext=&nr=1~2F1993&part=&name=&rpp=15

27 Role orgánů pro kybernetickou bezpečnost bude v tomto případě minimální.

Úroveň Ministerstva obrany – propojení kybernetické bezpečnosti a obrany

Na úrovni MO pokrývá návrh rezortní strategie a související akční plán většinu identifikovaných požadovaných schopností. Jistým slabým místem je do velké míry oddělené budování a řízení kybernetické bezpečnosti a kybernetické obrany.

Řešením je více propojit na strategické a operační úrovni oba koncepty. Dělat kybernetickou obranu bez zajištění základu kybernetické bezpečnosti, tedy odolnosti infrastruktury a bezpečnosti informací nedává velký smysl. Naopak bezpečnost bez obrany nebude kompletní a v některých situacích by tak chyběly nástroje pro řešení situace. V Tabulce č. 4 je vidět navrhovaná struktura rolí v obou konceptech, rozdělení schopností pro vlastní plnění úkolů a integrace v rámci rezortu.

	Rada pro kybernetickou bezpečnost MO		
	Vojenské zpravodajství	AČR	Odbor bezpečnosti MO
Role v KB	Výkonná	Výkonná	Gestor, koncepční a normotvorná
Role v KO	Gestor, koncepční a normotvorná, výkonná	Výkonná	Integrující
Schopnosti	Strategické zpravodajství	Operační a taktické zpravodajství	
	Kybernetické operace	Integrace do operací	
		Informační operace v kybernetickém prostoru	
	Odolnost a bezpečnost informací vlastní IS	Odolnost a bezpečnost informací vlastních a rezortních IS	

Tabulka č. 4: Systémové uspořádání kybernetické bezpečnosti a kybernetické obrany

Rada pro kybernetickou bezpečnost MO je poradním orgánem ministra, a řídícím a koordinačním prvkem pro oblast kybernetické bezpečnosti. V rámci návrhu by se do její působnosti zahrnula i kybernetická obrana pro zvýšení synergie a zajištění provázanosti opatření. V kybernetické obraně by měl Odbor bezpečnosti Ministerstva obrany (OB MO) jako gestor širšího konceptu[28] integrující roli do zajišťování kybernetické bezpečnosti.

V rámci zajišťování kybernetické bezpečnosti je gestorem OB MO. Zodpovídá za koncepční a metodické řízení zajišťování kybernetické bezpečnosti. Stanovuje normy a standardy ve své oblasti. Spolupracuje s Národní autoritou pro KB a v rámci mezinárodních organizací. V rámci rezortu odborně řídí osvětu a vzdělávání, výzkum a vývoj, a spolupráci s průmyslem v oblasti zajišťování kybernetické bezpečnosti.

Vojenské zpravodajství (VZ) musí v rámci kybernetické obrany ČR[29], naplňovat všechny role. VZ je gestorem zodpovědným za oblast kybernetické obrany ČR, kterou koncepč-

28 Jako gestor širšího konceptu.

29 Zde je nutno zmínit rozdílné chápání pojmu kybernetická obrana mezi VZ a AČR, viz ref. 2.

ně a metodicky řídí. Zároveň ale buduje své síly a prostředky pro vedení kybernetické obrany.

Vojenské zpravodajství musí být schopno získávat strategické informace z kybernetického prostoru a o kybernetickém prostoru, ochránit své vlastní sítě a vést kybernetické operace. Kybernetické operace (defenzivní a ofenzivní) musí být schopno vést samostatně na národní úrovni, nebo ve prospěch operací AČR.

AČR má jak v zajišťování kybernetické bezpečnosti, tak obrany z pohledu rezortu výkonnou roli. AČR musí být schopna zabezpečit své i určené rezortní informační sítě a kritickou infrastrukturu. Pro vedení operací pak získávat vlastní informace z a o kyberprostoru. Armáda musí být schopna v součinnosti s VZ integrovat kybernetické operace prováděné VZ do plánování a vedení operací. V neposlední řadě pak vybudovat schopnost vést informační operace i v kybernetické doméně.

Kybernetický prostor je výraznou částí informačního prostředí a propojenost vedení operací je nutností. Na strategické úrovni je vhodné ponechat informační působení odděleně.[30] Na operační však již musí být zahrnuty kybernetické operace do prostředků, které mohou provádět vojenské informační aktivity, a naopak například psychologické operace musí rozvinout a integrovat i své schopnosti v kybernetickém prostoru jako dalším prostředí.

Úroveň Armády České republiky – výkon kybernetické bezpečnosti a vedení společných operací v kybernetickém prostoru

Armáda se musí soustředit především na výkonnou část kybernetické bezpečnosti a integraci kybernetických schopností do vedení společných operací. Níže je návrh, co je třeba udělat v jednotlivých oblastech a jaké struktury je k zabezpečení plnění úkolů nutné vytvořit.

Informační operace v **kybernetickém prostoru.** Informační operace jsou v chápání NATO štábní koordinační funkce, při které se využívají různé schopnosti, nástroje či techniky.[31] Do používaných nástrojů v rámci AČR tak bude nutné zahrnout i kybernetické operace.[32] Ostatní nástroje bude nutné připravit a přizpůsobit i pro působení v kybernetickém prostoru. Například psychologické operace, klamání nebo operační bezpečnost mají v kybernetickém prostoru svá specifika. Kybernetický prostor je významnou částí informačního prostředí a jeho význam a podíl na vůli, porozumění a vliv lidí neustále roste a AČR se tomuto trendu musí přizpůsobit. Výzkum a vývoj efektivních metod informačního působení, odhalování nepřátelského působení a zvyšování vlastní odolnosti si vyžádá úzkou spolupráci s civilními univerzitami a výzkumnými pracovišti. K tomu je třeba přizpůsobit i možnosti využití výzkumných grantů v této oblasti.

Operační a **taktické zpravodajství**. V rámci Zpravodajského zabezpečení AČR vytvořit potřebné schopnosti pro získávání informací z kybernetického prostoru na operační a taktické úrovni. V rámci armádních zpravodajských úkolů by se jednalo především o:

- schopnosti v rámci zpravodajství z otevřených zdrojů,

30 Viz ŘEHKA, Karel. *Strategická komunikace a informační operace v resortu MO ČR*, s. 41-49.

31 *MC 0422/5. NATO Military Policy for Information Operations. Brussels: NATO Military Committee*.

32 V pojetí NATO již začleněny.

- rozvoj a začlenění vhodných nástrojů pro analýzu informací,
- využívání pokročilých metod práce s daty a informacemi,
- sledování a vyhodnocování otevřených zdrojů především sociálních sítí,
- geolokace pohybu,
- to vše bez překonávání zabezpečení. Schopnost překonávat zabezpečení pro vedení operací by měla být poskytována v rámci podpory od Vojenského zpravodajství. Informace z a o kybernetickém prostoru se musí stát součástí společného operačního obrazu (COP).

Integrace kybernetických operací do vedení společných operací. Dle rozdělení působností v kybernetickém prostoru je schopnost vedení kybernetické obrany (v rámci kybernetických operací) přidělena VZ. VZ podporuje operace sil v zahraničí již nyní. Poskytuje informace a specifické schopnosti v rámci National Intelligence Cell (NIC) a National Intelligence Support Team (NIST) nebo jednotlivce v rámci úkolových uskupení. Pro potřeby operací je možné poskytovat stejným způsobem.

VZ musí vybudovat schopnosti nasaditelné v rámci úkolových uskupení, tj. týmy umožňující vedení kybernetických operací na odborné úrovni[33] a zároveň jejich integraci do společných operací, tedy plánování a řízení.[34] Pro efektivní vedení operací v kyberprostoru v rámci integrovaných společných operací je zároveň nezbytnou podmínkou společný výcvik a pochopení možností[35] v kybernetickém prostoru veliteli a štáby.[36]

Odolnost a **bezpečnost informací vlastních** a **rezortních informačních systémů**. Jak již je zmíněno výše, schopnost chránit své vlastní infrastrukturní sítě je na koncepční úrovni dobře zpracována. Je třeba „jen" naplnit záměry v návrhu rezortní strategie kybernetické bezpečnosti, dobudovat technologické zabezpečení, mít dostatek odborníků, a hlavně **vzdělávat uživatele všech úrovní**.

U taktických jednotek je třeba vybudovat nasaditelnou část schopností, zajišťující odolnost a bezpečnost informací při působení v operacích a struktury implementující opatření kybernetické bezpečnosti do běžné činnosti vojsk.

NÁVRH MOŽNÝCH PRVKŮ

Pro zabezpečení úkolů spojených s výstavbou schopností je nutné vytvořit strukturu následujících prvků a jejich vzájemných vazeb. Na Obrázku 2 je možné vidět návrh prvků zabezpečující požadované schopnosti v rámci AČR, vycházející z aktuálního i navrhovaného rozdělení rolí a působností.

33 Využívající reachback podle potřeby.

34 Jsou potřeba jak operátoři-bojovníci (IT specialisté) tak lidé schopni naplánovat, řídit, a vysvětlit schopnosti a možnosti kybernetických operací pro vedení společných operací.

35 VZ bude muset sdílet všeobecné informace o svých schopnostech, samozřejmě v režimu utajení.

36 Pokud podmínky nebudou splněny, uvedený model rozdělení působností nebude pro AČR životaschopný a bude muset si své schopnosti vybudovat sama.

Prvky orámované plnou čárou již v rámci AČR existují a není potřeba zásadních změn. Systém sestávající se z koordinační a výkonné části CIRC, napojený na správce jednotlivých sítí je vhodný model pro zajištění infrastrukturní bezpečnosti. Tyto prvky však komplexně nezajistí vedení operací v kybernetickém prostoru. V souladu s návrhem na požadované schopnosti je nutné vytvořit prvky označené orámováním přerušovanou čárou.

Koncepční a řídící orgán v rámci AČR, zaštiťující oblast KB a KO. Vhodným umístěním je v dnešní situaci odbor KIS Sekce podpory MO, tedy nejvyšší koncepční orgán v rámci spojovacího vojska.

Strukturu orgánu v rámci jednotlivých taktických stupňů velení specificky se zaměřujících na implementaci a integraci pohledu kybernetické bezpečnosti do každodenního života jednotek, a především vedení operací. Jejich začlenění je podle autorů nejvhodnější v rámci spojovacích skupin, oddělení a odborů.

Nasaditelná odolnost by měla být vytvořena a začleněna v rámci jednotky, která konkrétní informační systém zajišťuje.

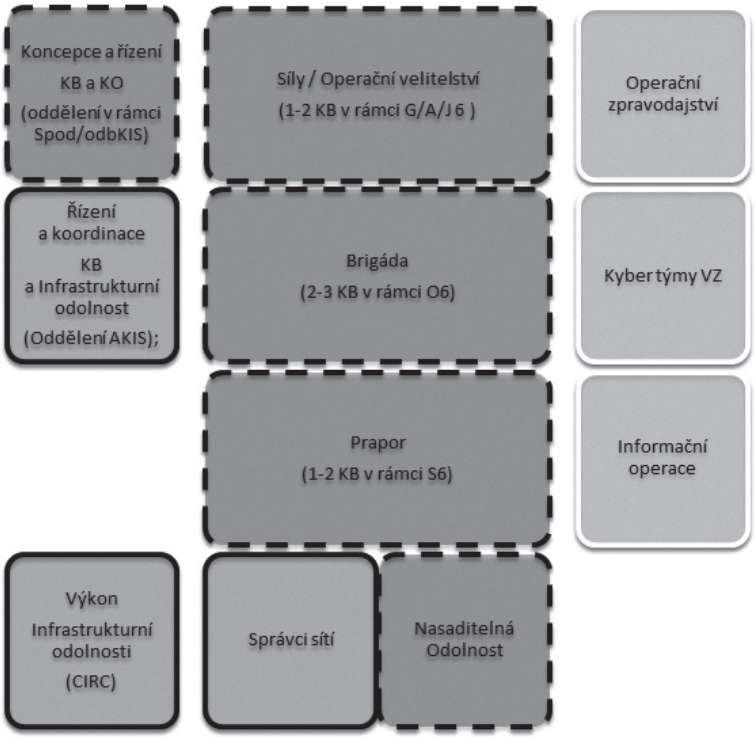
Doporučujeme ponechat či přidělit oblast KB a KO spojovacímu vojsku. V současnosti není ještě mnoho důvodů (na koncepční úrovni) oddělit v rámci AČR zabezpečení komunikační a informační podpory od zajištění KB a vedení KO. Největším problémem je celkové oddělení současné kultury spojovacího vojska od vedení operací. Neexistence operačního stupně, neprobíhající výcvik vede k důrazu na infrastrukturní (rezortní) problematiku. Vše ostatní je řešeno nevhodným způsobem. Místo aktivní práce a předkládání návrhů řešení problémů operačního stupně ze svého odborného pohledu se čeká na zaslání požadavku. Pokud se nevhodné nastavení nezmění, bude nutné vytvořit v rámci Sekce rozvoje a plánování schopností MO (SRPS MO) i část koncepčního orgánu zabývajícího se KB a KO z pohledu operací. V tomto případě bude ale také nutné vyčlenit i část odborných a koncepčních kapacit spojovacího vojska.

Operační zpravodajství, kybernetické týmy VZ a informační operace jsou rozebrány výše a je nutné je integrovat do vedení operací, s jednotným velením, cílem a pro vytváření společných účinků.

ZÁVĚR

Článek se zabývá problematikou zabezpečení bezpečnosti a obrany v kybernetickém prostoru s důrazem na Ministerstvo obrany a ozbrojené síly. Navazuje na dříve provedenou analýzu požadovaných schopností kybernetické obrany. Snahou autorů bylo definovat, jakými schopnostmi by měl rezort obrany disponovat a jak rozdělit role, odpovědnosti a požadované schopnosti. Návrh se soustředí na kvalitativní část schopností, tedy co je nutné vytvořit, splnit, být schopen.

Dále jsou řešeny jednotlivé problémy a bílá místa současného uspořádání kybernetické bezpečnosti a kybernetické obrany na úrovních ČR, rezortu obrany a AČR tak, aby navrhované řešení umožnilo komplexní a systémové řešení zajišťování bezpečnosti a obrany v kybernetickém prostoru. Návrhy doplňují státní a rezortní uspořádání v případě, pokud řešení neexistuje, či je podle autorů problematické nebo nedostatečně rozpracované.



Obrázek č. 2: Návrh prvků KB a KO v rámci AČR

Předložené řešení není autory chápáno jako jediné možné, ale zabezpečí požadované schopnost vyplývající z úkolů, které rezort MO musí plnit.

Článek je zaměřen na koncepční a doktrinální uspořádání problematiky. K zajištění bezpečnosti a obrany v kybernetickém prostoru ovšem nestačí pouze naplnit navrhovaná řešení, ale je nutné splnit mnoho dalších cílů stanovených v rezortní strategii a akčním plánu. Kvantitativní stránka požadovaných schopností a bude muset být předmětem další analýzy zejména v oblasti aktivního působení, které předpokládá informace o segmentu kyberprostoru, ve kterém chceme působit, znalost zranitelností, schopnost jejího využití a schopnost doručení kybernetické zbraně. Všechny tyto schopnosti jsou náročné na lidské, finanční i materiální zdroje.

Kybernetický prostor se pro vojáky stal doménou, působení v něm není otázkou volby, ale nutností. Aktivní působení v kybernetickém prostoru je v rámci rezortu obrany a AČR zcela novou oblastí. Hledání a vývoj koncepcí použití, operačních a taktických postupů a procedur a samozřejmě i vzdělávání vojáků všech stupňů bude vyžadovat velké úsilí.

O autorech: ***Plk. gšt. Ing. Miroslav Feix, M.S.,*** *narozen 1974. Je absolventem VVŠ PV ve Vyškově a Naval Postgraduate School v Monterey, CA, USA. Působil na různých velitelských a štábních funkcích u Speciálních sil. V současné době pracuje na Ředitelství speciálních sil v oblasti koncepcí a strategií, ve funkci zástupce ředitele speciálních sil Armády České republiky.*

RNDr. Dalibor Procházka, CSc., (pplk. v z.), *narozen v roce 1962. V roce 1986 ukončil Fakultu numerické matematiky a kybernetiky Moskevské státní univerzity. V letech 1987–1995 působil jako odborný asistent na katedře Technické kybernetiky a vojenské robotiky Vojenské akademie v Brně, v letech 1995–1997 se zabýval školící a projektovou činností na informačním systému logistiky. Od r. 1998 do roku 2005 se podílel na výzkumu a zavádění prostředků modelování a simulace pro potřeby výcviku a vzdělávání do AČR, v letech 2000–2005 jako velitel Centra simulačních a trenažérových technologií, v letech 2006–2009 jako projektový manažer ve společnosti VR Group, a.s. V letech 2011–2013 se v rámci Sekce obranné politiky a strategie Ministerstva obrany věnoval oblasti informačních systémů, zejména kybernetické obraně. Od června 2013 pracuje jako odborný asistent Centra bezpečnostních a vojenskostrategických studií UO. Zabývá se problematikou modelování a simulace a kybernetické obrany.*

Jak citovat: FEIX, Miroslav a PROCHÁZKA, Dalibor. Zajištění požadovaných schopností kybernetické obrany. *Vojenské rozhledy*. 2017, 26 (4), 35-54. DOI: 10.3849/2336-2995.26.2017.04.035-054. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz