Informace

Příčiny vzniku a začlenění kybernetických sil a informačních operací do Armády České republiky

Reasons of formation and integration of cyber forces and information operations into the Army of the Czech Republic

Martin Havlík

Abstrakt: Cílem tohoto informativního článku je komplexně popsat příčiny vzniku a začlenění kybernetických sil a informačních operací do struktury Armády České republiky, včetně dalších významných konotací. Záměrem není prezentovat nové vědecké poznatky, ale poukázat na smysl existence kybernetických sil a informačních operací, jako nutné separátní složky Armády České republiky schopné reakce na dynamický vývoj bezpečnostního prostředí a neutichající rozvoj moderních technologií. Obsah a hlavní argumenty tohoto článku reflektují přechod od klasické formy válčení k platformě nové, reprezentované zejména kybernetickým prostorem a hybridní kombinací široké škály nástrojů moci s důrazem na informační operace.

Abstract: The goal of this informative article is to comprehensively describe the causes of the formation and integration of cyber forces and information operations into the structure of the Army of the Czech Republic, including other significant connotations. The intention is not to present new scientific findings, but to point out the meaning of the existence of cybernetics and information operations as a necessary separate component of the Army of the Czech Republic capable of responding to the dynamic development of the security environment and the continuous development of modern technologies. The content and main arguments of this article reflect the transition from the classical form of warfare to the new platform, represented mainly by cyber space and a hybrid combination of a wide range of power tools with an emphasis on information operations.

Klíčová slova: Bezpečnost; operace; moderní technologie; multidoménový boj.

Keywords: Security; Operation; Modern Technology; Multi-Domain Battle.

ÚVOD

Informativní článek zaměřený na integraci kybernetických sil a informačních operací do struktury Armády České republiky (AČR) je určen pro vojenské publikum v rámci České republiky, českou odbornou bezpečnostní komunitu i širokou veřejnost jakožto nástroj osvěty a potřeby reflektovat význam kybernetického prostředí v současném světě. Řešená problematika koresponduje s aktuálním rámcem výstavby a rozvoje schopností AČR, který je doktrinálně ukotven v příslušných koncepčních dokumentech AČR a rezortu ministerstva obrany České republiky.

V úvodu je nutné si uvědomit, že samotné výsledky, přínos a efektivitu popisované integrace nových kyberneticky orientovaných schopností do AČR bude možné expertně posoudit až s odstupem několika let či dekád. Metodologický přístup k tomuto článku je interpretativního typu, který je pro výklad a objasnění tématu užitečnější, než například teorie a výzkumný přístup explanační.

Na úvod je vhodné zmínit také limitující podmínky a základní východiska, jež reálně omezují hloubku interpretovaných faktů a argumentů. Jde především o celkový rozsah a předem definovaný strukturální rámec informativního článku, které omezují obsahovou zevrubnost, včetně hloubky provedených rozborů vztahujících se k hlavním argumentům a ukazatelům. Mimo uvedené omezení je nutné brát v potaz citlivost samotného tématu ve vztahu k unikátním vojenským schopnostem a ochraně souvisejících utajovaných informací.

Deskripce jednotlivých kapitol kopíruje z pohledu autora záměrně realistické vymezení bezpečnosti, které obecně zdůrazňuje, že si jednotliví státní aktéři musí zajistit svou bezpečnost vlastními silami (tedy schopnostmi, případně i kumulací moci), kdy dochází logicky k nárůstu vyzbrojování, posilování a modernizaci armády (a dalších bezpečnostních subjektů) a uzavírání případných dohod s dalšími aktéry (ve smyslu bilaterálních či multilaterálních dohod[1]). Celý obsahový kontext článku reflektuje vlastní lokaci autora, kdy pohled na zkoumanou problematiku je typu „insider".[2]

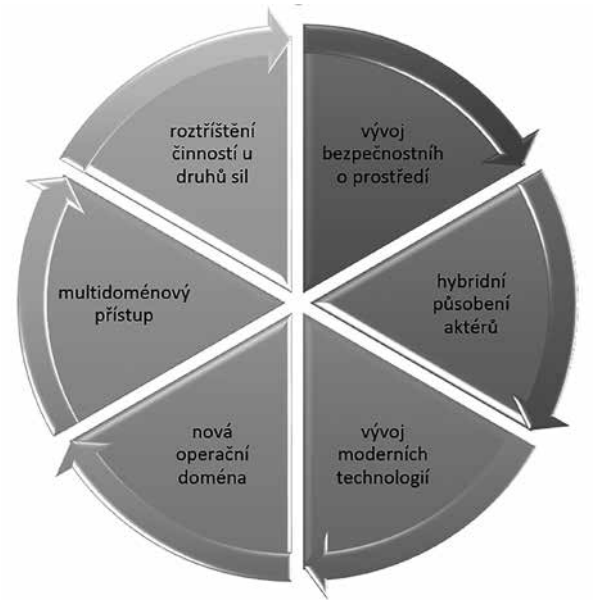
1 PŘÍČINY VZNIKU KYBERNETICKÝCH SIL A INFORMAČNÍCH OPERACÍ V AČR

Vznik kybernetických sil a informačních operací byl v uplynulých letech iniciován a determinován několika významnými faktory (konkrétně viz následující obrázek), které

1 Například spolupráce v rámci OSN (Organizace spojených národů), NATO (North Atlantic Treaty Organization), EU (European Union) či V4 (Visegrádská čtyřka).

2 Pohled typu „insider" lze obecně chápat tak, že se autor článku (studie, kvalifikační práce apod.) pohybuje přímo v dané oblasti zájmu, případně v konkrétním regionu, jde-li například o specifickou regionální analýzu zaměřenou na vybraného státního aktéra.

mají majoritně nadnárodní globální rozměr (až na roztříštěnost či decentralizaci kybernetických a informačních činností u jednotlivých druhů sil v rámci AČR). Mimo uvedené je vhodné zdůraznit, že některými schopnostmi ze spektra informačních operací v kybernetickém prostoru AČR vůbec nedisponovala. V této kapitole bude dále jednotlivým faktorům (těm nejvýznamnějším) věnována bližší pozornost s cílem osvětlení vážnosti a implikací, které následně vedly ke vzniku kybernetických sil a informačních operací, jakožto nedílné a samostatné součásti AČR.



Obrázek č. 1: Hlavní příčiny vzniku kybernetických sil a informačních operací v AČR

1.1 Změna a dynamický vývoj bezpečnostního prostředí (strategického i operačního), a to nejen v kontextu aktuální situace v Evropě, Africe či na Blízkém a středním východě ve vztahu k migrační krizi a související hrozbě teroristických útoků

Strategické prostředí zahrnuje mezinárodní vztahy a je charakterizované celosvětově, a to většinou na základě bezpečnostních hrozeb (mezinárodní terorismus, neschopnost vlád spravovat území vedoucí až ke zhroucení státu, šíření zbraní hromadného ničení, mezinárodní organizovaný zločin, místní či regionální etnické a teritoriální konflikty, humanitární krize jako důsledek ozbrojených konfliktů, nevratné změny životního prostředí, přírodní katastrofy, průmyslové havárie a pandemie). Strategické prostředí je nadále charakterizováno vysokou dynamikou změn, rostoucí různorodostí aktérů a stále složitější

provázaností bezpečnostních trendů a faktorů. Hrozby, rizika a jejich zdroje jsou mnohdy obtížně lokalizovatelné a nyní mají převážně nestátní a nadnárodní charakter.[3],[4]

Operační prostředí je tvořeno souborem činitelů, okolností a vlivů, jež určují konkrétní podmínky, ve kterých bude prostřednictvím vojenské operace dosahováno stanovených cílů. Patří sem mimo jiné terén, klimatické a povětrnostní podmínky, charakter státu, sociální demografie, regionální a mezinárodní vztahy, vojenské schopnosti všech stran konfliktu, informační situace, technologie, externí (nevojenské, nevládní) organizace zúčastněné v prostoru operace, národní zájmy všech zúčastněných stran, čas, ekonomika v dané oblasti a další vlivy. Operační prostředí, ve kterém jsou nebo budou ozbrojené síly nasazeny, ovlivňuje způsob vedení operací na všech stupních velení a řízení. Pochopení operačního prostředí a jeho součástí v politické, ekonomické, vojenské, sociální, bezpečnostní a informační oblasti a stavu infrastruktury je klíčovým faktorem pro dosažení cílů operace. Informační procesy, včetně zpravodajského zabezpečení či kybernetické ochrany, musí být schopny identifikovat hrozby vůči záměrům dosažení stanovených cílů a bezpečnosti vlastních sil ve všech fázích operace bez ohledu na to, v jak složitém prostředí budou vojenské síly operovat.[5],[6]

Výše uvedené vymezení strategického a operačního prostředí a zejména jejich nedávný vývoj generovaly potřebu reagovat na změny ve způsobech prosazování zájmů státních i nestátních aktérů. V této souvislosti se napříč českou bezpečnostní komunitou stále více akcentovala otázka významu či dopadu kybernetických útoků. Mimo armádní oblast, kde se kybernetické problematice v omezené míře věnovalo Centrum CIRC[7] pod AKIS (Agentura komunikačních a informačních systémů), se uvnitř rezortu obrany ČR problematikou kybernetické bezpečnosti, obrany a ochrany začaly intenzivněji zabývat také Vojenské zpravodajství a Odbor bezpečnosti Ministerstva obrany. Dílčími schopnostmi vést informační operace pak disponovaly Speciální síly a také 103. centrum CIMIC/PSYOPS v podřízenosti Pozemních sil AČR.

1.2 Nárůst hybridního působení, aktivit a hrozeb státních i nestátních aktérů s využitím kybernetického prostoru a informačních nástrojů

V kontextu vývoje bezpečnostního prostředí je vhodné dodat, že v současné době existuje pro společnost (v globálním i regionálním pohledu) mnoho odlišných a aktuálních hrozeb, u nichž je nejistá pravděpodobnost a velmi nízká předvídatelnost. Jakákoliv

3 MINISTERSTVO OBRANY ČR. Odbor komunikace a propagace MO. *Bílá kniha o obraně.* Praha, Ministerstvo obrany ČR, 2011. ISBN 978-80-7278-564-3. Str. 168.

4 KOVÁŘ, František, KRCHOVÁ, Hana. *Strategický management.* 1. vydání. Praha: Vysoká škola ekonomie a managementu, 2006. ISBN 978-80-86730-29-5. Str. 178.

5 JANÁČ, Karel. *Zpravodajství z lidských zdrojů na operačním a taktickém stupni v podmínkách AČR.* 2011, Vyškov: Správa doktrín ŘeVD.

6 *Doktrína AČR v mnohonárodních operacích.* 2008, 1. vyd. Vyškov: Správa doktrín ŘeVD. Str. 144.

7 CIRC (Computer Incident Response Capability) reprezentuje schopnost reakce na počítačové incidenty.

forma odstrašování není v současné době již plně relevantní a příslušné vojenské strategie musí být proto sestaveny tak, aby byly připraveny na nejistotu a šok. Tyto skutečnosti mají velmi významný dopad také na hodnocení a predikci vývoje bezpečnostní situace v celosvětovém měřítku, a to z pohledu akademických, politických, vojenských či zpravodajských subjektů.[8] Nejvíce je v posledních pěti letech skloňován význam takzvaného hybridního působení a hybridních hrozeb státních i nestátních (případně také proxy-státních) aktérů, jež preferují použití nekonvenčních nástrojů moci s velmi zásadním a stále intenzivnějším využíváním kybernetického prostoru. V této souvislosti lze kybernetické prostředí efektivně využít k prosazení nejrůznějších zájmů. V oblasti obrany je proto zapotřebí alternativně rozvíjet bezpečnostní, obranné a ochranné mechanismy a procesy, které by byly schopny detekovat, identifikovat, analyzovat, ochránit či zabezpečit vlastní kybernetický prostor a k němu afilovanou kritickou infrastrukturu (a všechny související referenční objekty či chceme-li aktiva). Je proto logické, že ani AČR nemohla v této souvislosti zůstat stranou a nereagovat na evidentní bezpečnostní hrozby a výzvy.

1.3 Neustálý vývoj a s ním spojená široká implementace moderních technologií (včetně umělé inteligence, IoT – Internet of Things, nanotechnologií či autonomních robotických systémů apod.) v komerční sféře i vojenském segmentu potenciálních protivníků

Pokud budeme chtít reflektovat dlouhodobé, střednědobé i aktuální (krátkodobé) požadavky vládních autorit zakomponované v bezpečnostní i zahraniční politice s ohledem na působení proti potencionálním hrozbám, bude potřeba, aby jednotlivé subjekty podílející se na obraně proti hrozbám včasně a nepřetržitě reagovaly na okolní prostředí, jež se velmi dynamicky mění. Na základě těchto předpokladů je důležité, aby se, jak jednotlivé složky ozbrojených sil, tak i dalších státních subjekty (včetně zpravodajských institucí) a integrovaného záchranného systému kontinuálně přizpůsobovaly novým trendům a metodám s využitím nejmodernějších technologií.

Trvalým úkolem Armády České republiky je připravovat se k obraně země a bránit ji proti vnějšímu napadení a zároveň se připravovat k zapojení do obrany v rámci systému kolektivní obrany NATO. Armáda musí disponovat schopnostmi pro naplnění politicko-vojenských ambicí České republiky[9] a dalších úkolů a závazků. Předpokládaný vývoj bezpečnostního prostředí a záměr použití armády vyžaduje, aby byly rovnoměrně rozvíjeny všechny požadované schopnosti (včetně kybernetické ochrany a aktivního informačního působení v kybernetickém prostoru). Zde nepopiratelnou roli hrají i kybernetické síly a široké spektrum souvisejících informačních operací.

8 HAVLÍK, Martin. *Fenomén Big Data jako trend ovlivňující technické zpravodajské disciplíny.* Brno - Vojenské rozhledy, 2014, roč. 23 (55), č. 4. ISSN 1210-3292. Str. 124 – 132.

9 Usnesení vlády ČR ze dne 26. září 2012 č. 699 o Obranné strategii České republiky.

V souvislosti s masivním rozvojem moderních technologií v posledních letech narůstá také intenzita, počet a nebezpečnost samotných útoků na informační a komunikační infrastrukturu (obecně kritickou infrastrukturu). Do popředí se ve vojenské oblasti dostávají zejména prostředky pasivního monitoringu a sledování kybernetického prostoru, které poskytují nové výhody v získávání, analýze a distribuci tolik potřebných informací (často také zpravodajských informací) o prostoru zpravodajského zájmu z multidoménového pohledu. Je přínosné reflektovat to, že jak softwarové, tak i hardwarové prostředky by měly být vyvíjeny na modulárním základě z důvodu jejich efektivnějšího využití a všestranné výhodnosti při jejich budoucí modernizaci. Se zefektivňováním organizačních struktur úkolových uskupení v operacích lze očekávat další těsnější logické propojení zpravodajství, elektronického boje a informačních operací, a to zejména na operačním a taktickém stupni.

1.4 Akceptace kybernetického prostoru jako další (vedle pozemní, vzdušné, námořní a vesmírné[10]) operační domény NATO, a to konkrétně na summitu NATO ve Varšavě v roce 2016

Od konce Studené války do dnešních dnů je patrný vývoj v oblasti dimenzí (viz následující obrázek) ozbrojených konfliktů a také s tím souvisejících operací, který souvisí s přechodem od fyzické podoby válčiště k platformě mnohem více imaginární reprezentované zejména kybernetickým prostorem.

Obrázek č. 2: Uznané operační domény NATO od konce roku 2019

10 Vesmírná doména byla v rámci NATO akceptována až no konci roku 2019.

Přes uvedené skutečnosti však nelze tvrdit, že se jednotlivé strany současných a zcela jistě také budoucích konfliktů budou výhradně soustředit na válku v kybernetickém prostoru, ale budou využívat kombinaci všech pěti dimenzí. V oblasti vojenských (zejména zpravodajsky orientovaných) aktivit světových velmocí zaměřených na pronikání do strategických subjektů kritické infrastruktury (například průnik USA a Izraele do íránských zařízení pro obohacování uranu), získávání strategicky významných informací v oblasti průmyslové špionáže (zejména v případě Čínské lidové republiky), bude prostor kybernetický majoritním působištěm budoucích konfliktů a také širokého spektra bezpečnostních operací. Pokud budeme reflektovat současné trendy v oblasti vývoje a zaměření operací, lze poukázat na následující parametry, které strukturálně nejvíce charakterizují operace budoucnosti. Jedná se o:

- komplexní operace vedené ve všech pěti dimenzích (doménách);
- důraz na informační operace vedené v kybernetickém prostoru;
- komplexní rozměr operací v celém spektru možných konfliktů;
- vedení více souběžných operací na mnoha různých místech v globálním pohledu;
- vzrůstající operační tempo budoucích operací.[11]

1.5 Potřeba komplexního propojení všech operačních domén a multidoménový (multi-domain) přístup k efektivnímu plánování a vedení operací

V případě kybernetického prostoru jde vůbec o první doménu, která není jednoznačně ohraničena a široce se prolíná všemi ostatními operačními doménami (více viz následující obrázek). Naopak můžeme tvrdit, že kybernetický prostor zastřešuje a pokrývá všechny ostatní operační domény (i když například v případě vesmíru tomu tak není komplexně).[12] Efektivní působení v kybernetické doméně z pohledu AČR není zcela pochopitelně možné zabezpečit jinak, než záměrnou výstavbou nových, separátních a speciálně zaměřených prvků ve struktuře AČR disponujících adekvátními prostředky a schopnostmi.

Poměrně nový multidoménový přístup vyspělých armád musí reagovat na bezpečnostní výzvy a zejména na strukturu schopností a přístupy potenciálních protivníků. Je tedy žádoucí, aby armády „západní" společnosti byly schopné společným úsilím zvítězit v případné budoucí multidoménové válce, která bude reprezentována kombinací konvenčních zbraní (využívajících moderní technologie), elektronického boje, informačních operací v kybernetickém prostoru a také působení ve vesmíru. Multidoménové operace budoucnosti budou mnohem komplikovanější a náročnější ve vztahu k nasazeným silám a prostředkům. Cílem bude nadále minimalizovat rizika vlastního

11 HAVLÍK, Martin. *Vývoj operačního prostředí v kontextu budoucích konfliktů a směřování zpravodajské podpory*. Bezpečnostní teorie a praxe. 2015, č. 4. ISSN 1801-8211.

12 Vždy je nutné reflektovat prostor pokrytí jednotlivých domén dostupnými kybernetickými prostředky.

ohrožení a posilovat efektivitu při plnění náročných operačních požadavků. Zde (jakožto součást multidoménového boje) bude nezanedbatelnou (v budoucnu naopak klíčovou) roli hrát právě kybernetický prostor a informační operace v něm vedené.

Obrázek č. 3: Provázání kybernetické domény s ostatními operačními doménami

Některé zdroje uvádějí, že se díky pokroku především v síťových technologií budou postupně potírat rozdíly mezi jednotlivými operačními doménami v případě zmiňovaného multidoménového boje. Činnost v jedné doméně tedy obecně výrazně ovlivní situaci v další doméně. Letouny, pozemní protivzdušná obrana, prostředky aktivního kybernetického boje, vesmírné senzory a další vojenské systémy budou v multidoménovém boji vytvářet síťově propojený bojový systém, který v reálném čase povede koordinovanou bojovou činnost. Vojáci budou postupně čelit hrozbám ve všech doménách války, operacím v komplexních prostředích, hybridním strategiím a případně také zbraním hromadného ničení.[13],[14]

Americký TRADOC (Training and Doctrine Command) v poměrně zdařilém přehledovém dokumentu[15] definoval v této souvislosti celkem 12 stěžejních okruhů (vývojových trendů), které budou determinovat budoucí podobu, pojetí a rozměr moderní války.

Jedná se o:

---

13 AN – Armádní Noviny. *Bojiště budoucnosti 2050 podle americké armády.* [online]. 2017 [cit. 2020-03-20]. Dostupné z: https://www.armadninoviny.cz/bojiste-2050-americka-armada-se-pripravuje-pro-bojiste.html

14 AN – Armádní Noviny. *Americké tanky budoucnosti: Klíčem je mobilita a údržba.* [online]. 2019 [cit. 2020-03-20]. Dostupné z: https://www.armadninoviny.cz/americke-tanky-budoucnosti-mobilita-a-udrzba.html

15 US TRADOC. *The Operational Environment and the Changing Character of Future Warfare.* [online]. 2017 [cit. 2020-03-20]. Dostupné z: https://community.apan.org/wg/tradoc-g2/mad-scientist/m/visualizing-multi-domain-battle-2030-2050/200203

- BigData (velkoobjemová data);
- výroba energie a její ukládání (skladování);
- kybernetický prostor a vesmír;
- Collective Intelligence (inteligentní propojení sociálních sítí a zařízení);
- technologie, inženýrství a výroba;
- klimatické změny a konkurenční boj o suroviny;
- Artificial Intelligence (umělá inteligence);
- propojení člověka a počítačů;
- demografie a urbanizace;
- změny v ekonomické rovnováze;
- zvyšování úrovně lidské výkonnosti;
- robotika.

Všechny výše uvedené okruhy trendů budou (jak již bylo nastíněno výše) stále intenzivněji ovlivňovat způsob vedení války i jejich budoucí výsledky. Je proto nutné z pohledu bezpečnostního aparátu ČR (včetně samotné AČR) reflektovat tyto trendy a přizpůsobit nově budované schopnosti takto směřovanému vývoji.

1.6 Roztříštění existujících vojenských činností kybernetického a informačního charakteru ve struktuře jednotlivých druhů vojsk bez jednotného systematického řízení a rozvoje

Decentrální a nesystémové roztříštění elementů i jednotlivců zabývajících se problematikou informačních operací a dalšími činnostmi v kybernetickém prostoru ve struktuře ostatních druhů sil i vojsk bez jednotného velení a řízení podpořilo iniciaci vzniku samostatného organizačního celku, který do budoucna komplexně pojme celou související problematiku kybernetické domény. Toto bylo dále umocněno tím, že některé dílčí schopnosti informačního charakteru (zejména vedení informačních operací v kybernetickém prostoru) nebyly v rámci AČR pokryty vůbec. S ohledem na uvedené bylo proto hlavní úsilí v rámci výstavby kybernetických sil a informačních operací u AČR zaměřeno na sjednocení existujících činností v kybernetickém prostoru a informačním prostředí. Příslušná koncepce výstavby a rozvoje schopností kybernetických sil a informačních operací v AČR však i nadále počítá s tím, že jednotliví specialisté kybernetické problematiky budou působit u útvarů ostatních druhů sil a budou primárně poradním orgánem velitele pro oblast působení v kybernetickém prostoru. Mimo to budou také odpovídat za spolupráci s odborně nadřízenými útvary.

2 MISE, VIZE, HODNOTY A STRATEGIE KYBERNETICKÝCH SIL A INFORMAČNÍCH OPERACÍ

Mise a vize organizací se velmi často ve společnosti zaměňují, uživatelé je nedokáží striktně odlišit a někdy dokonce dochází k tomu, že tyto pojmy někteří jedinci (někdy i samotní zaměstnanci) považují dokonce za synonyma bez obsahového rozdílu. Je potřeba zdůraznit, že tomu tak není a jedná o různé termíny, jejichž vymezení je zcela odlišné. Jediné co lze v případě vize a mise organizace unifikovat je to, že obsah obou těchto významných termínů (vztažených ke konkrétní organizaci) je potřeba široce komunikovat a sdílet, a to jak směrem k vlastním příslušníkům, tak i dalším „stakeholders" (všem zainteresovaným stranám). Prezentace a sdělení by pak měly být srozumitelné, aby ji všichni jednoznačně pochopili a zejména, aby všichni společně postupovali k jejich naplnění. Takováto vysvětlující kampaň pak zcela jistě pomůže šířeji pochopit to, co daná organizace dělá a všichni zainteresovaní následně podpoří její působení.

2.1 Mise

Mise organizace by měla vycházet z formulací vrcholového vedení, aby co nejlépe reflektovalo podstatu a stanovené cíle organizace. Obecně je mise definována tak, aby byla srozumitelná a poměrně snadno zapamatovatelná všemi zainteresovanými stranami a subjekty. Mise velmi často vychází ze samotného účelu a předmětu (či chceme-li smyslu) existence dané organizace a je v čase poměrně stálá, tedy neměnná.

Smyslem existence kybernetických sil a informačních operací je vybudování samostatného druhu sil ve struktuře AČR, který bude schopen integrovat kybernetické a informační schopnosti do vedení společných a komplexních multidoménových operací AČR.

2.2 Vize

Vize v manažerském pojetí ve vztahu k organizacím obecně vymezuje a popisuje to, čeho chce daná organizace v dlouhodobém horizontu dosáhnout a jaké cíle v této souvislosti naplnit. Vize může obecně existovat (a často tomu s ohledem na duševní vlastnictví a příslušná „know-how" tak je) pouze v myšlenkách a hlavách zakladatelů, případně sdílena mezi velmi úzkou skupinou vedení předmětné organizace (někdy také i v rámci celé organizace), anebo může být naopak veřejně dostupná a prezentovaná. V případě citlivých oblastí zájmu je někdy přímo žádoucí, aby široká veřejnost nevěděla konkrétně, čeho chce přesně daná organizace v dlouhodobém horizontu dosáhnout. Ve všech případech by však samotná vize měla být dostatečně ambiciózní a měla by umožňovat vlastní modifikaci s ohledem na dosahování stanovených cílů, vývoj okolního prostředí a případné požadavky nadřízených subjektů.

V případě kybernetických sil a informačních operací jako integrální součásti AČR je vize zaměřena na následující oblasti:

- kybernetické síly a informační operace AČR budou schopny působit a mít vliv v informačním prostředí a kybernetické doméně;
- kybernetické síly a informační operace AČR budou schopny chránit své i resortní síly a prostředky (včetně informačních systémů a další infrastruktury), získávat informace a ve spolupráci s Vojenským zpravodajstvím vést kybernetické operace;
- působení v kybernetické doméně a související informační operace budou plně integrovány do vedení společných operací s cílem propojit stávající taktické schopnosti, vytvořit a rozvinout chybějící síly a prostředky ve všech fázích konfliktu, a to konkrétně:
    - zajištěním plánování v kybernetické doméně;
    - zajištěním koordinace informačních operací;
    - zajištěním koordinace civilně-vojenské interakce[16];
- kybernetické síly a informační operace AČR budou schopny poskytovat široké spektrum informací do sdíleného operačního obrazu ve všech fázích konfliktu.

2.3 Hodnoty

Úkolem kybernetických sil a informačních operací jako integrální součásti AČR je podpořit multidoménový přístup k vedení společných operací a přímo se do tohoto společného úsilí zapojit, kdy nejširší spektrum zainteresovaných subjektů jednoznačně chápe a podporuje význam kybernetického prostoru (jakožto nové operační domény) a vedení souvisejících informačních operací k prosazování zájmů České republiky v oblasti obrany.

Klíčovým hybatelem je jednoznačně kontinuálně se vzdělávající lidský personál s nedogmatickou (otevřenou) myslí, který vytváří stěžejní základ pro působení v nové operační doméně (kybernetickém prostoru) a je proaktivně a flexibilně schopný absorbovat nové informace k výkonu všech potřebných činností.

2.4 Strategie

Strategie kybernetických sil a informačních operací není s ohledem na citlivost tématu veřejná. Rámcově jsou strategické postupy a také důležité časové milníky rozvoje vymezeny v existujících koncepčních dokumentech AČR, kde stěžejním je samotná *Koncepce výstavby a rozvoje schopností kybernetických sil a informačních operací v AČR*.[17]

16 Často označováno anglickým termínem Civil-Military Interaction ~ CMI.

17 Vychází dále také z Bezpečnostní strategie ČR, Obranné strategie ČR, Dlouhodobého výhledu pro obranu 2035, Doktríny AČR, Auditu národní bezpečnosti a Cílů výstavby schopností 2017 (CT 2017).

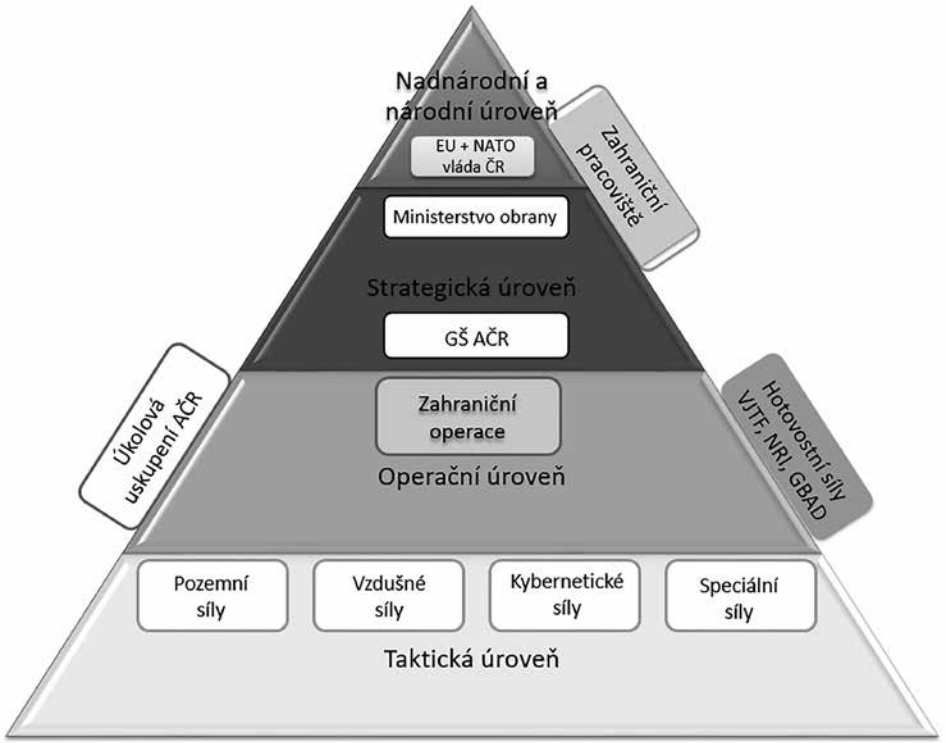
Koncepce výstavby a rozvoje schopností kybernetických sil a informačních operací v AČR je strategickým dokumentem pro výstavbu schopností kybernetických sil a informačních operací. Shrnuje současný stav a definuje úkoly a opatření nezbytná k dosažení požadovaných schopností s cílovým stavem k roku 2030. Tento zmíněný dokument logicky navazuje a blíže determinuje nadřízenou armádní koncepci KVAČR (Koncepce výstavby AČR) a je součástí soustavy koncepčních dokumentů rezortu ministerstva obrany (ustanovena jako koncepce 3. řádu).

3 INTEGRACE KYBERNETICKÝCH SIL A INFORMAČNÍCH OPERACÍ DO AČR

Zámysl vzniku kybernetických sil a informačních operací je datován k přelomu let 2017 a 2018, a to v kontextu výsledků a závěru summitu NATO v Polsku (viz rozšíření počtu operačních domén o kybernetický prostor uvedený v předcházející kapitole) a potřebě reflektovat existenci a význam kybernetického operačního prostoru. Myšlenka vybudování separátního organizačního celku ve struktuře AČR, který se bude předmětnou problematikou zevrubněji zabývat, byla následně podpořena vznikem operačně-organizačního jádra pro výstavbu, a to k 1. lednu 2019 s následným vznikem a zahájením činnosti Velitelství kybernetických sil a informačních operací (VeKySIO) k 1. červenci 2019 se sídlem v Brně. V další fázi rozvoje a budování schopností bylo do podřízenosti VeKySIO transformováno 103. centrum CIMIC/PSYOPS a přejmenováno na Skupinu kybernetických sil a informačních operací (SkKySIO), a to konkrétně k 1. lednu 2020.

Dislokace VeKySIO v Brně byla systematicky prosazena s ohledem na přítomnost Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) a dalších institucí zabývajících se kybernetickou problematikou (akademická pracoviště Masarykovy univerzity, Vysokého učení technického či Univerzity obrany, sídlo armádního centra CIRC, komerční subjekty apod.).

V kontextu dalších rozsáhlých změn v organizační struktuře AČR a s přechodem na staronový trojstupňový systém velení a řízení k 1. lednu 2020 došlo k integraci kybernetických sil a informačních operací (KySIO) na taktickou úroveň vedle pozemních sil, vzdušných sil a speciálních sil. Blíže demonstruje začlenění KySIO do struktury AČR následující schéma.



Obrázek č. 4: Integrace kybernetických sil do struktury AČR/MO[18]

V kontextu integrace kybernetických a informačních operací do struktury AČR a v rámci navazující spolupráce a zejména komunikace se zahraničními subjekty je vhodné unifikovat také používané překlady organizačních součástí kybernetických sil a informačních operací. Oficiálně schválené zkratky a překlady názvů jsou následující:

- *Velitelství kybernetických sil a informačních operací (VeKySIO) => Cyber and Information Warfare Command (CIWC);*
- *Skupina kybernetických sil a informačních operací (SkKySIO) => Cyber and Information Warfare Group (CIWG).*

S ohledem na vše uvedené je proto doporučeno, aby byly v komunikaci s jinými organizačními celky v rámci rezortu ministerstva obrany a v komunikaci se zahraničními partnery používány schválené jednotné názvy, překlady a zkratky.

18 Ve schématu použité zkratky: AČR – Armáda České republiky, ČR – Česká republika, EU – Evropská unie, GBAD – Ground Base Air Defence, GŠ – Generální štáb, NATO – North Atlantic Treaty Organization, NRI – NATO Readiness Initiative, VJTF – Very High Readiness Joint Task Force.

ZÁVĚR

V budoucích operacích je nutné si uvědomovat, že půjde v první řadě o ovládnutí informačního prostoru, prozkoumání a zmapování bojiště, udržení vlastních komunikačních kanálů a přerušení komunikačních tras protivníka. Primární úlohu budou hrát nevojenské hybridní (komplexní) aktivity na jedné straně s kinetickými operacemi ozbrojených jednotek na straně druhé, na se něž primárně zaměřuje západní vojenské myšlení. Je nutné brát v potaz, že na fyzický boj má dojít až úplně naposled, a to za vhodně vymodelovaných a dodržených podmínek. Ideálně však tehdy, když protivník už de facto v informační sféře i politicky prohrál – tedy my jsme získali značnou informační převahu a kontrolu nad jeho vlastním informačním prostorem.

V dnešním globalizovaném světě se bezpečnostní aparát neobejde bez nasazení technických prostředků umožňujících vedení informačních operací či shromažďování informací v kybernetické doméně i celkovém bezpečnostním prostředí. Monitorování komunikací a činnosti v informačním prostředí jsou rozhodujícími instrumenty, které jsou využívány pro identifikaci hrozícího nebezpečí, teprve poté následují obranná opatření, která mají toto nebezpečí minimalizovat. Nasazení moderních technologií v kybernetickém prostoru je proto nezbytné pro udržení vysoké úrovně bezpečnosti státu a nemá nic společného s velmi často mediálně proklamovaným masovým sledováním občanů.

Agresivita regionálních velmocí, soupeření o suroviny, hybridní působení, masivní migrační vlny (související s vývojem na Blízkém východě, Asii či Africe) nebo pandemie jsou hlavními hrozbami pro Českou republiku i Evropu. Dynamický rozvoj vědy a moderních technologií s sebou přináší vyšší dostupnost vyspělých technologií. Dostupnost informačních, nano a biotechnologií a snadnější výroba či automatizace budou přispívat k růstu schopností potenciálních protivníků a jejich zbraňových systémů, jejichž primární ovládání bude realizováno prostřednictvím kybernetického prostoru. V komerční sféře i celé společnosti nadále poroste závislost na informačních technologiích. S tímto budou logicky souviset i kybernetické útoky, které mohou zásadně ohrozit funkčnost státu ve všech jeho dimenzích, včetně ozbrojených sil. Řada států i nestátních entit cíleně proto buduje schopnosti kybernetického útoku na elektronické systémy státních i nestátních institucí a kritickou informační infrastrukturu.[19] Proto je nutné, aby se také Česká republika a její bezpečnostní, ochranné a obranné segmenty také zaměřily na rozvoj a budování schopností čelit kybernetickým hrozbám a efektivně působit v kybernetickém prostoru s cílem zajištění vlastních zájmů. Zde právě hraje významnou roli také výše popisované nově vzniklé kybernetické síly a informační operace, které se v nedávné době staly neodmyslitelnou integrální součástí AČR a rozšířily a doplnily tak systémovou mozaiku národního působení v kybernetickém prostoru.

19 MINISTERSTVO OBRANY ČR. *Dlouhodobý výhled pro obranu 2030.* Praha: Ministerstvo obrany ČR, 2015. 14 s.

Autor: ***Mgr. Ing. Martin HAVLÍK, Ph.D., MBA, MSc.*** *Pracovník Ministerstva obrany České republiky. Specializuje se na zpravodajskou problematiku, zejména pak na oblast technických zpravodajských disciplín, informačních a kybernetických operací jakožto nedílné součásti hybridního působení státních i nestátních aktérů. Mimo uvedené se dlouhodobě zaměřuje na analýzy bezpečnostních hrozeb a rizik v oblastech konfliktů (především v Asii) s dopadem na obranu a bezpečnost České republiky.*

Jak citovat: HAVLÍK Martin. Příčiny vzniku a začlenění kybernetických sil a informačních operací do Armády České republiky. *Vojenské rozhledy.* 2020, 29 (3), 072-086. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz.