 DOI: 10.3849/2336-2995.26.2017.03.031-050

Recenzovaný článek

Aktuální úkoly kybernetické obrany rezortu Ministerstva obrany

Recent Objectives of Cyber Defence in the Department of Defence

Miroslav Feix, Dalibor Procházka

Abstrakt: Článek se zabývá problematikou kybernetické bezpečnosti, kybernetické obrany a operací v kybernetickém prostoru s důrazem na rezort obrany. V článku je provedena analýza úkolů kybernetické obrany vyplývající ze strategických dokumentů České republiky, NATO a Evropské unie a role jednotlivých subjektů, které se na zajištění kybernetické obraně či bezpečností podílejí. Jako další zdroj úkolů jsou vytvořeny čtyři scénáře, které popisují možné situace, které budou vyžadovat schopnosti kybernetické obrany. Tato analýza je předpokladem pro stanovení požadovaných schopností a návrh řešení, jak rozdělit role, odpovědnosti a požadované schopnosti.

Abstract: The paper deals with cyber security, cyber defence and operations in cyber space focusing on the department of defence. Tasks implied from the Czech Republic's, NATO's and European Union strategic documents and roles of participating subjects have been analysed. Four scenarios as another source of identified tasks were created and used to describe possible situations requiring cyber defence capabilities. The presented analysis is a prerequisite for specifying required capabilities, and a proposal how to assign roles, responsibilities and required capabilities.

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

Keywords: Cyberspace; Cyber Security; Cyber Defence; Cyber Operations

ÚVOD

V odborné i laické debatě je stále častěji možné se setkat s pojmy, jako jsou kyberprostor, kybernetické hrozby, kybernetická kriminalita, kybernetická bezpečnost a s ní spojená kybernetická obrana. Vzhledem k tomu, jak často se modifikující (i samostatně stojící) termín „kybernetická obrana" používá, je vhodné si ho přesněji vymezit, pochopit a používat v odborné bezpečnostně-obranné debatě. Je přijat a novelizován zákon o kybernetické bezpečnosti, zajištění kybernetické bezpečnosti a obrany se dostává mezi strategické zájmy České republiky. V poslanecké sněmovně je připravena novela zákona o Vojenském zpravodajství, v jeho rámci i novela zákona o obraně. NATO vyhlašuje kybernetický prostor jako další plánovací a operační doménu na úrovni domén země, vzduch, moře a vesmír. Dále NATO prohlašuje, že napadení v kybernetickém prostoru je napadení podle článku 5 Washingtonské smlouvy a zakládá právo na aktivaci společné obrany. Je třeba kriticky zhodnotit, zda jsou bezpečnostní a obranný systém ČR, Ministerstvo obrany a ozbrojené síly připraveny čelit výzvám budoucího prostředí.

Článek se zabývá problematiku kybernetické bezpečnosti, kybernetické obrany a operací v kybernetickém prostoru se zaměřením na rezort obrany České republiky. Důraz je kladen na aktuálnost a důležitost kybernetického prostoru v rámci současného a budoucího operačního prostředí. Metodou analýzy, faktorové analýzy PESTLE a metodou scénářů jsou identifikovány úkoly kybernetické obrany, k jejichž plnění bude muset rezort obrany disponovat odpovídajícími schopnostmi.

Chápání kybernetické obrany je v České republice, a především v rezortu obrany, nejednotné. Armáda nemá doktrínu pro vedení operací v kybernetickém prostoru ani odborníky, kteří by se problematice systematicky věnovali.

Ohrožení České republiky v kybernetickém prostoru není hypotetickou hrozbou. 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 shrnuje část výsledků dosažených při zpracování závěrečné práce v kurzu generálního štábu, diskutuje úkoly, které stojí v oblasti kybernetické obrany. Výsledky analýzy jsou použity k odvození požadovaných schopností a k návrhu jejich přiřazení nositelům, ale návrh řešení je mimo záměr tohoto článku.

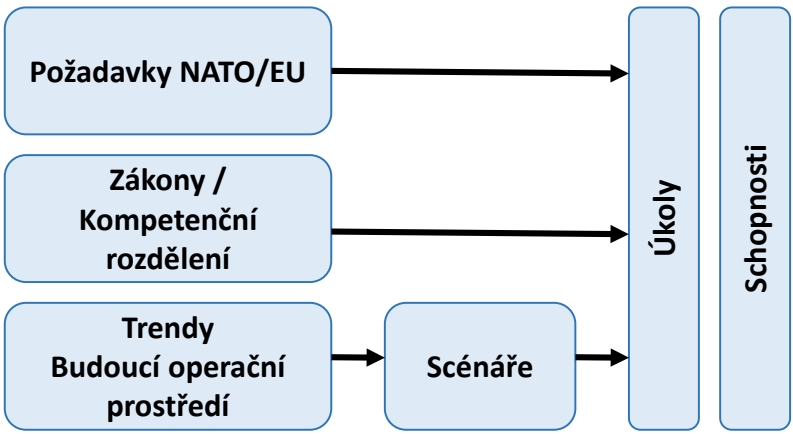
1. POUŽITÉ METODY

Metoda analýzy byla aplikována na dostupné prameny, které zahrnují zákonné, koncepční a doktrinální dokumenty ČR, Severoatlantické aliance i Spojených států amerických, odborné publikace a články v médiích. Závěry byly konzultovány s vybranými odborníky zabývajícími se problematikou bezpečnosti a obrany v kyberprostoru.

Nejprve je analyzován současný stav a úkoly kybernetické bezpečnosti a kybernetické obrany v České republice získané především z analýzy oficiálních dokumentů. Na analýzu navazují další úkoly potřebné pro stanovení požadavků na schopnosti. K tomu je využi-

ta analýza trendů a implikací k charakteristice budoucího operačního prostředí a jsou zpracovány čtyři scénáře pokrývající některé možné situace působení v kybernetickém prostoru, ze kterých úkoly vyplývají.

Pro zpracování analýzy trendů je využita faktorová analýza PESTLE. Trendy jsou analyzovány v šesti oblastech, politické, ekonomické, sociální, technologické, právní a environmentální. Hlavním zdrojem informací o trendech a budoucím prostředí byly analytické dokumenty NATO a Spojených států amerických. Možná budoucnost je dále zpracována v jednotlivých scénářích. Scénáře jsou vhodnou prognostickou metodou pro porozumění a vizualizaci možné budoucnosti. V České republice je metoda scénářů pro potřeby obrany a ozbrojených sil poněkud zanedbávána, přitom vhodně zvolený scénář umožňuje popsat budoucí vývoj a možné budoucí situace. Zpřesní potenciální cíle, efekty a úkoly a následně lze odvodit požadavky na schopnosti potřebné k zvládnutí situace. Pro přesnější zpracování kontextu je použita systémová analýza PMESII, která je založena na rozpracování operačních proměnných v oblastech politické, vojenské, ekonomické, sociální, informační a infrastrukturní, což umožňuje popsat situaci ve své komplexnosti. Zdroje úkolů jsou znázorněny na obrázku č. 1.



Obrázek č. 1: Zdroje úkolů a schopností

2. VYMEZENÍ POJMŮ

Kybernetický prostor (cyberspace, též kyberprostor) vymezuje další pojmy, jako například kybernetické operace či kybernetická bezpečnost, jeho definice je tedy primární. Zákon o kybernetické bezpečnosti definuje kybernetickým prostorem „digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací". Kybernetický prostor je zde jasně definován technickým výčtem potřebné infrastruktury a výčtem, co infrastruktura umožňuje.

Jiné definice nejsou již tak restriktivní. Definice Spojených států zdůrazňují a rozšiřují definici o globální rozměr a informační okolí. V definici NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) je to ještě výraznější „…prostředí formované fyzickými a nefyzickými částmi…". Na druhé straně spektra je pak ruské pojetí, kde se vychází z centrality informací a informačního prostoru, kybernetický prostor je jeho částí a zdůrazňuje se lidská aktivita v tomto prostoru. Český výkladový slovník pak přidává „…označení virtuálního světa… operační doména…".

Kybernetický prostor je tedy tvořen globální fyzickou sítí technologických infrastruktur umožňující vznik, zpracování, ukládání, výměnu informací a lidské aktivity či virtuální život v něm.

Kybernetická doména je pak 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. V současné době NATO uznává čtyři tradiční domény mající fyzickou podstatu: země, moře, vzduch a vesmír. Na Summitu ve Varšavě je uznána i člověkem vytvořená kybernetická doména.

Kybernetická doména má zvláštní povahu, je doménou sama o sobě a zároveň propojuje vojenské platformy působící v ostatních doménách a také vytváří virtuální informační prostor. Přiznání kyberprostoru jako válečné domény není komunitou vnímáno jednoznačně.

Termínem bezpečnost rozumíme „bezpečnost jako stav, kdy jsou na nejnižší možnou míru eliminovány hrozby pro objekt (zpravidla národní stát, popř. i mezinárodní organizaci) a jeho zájmy a tento objekt je k eliminaci stávajících i potenciálních hrozeb efektivně vybaven a ochoten při ní spolupracovat".

Kybernetické bezpečnost je stav, kdy jsou na nejnižší míru eliminovány hrozby pro ČR působící z kybernetického prostoru.

Obrana je definována v zákoně o obraně takto:

> „Obrana státu je souhrn opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením. Obrana státu zahrnuje výstavbu účinného systému obrany státu, přípravu a použití odpovídajících sil a prostředků a účast v kolektivním obranném systému."

Obrana je kombinací defenzivních a ofenzivních činností a opatření, ať už aktivního, či pasivního charakteru. Dále je termín obrana používán jen v nejširším významu jako souhrn ofenzivních a defenzivních činností na úrovni státu.

V souvislosti s kybernetickou obranou (obranou v kybernetickém prostoru) se vznášejí nad termínem pochybnosti. Jako protiklady se pak staví obrana zaměřená na odolnost a aktivní obrana. Aktivní obrana je ale z pohledu vojáka nedílnou součástí obrany.

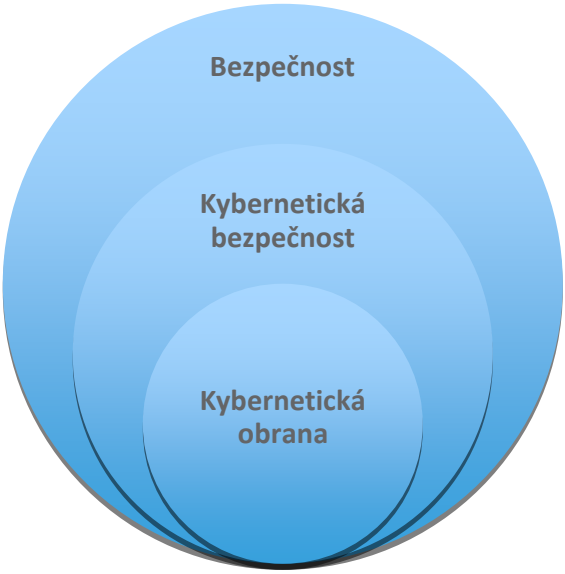
Kybernetická obrana je zde chápána jako obrana v kybernetickém prostoru a skrze (prostřednictvím) něj.

3. SOUČASNÝ STAV KYBERNETICKÉ OBRANY A STANOVENÉ ÚKOLY

Úroveň České republiky. Legislativní zpracování zajišťování kybernetické bezpečnosti je v ČR na velmi vysoké úrovni. Platí zákon o kybernetické bezpečnosti, je zpracována strategie směřování a akční plán dosažení cílů. Gestorem za oblast kybernetické bezpečnosti byl Národní bezpečnostní úřad (NBÚ) a jeho součást Národní centrum kybernetické bezpečnosti (NCKB), od 1. 8. 2017 je to Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). K jeho hlavním úkolům patří provoz vládního CERT (Computer Emergency Response Team) České republiky, a jeho spolupráce s obdobnými organizacemi na národní i mezinárodní úrovni, státními či nestátními. K celkovým činnostem patří i osvěta a podpora vzdělávání, výzkum a vývoj v oblasti kybernetické bezpečnosti a v neposlední řadě také tvorba příslušných standardů.

NÚKIB vzhledem ke své působnosti dané zákonem číslo 205/2017 Sb. může řešit útoky pouze ochranou a zvyšováním odolnosti vlastních systémů. Zasažení a eliminace útočníka, popřípadě jeho izolace je v této době v poněkud šedé zóně. Budování schopností kybernetické obrany ČR je přiděleno Vojenskému zpravodajství.

Kybernetická obrana je konsensuálně chápána jako součást širšího konceptu kybernetické bezpečnosti, viz obrázek č. 2.



Obrázek č. 2: Vztah bezpečnosti, kybernetické bezpečnosti a kybernetické obrany

Úroveň Ministerstva obrany: V letech 2005–2009 bylo vybudováno centrum CIRC v rámci přijetí a plnění závazků vůči NATO v oblasti neutajovaných systémů. Dále byla v roce 2012 zpracována *Koncepce kybernetické obrany rezortu Ministerstva obrany*. Rezort zahájil spolupráci s NBÚ a NCKB na legislativních změnách a byla identifikována kritická obranná komunikační infrastruktura rezortu obrany.
Na Ministerstvu obrany je gestorem odpovědným za oblast kybernetické bezpečnosti odbor bezpečnosti MO (OB MO). Vojenské zpravodajství je odpovědné za oblast kybernetické obrany ČR včetně výstavby sil a prostředků pro zajištění kybernetické obrany ČR.[1]

V průběhu let 2015 a 2016 dochází vlivem přijetí národní strategie kybernetické bezpečnosti ke kvalitativnímu posunu vnímání zajišťování kybernetické bezpečnosti. OB MO zpracovává návrh *Strategie kybernetické bezpečnosti rezortu Ministerstva obrany na období let 2017 až 2020* (dále rezortní *strategie*) a souvisejícího akčního plánu.[2] V průběhu zpracování je jedna z největších překážek nezájem či absence operační komunity.

Strategie rozvíjí a upevňuje část zajišťování bezpečnosti, odolnosti a bezpečnosti informací. Je zde velmi patrná snaha o rozšíření kybernetických aspektů do vedení operací v souladu s požadavky NATO na Cyber Defence a zajištění bezpečnosti dodavatelského řetězce. Na rezortní úrovni také strategie správně zahrnuje do zajišťování kybernetické bezpečnosti jak utajované, tak neutajované systémy. V oblasti spolupráce s průmyslem a zahraniční spolupráce je velmi vyčerpávající.

V přípravě a výcviku je dle názoru autorů nedostatečně zdůrazněn význam vzdělávání všech příslušníků rezortu, a to na základní uživatelské úrovni, kde dochází k nejčastějším narušením bezpečnosti. Techniky využívající sociálního inženýrství a lidský faktor všeobecně jsou v kybernetickém prostoru jedním ze slabých míst v bezpečnosti.

Celkově současné uspořádání je v základním konceptu vhodné a pokrývá potřeby rezortu. Systém ale trpí podobnými problémy jako na státní úrovni. Budování schopností obrany a bezpečnosti probíhá do značné míry odděleně a s nejasnostmi při přechodu mezi jednotlivými oblastmi. Je poměrně jasně stanoveno a prodiskutováno dělení v negativním pojetí, tedy co kdo nedělá nebo nesmí dělat, ale jak jednotlivé nástroje rezortu efektivně integrovat pro plnění úkolů je nedořešeno. V současném bezpečnostním prostředí, kde jsou hranice mezi jednotlivými hrozbami velmi nejasné a často i tak záměrně postavené, již není možné pracovat pouze v jednotlivých oblastech bez společného působení. Integrace kybernetických schopností v rámci společného působení disponibilních sil a prostředků je nutností.

I na rezortní úrovni je zcela zřejmá tendence redukce bezpečnosti v kybernetickém prostoru pouze na řešení hrozeb technického charakteru. O informačním působení a strategické komunikaci se ani *koncepce*, ani nová *strategie* nezmiňují.

---

1 *Usnesení vlády České republiky ze dne 25. května 2015 č. 382: k Akčnímu plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020.* 2015.

2 *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020.* Dostupné z: 1url.cz/ht4m2.

Úroveň Armády České republiky: Na koncepční a doktrinální úrovni má AČR dobře zpracovánu schopnost odolnosti a bezpečnosti informací v rezortních neutajovaných sítích. Založení CIRC předběhlo dobu. Dosažení potřebné úrovně schopností však brání nedostatek kvalifikovaného personálu a financí na jedné straně a neochota vojáků všech stupňů brát kybernetickou obranu vážně na straně druhé. Možnosti a funkce CIRC jsou tak v praxi bohužel omezené a to tak plně nezabezpečuje ochranu rezortních sítí.

V požadovaném stavu v roce 2025 je v KVAČR uvedeno: „Armáda ČR bude mít, v součinnosti s orgány odpovědnými za kybernetickou bezpečnost a obranu, schopnosti plánování a řízení operací v kybernetickém prostoru...“.[3] Následně jsou uvedeny tři oblasti: (1) kybernetická bezpečnost bude řešena komplexně a vytvoří se struktura řídících a výkonných orgánů, (2) významnou částí je CIRC (s výčtem jaké schopnosti by měl mít) a (3) obranu má na starosti VZ, jak národní, tak podporu operací AČR.

Je zde zřetelná silná redukce zajišťování bezpečnosti na schopnost odolnosti a bezpečnosti informací, a to ještě v rámci mírové infrastruktury rezortu. Z textu je zřejmý náhled na zajišťování kybernetické bezpečnosti jako technickou odbornou službu, která není integrována a není součástí vedení operací. Další významné schopnosti potřebné pro vedení operací v kybernetické doméně se neřeší.

Rozdíly v chápání pojmu kybernetická obrana. Je nutné zdůraznit skutečnost, že ve vnímání pojmů „Cyber Defence“ a „kybernetická obrana“ jsou v prostředí České republiky významné rozdíly. V souvislosti s vymezením působností tak působí proti efektivnímu koordinovanému přístupu k hrozbám, a potencionálně vytváří duplicity nebo, a to je častější, mezery v celkovém systému.

V zákoně o zajišťování obrany je obrana souhrn opatření zahrnující výstavbu, přípravu a použití sil a prostředků „k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením“.[4] Zákon nespecifikuje, jakou povahu má vnější napadení.

Úkoly proto zahrnují reakce na technické a informační napadení, získávání informací, ofenzivní a defenzivní operace a jako základ odolnost vlastních sítí a takto vymezují i obranu v kybernetickém prostoru. Z pohledu obrany tedy zahrnují vše kromě odolnosti nevojenských sítí.

NATO chápe kybernetickou obranu jako ochranu a odolnost vlastních sítí tedy aplikaci bezpečnostních opatření k obraně infrastruktury komunikačních a informačních systémů (KIS) proti kybernetickým útokům. Pojem kybernetická bezpečnost nedefinuje, využívá pojem bezpečnost KIS (CIS Security). Požadavky NATO v oblasti Cyber Defence se ve velké míře překrývají s požadavky na realizaci opatření kybernetické bezpečnosti ve smyslu zákona o kybernetické bezpečnosti u systémů kritické informační infrastruktury. Pohled NATO na kybernetickou obranu se tedy ve velké míře překrývá s pohledem a vymezením kybernetické bezpečnosti.

Nutno ale zmínit, že pohled NATO se v průběhu času rozšiřuje do zajištění odolnosti systémů (včetně nasaditelných) při vedení operací. V rezortu obrany, a především pak

---

3 Koncepce výstavby Armády České republiky 2025: upravená verze ke zveřejnění. Praha: Ministerstvo obrany, 2015.

4 Zákon č. 222/1999 Sb., o zajišťování obrany České republiky. In: *Sbírka zákonů*. 1999.

v ozbrojených silách, nebyl zatím tento rozšířený pohled dostatečně vnímán. Často je kybernetická bezpečnost a kybernetická obrana chápána pouze jako zabezpečení sítí bez vlivu na vedení operací. Tento názor se však v posledních dvou letech začíná měnit.

Pohled NÚKIB (dříve NCKB) je do značné míry vymezen v zákoně o kybernetické bezpečnosti a rozdělením rolí v rámci státní správy. Je zde užší pojetí ve smyslu útoků pouze technického rázu a informační působení nepřítele vůbec neuvažuje. Kritéria, zda se jedná o kybernetickou bezpečnost nebo obranu, jsou následující: (1) povaha hrozby a (2) typ a cíl útoku.[5] V případě kybernetické obrany útoky pochází ze zahraničí a jejich motivací jsou politické cíle, na rozdíl od kriminality, kde je primární finanční prospěch. Dále cílem musí být národní aktiva kritická pro fungování státu a intenzita musí překročit schopnost účinné reakce v rámci zákona o kybernetické bezpečnosti. Je tedy možné říci, že pokud útok přichází zvenčí, má jiné než finanční zájmy (kriminalita), útočí na kritickou infrastrukturu a intenzita překročí určitou mez, je možné nebo nutné použít prostředky kybernetické obrany.

Kybernetická obrana ČR je přidělena v rámci rezortu obrany Vojenskému zpravodajství. **Vnímání Vojenského zpravodajství** je ovlivněno charakterem a zaměřením instituce a zároveň jejím začleněním pod Ministerstvo obrany jako součást obranného systému. Chápání VZ je možné odvodit z návrhu novelizace zákona o Vojenském zpravodajství. V zákoně o zajišťování obrany se přidává „Obrana státu, jejíž součástí je také obrana státu v kybernetickém prostoru (dále jen „kybernetická obrana")" a také „Kybernetickou obranou se rozumí souhrn opatření […] podle zákona o Vojenském zpravodajství. V zákoně o Vojenském zpravodajství se navrhuje svěřit VZ „předcházení, zastavení nebo odvrácení kybernetického útoku ohrožujícího zajišťování obrany České republiky" a používat k tomu technické prostředky a související postupy a opatření. VZ svou úlohu vidí jednak v efektivním sběru informací v a prostřednictvím kybernetického prostor a hlavně při obraně kybernetického prostoru ve smyslu aktivního působení na původce útoku. Tedy vlastně vedení kybernetických operací buď (a to především) ve prospěch obrany ČR, nebo i při podpoře zasazených jednotek ozbrojených sil.

Vyjasnění terminologie je pro studium a vedení odborného diskurzu zásadní. V praxi tyto nejasnosti přinášejí mnohé problémy a rozpory. Zatím se to řeší tak, že pokud se mluví o kybernetické obraně ve smyslu NATO, používá se anglický termín Cyber Defence. Pokud se použije termín kybernetická obrana, máme na mysli odpovídající činnost Vojenského zpravodajství, a pokud mluvíme o odolnosti a zabezpečení vlastních sítí, informačních systémů a infrastruktuře, jde o kybernetickou bezpečnost.

Autoři vycházejí z předpokladu, že budování a použití prostředků obrany v kybernetickém prostoru patří do rezortu obrany, stejně jako ozbrojené síly, které jsou dominantní složkou silového působení v obraně obecně. Zatím lze obecně vycházet ze zákona o zajišťování obrany, jehož zatím blíže nespecifikovanou součástí je i obrana v kyberprostoru.

V současném systému tak chybí přesné vymezení, co je obrana v kybernetickém prostoru, a od toho se odvíjejí problémy způsobené neexistencí systémů řízení a koordinace mezi kybernetickou bezpečností a kybernetickou obranou mimo běžné sdílení informací.

5 PAČKA, Roman. Difference between Cyber Security and Cyber Defence from Czech perspective. *Cyber Security Review*. 2015, (Spring 2015), 20-24. ISSN 2055-6950.

Vymezení zodpovědností v různých intenzitách a rozsahu útoků, předávání zodpovědností, tedy kdo rozhoduje a řídí, je v dnešní době nejasné.

Využívání informací jako nástroje moci, a tedy i informačního působení ve své nejširší podobě není v České republice téměř vůbec rozvinuté.[6] Na národní úrovni je zahrnutí informačního působení ve strategických dokumentech na minimální úrovni. Informační působení v kyberprostoru není výjimkou. Ve světle hybridních hrozeb začíná rezort obrany podnikat kroky k nápravě a rozvíjet teorii a praxi strategické komunikace a v jejím rámci informační operace[7]. Řešení absence informačního působení na úrovni ČR jde za rámec článku, přesto je nezbytné upozornit na mezeru v bezpečnostním systému ohrožující zájmy České republiky.

Severoatlantická aliance: Principy použití ozbrojených sil jsou stanoveny v doktrínách. Přesné požadavky na schopnosti, tedy co, v jaké kvalitě a kvantitě je třeba mít k dispozici, NATO formuluje v rámci obranného plánování jako cíle schopnosti (CT – Capability Targets).

Je třeba zdůraznit, že konsensuální rozhodovaní Aliance determinuje i stanovené úkoly a požadované schopnosti. V rámci kompromisu se vždy jedná o minimální společně odsouhlasené konkrétní požadavky a náročné vize či směřování, tedy i v případě Cyber Defence.

Z pohledu NATO je kladen v oblasti Cyber Defence důraz na odolnost sítí a bezpečnost informací. Postupem času se stále více prosazuje myšlenka a nutnost integrovat opatření Cyber Defence do přípravy a operačního použití sil, což se ukazuje právě i na deklaraci kybernetického prostoru jako domény. Na druhou stranu ale nepanuje shoda ohledně ofenzivního působení v kybernetickém prostoru. Budování ofenzivních schopností se tak nechává na rozhodnutí jednotlivých států a zároveň se mlčky předpokládá, že v případě potřeby budou tyto schopnosti poskytnuty ve prospěch všech.

Evropská unie: Vývoj v Evropské unii probíhá v podstatě obdobně, i s tradičním rozdělením rolí či pohledů mezi EU a NATO. Strategie EU se více zabývá nevojenskou složkou,[8] internetem a jeho dopady na každodenní život. Oblast Cyber Defence je v EU vnímána jako dimenze kybernetické bezpečnosti.[9] Je také považována za opatření k obraně kritických systémů a informací za účelem dosažení kybernetické bezpečnosti.[10] Mezi NATO a EU je v únoru 2016 podepsáno ujednání o spolupráci (Technical arrangement in Cyber Defence).

Velký důraz je tak kladen na minimalizaci kybernetické kriminality a mezinárodní spolupráci, zavedení a sladění soudržné mezinárodní politiky EU v kybernetickém prosto-

---

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

7 Ibid, s. 68 „Informační operace jsou vojenská štábní funkce pro koordinaci informačních aktivit s cílem vytvářet požadované účinky na vůli, porozumění a schopnost protivníků, potencionálních protivníků a dalších cílových skupin k podpoře zabezpečení obrany ČR a cílů operací AČR."

8 Ve srovnání s NATO, což je pochopitelné. NATO je obranná aliance, EU má mnohem širší záběr.

9 Většinově chápána jako vojenská dimenze, ale zahrnující jak vojenské, tak civilní přístupy.

10 *EUROPEAN UNION CONCEPT FOR EU-LED MILITARY OPERATIONS and MISIONS* [online]. Dostupné z: 1url.cz/Nt4mG.

ru. Dalším prvkem evropské politiky je zdůraznění spolupráce v rámci Evropské obranné agentury (EDA – European Defence Agency) a s průmyslovým sektorem.

Souhrn úkolů vyplývajících z dokumentů NATO a EU

Analýzou politik, konceptů a cílů schopností je možné shrnout úkoly do následujících hlavních požadavků:

- zodpovědnost za vlastní sítě,
- odolnost a bezpečnost informací,
- interoperabilita sítí a kybernetické obrany,
- sdílení informací,
- společné vzdělávání,
- spolupráce s průmyslem,
- spolupráce s akademickou sférou,
- 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.

Úkol vyplývající ze zákona o kybernetické bezpečnosti[11] a souvisejících koncepčních dokumentů:

Úkoly dané právním řádem zahrnují:

- ochranu vlastních neutajovaných sítí a kritické infrastruktury,
- ochranu vlastních utajovaných sítí (zákon výslovně neřeší),
- kybernetickou obranu,
- splňování stanovených standardů pro systémy zařazené do významných informačních systémů a kritické infrastruktury,
- povinnost podávat a sdílet informace,
- provádění opatření k ochraně sítí a infrastruktury,
- systém koordinace,
- systém velení a řízení.

4. HODNOCENÍ AKTUÁLNÍHO STAVU A VYMEZENÍ PROBLÉMU

V rámci České republiky je v současné době kladen důraz na zajištění kybernetické bezpečnosti. Na velmi vysoké úrovni je právní rámec a rozvojové strategické dokumenty na úrovni ČR i rezortu obrany v oblasti kybernetické bezpečnosti. Gestorem za oblast kybernetické obrany bylo určeno Vojenské zpravodajství. Není však shoda, co vlastně kybernetická obrana vše zahrnuje. Panují nejasnosti v systému řízení a koordinace a vymezení zodpovědností v různých situacích.

V rámci rezortu a ozbrojených sil jsou schopnosti kybernetické bezpečnosti a kybernetické obrany budovány odděleně. Kybernetická obrana je tak nedostatečně integrována

11 Zákon nezahrnuje vojenské sítě, nicméně se v oblasti rezortní kybernetické bezpečnosti používá.

do komplexního vedení obrany a operací ozbrojených sil pod jednotným velením. Oblast obrany v kybernetickém prostoru je silně technicky orientována. Na kyberprostor se nepohlíží jako na součást informačního prostředí. Informační působení a zisk informací na operační úrovni tak není řešen vůbec.

Úkoly vyplývající ze členství v NATO a EU a stanovené právním řádem ČR se vzájemně prolínají a fakticky se soustředí opět spíše na kybernetickou bezpečnost. NATO rozšiřuje svůj pohled a požaduje integraci do vedení operací.

5. BUDOUCÍ OPERAČNÍ PROSTŘEDÍ, SCÉNÁŘE A VYPLÝVAJÍCÍ ÚKOLY

5.1 Analýza trendů

Analýza trendů slouží jako základ pro zpřesnění obrazu budoucího operačního prostředí a tvorbu scénářů. Níže jsou uvedeny jednotlivé faktory vnějšího prostředí relevantní pro kybernetickou obranu dle metody PESTLE.

Politický. V politické oblasti dojde k výrazným změnám v rovnováze moci a síly aktérů. Budou vznikat nová centra moci a tradiční se budou snažit udržet svůj podíl na mezinárodní scéně. Současné uspořádání mezinárodních vztahů bude pod tlakem vzájemně soupeřících zájmů, komplikované růstem vlivu nestátních a nadnárodních aktérů.

Ekonomický. Svět je a bude ekonomicky propojený a vzájemně závislý. Globalizace umožňuje obrovský pohyb zboží, kapitálu, práce a služeb a s tím navázaný růst. Stinnou stránkou je náchylnost k rychlému šíření krizí bez možnosti kontroly a vlivu většiny států, a nerovnoměrně rozvržené zisky z globalizace. Nárůst požadavků na zdroje rozvíjejících se zemí ve spojení s růstem populace povede ke zvýšení soutěže o zdroje.

Sociální. Lidská populace bude nerovnoměrně růst a přesunovat se do měst. Nerovnoměrné rozdělení bohatství, možností pro lidský rozvoj a přeplněností obyvatelstva v některých částech světa povede k migračním tlakům a s tím souvisejícími problémy integrace v jiných zemích. Technologické a kulturní změny urychlí rozpad tradičních hodnot a povedou ke krizím identity.

Technologický. Rozvoj technologií zrychluje změny ve světě a umožnuje propojení světa do jedné globální informační vesnice. Rozšíření a dostupnost technologií umožnilo využít vyspělých technologií i nestátním aktérům a jednotlivcům. Umělá inteligence, robotické systémy a jejich prolnutí do společnosti mění zavedené způsoby života. Některé vědecké a technologické objevy mohou mít až disruptivní potenciál a kontrola jejich dopadů bude obtížná.

Právní. Uspořádaní mezinárodních vztahů a právního sytému se bude kontinuálně vyvíjet. Všichni aktéři, tedy i nestátní, se budou snažit měnit a využívat současné normy a pravidla ve svůj prospěch. Právo se stane běžným nástrojem pro vedení konfliktů a formou zbraně. Roste význam individualit a uspokojení jejich potřeb. Lidská práva a jejich rozšiřování se stávají předmětem sporu.

Environmentální. Trendy v oblasti životního prostředí nejsou přímo relevantní.

Budoucí operační prostředí: Svět se rychle mění a s ním se mění i operační prostředí a charakter soudobých konfliktů. Válka se již nevyhlašuje, ubývá konfliktů mezi státními aktéry, klasický konvenční konflikt je už výjimkou. Naopak narůstá zapojení nestátních aktérů a jejich vliv na charakter konfliktů.[12]

Největší změny v mezinárodním uspořádání a mezinárodním právním systému je možné očekávat v oblastech, které jsou v současné době definovány nejasně, minimálně nebo vůbec. Jednotliví aktéři budou chtít prosadit své zájmy v rámci právě vytvářeného systému a stvořit normy a pravidla vyhovující jejich parciálním zájmům. Týká se především využívání globálních veřejných statků, specificky využívání přírodních zdrojů v mezinárodních vodách nebo využívání vesmíru, a především kybernetického prostoru.

Globalizovaný a propojený svět umožňuje rychlé přelévání konfliktů a jejich dopadů i do vzdálených oblastí.[13] Zároveň rozpad unipolárního světa vytvořil prostor k realizaci ambicí i lokálních aktérů, z čehož pak vyplývá rostoucí komplexita, provázanost a obtížná předvídatelnost bezpečnostního prostředí.

Roste podíl asymetrických, nekonvenčních složek konfliktů.[14] Různorodost aktérů současných konfliktů vede k široké škále používaných strategií a metod řešení konfliktů.

Na vzestupu jsou hybridní a komplexní strategie.[15] Stírají se rozdíly mezi vnitřní a vnější bezpečností. Hrozby jsou rozmanité a propojené. Využívá se nejasné hranice mezi mírovým soutěžením a agresí. Bez komplexního přístupu k řešení hrozeb již není možné efektivně reagovat.

Jedním z dominantních trendů poslední doby determinovaných technologickým rozvojem, je pak nástup centrality informací a kybernetického prostoru jako místa konfliktu. Svět charakterizuje „bezprecedentní a stále rostoucí informační propojenost světa v důsledku globalizace, a především díky dostupnosti internetu a informačních technologií".[16] Veřejná i soukromá sféra je závislá na informačních a komunikačních technologiích. S tím roste i riziko a závažnost dopadů na (kritickou) informační infrastrukturu.

Svět je poměrně snadné narušit útokem na „nervový systém", tedy propojenost vytvářenou v kybernetickém prostoru. Dalším vektorem útoku je rozvrácení morálky obyvatelstva v postmoderním světě, kdy člověk, který ztrácí morální a lidskou orientaci

12 *Bezpečnostní strategie České republiky 2015.* Dostupné z: 1url.cz/UtpJ6.

13 *Dlouhodobý výhled pro obranu 2030.* Praha: Ministerstvo obrany, 2015.

14 Ibid. *Bezpečnostní strategie*

15 HOFFMAN, Frank G. *Conflict in the 21st Century: The Rise of the Hybrid Wars* [online]. In: . Arlington, Virginia: Potomac Institute for Policy Studies, 2007 [cit. 2017-06-20]. Dostupné z: http://1url.cz/ztDNp+.

16 Ibid. ŘEHKA.

podléhá manipulativnímu působení propagandy. Vztah mezi člověkem a kybernetickým prostorem vytváří mnohé výzvy a příležitosti pro vojenské využití.[17]

5.2 Scénáře relevantní pro kybernetickou obranu

Byly zpracovány čtyři základní scénáře, přičemž dva jsou dominantně strategické úrovně s přesahem do operační úrovně. První je zaměřený na masivní technický kybernetický útok na zájmy státu a druhý je zaměřený na informační působení v kybernetickém prostoru. Další dva scénáře se zaměřují na roli kybernetické domény při vedení operací. První rozvíjí činnosti a úkoly při vedení společných (JOINT) operací a druhý při řešení národních úkolů při únosu českých občanů v zahraničí.

Zpracování scénářů umožní podrobněji rozpracovat možné úkoly, které bude nutné v rámci scénáře plnit. Vyplývající úkoly následně napomohou k přesnějšímu stanovení požadavků na schopnosti. Scénáře jsou dále doplňovány o podrobnosti z dalších relevantních zdrojů, tedy scénářů vytvořených pro potřeby NATO, či přímo ČR. Ze scénářů jsou použity části vztahující se ke kybernetickému prostoru nebo pro nutný kontext a okolí.

Struktura scénářů je následující:

- důvody pro scénář,
- příběh popisující možnou situaci a její vývoj,
- situace ve struktuře PMESII (kontext),
- cílový stav relevantní pro scénář,[18]
- úkoly, které bude nutné plnit.

Scénáře nejsou uvedeny v plném rozsahu. Pro účely článku je zestručněn příběh, vynechán kontext a shrnutí úkolů. Cíle a úkoly v rámci scénářů nemusejí být vždy v souladu se současnou právní úpravou nebo kompetenčním rozdělením působností. Scénáře představují výchozí návrh, jak odvodit požadované schopnosti kybernetické obrany a netvoří úplnou sadu pokrývající všechny možné situace.

Technologické napadení

Scénář kybernetického útoku technologického charakteru je jednou z deseti tzv. „nestabilních situací“ vyjádřených v FFAO.[19] Útok na kritickou infrastrukturu[20] v kybernetickém prostoru a prostřednictvím kybernetického prostoru má „závažný dopad na bezpečnost ČR, zabezpečení základních životních potřeb obyvatelstva nebo ekonomickou situaci”.[21]

17 DUGGAN, Patrick. Why Special Operations Forces in US Cyber-Warfare? *Cyber Defense Review* [online]. 2016(2) [cit. 2017-06-20]. Dostupné z: http://1url.cz/st4mz.

18 Strategické, politické, vojenské, operační dle relevance v rámci scénáře.

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

20 Jedná se o infrastrukturu kritickou pro fungování státu, nejen o kritickou informační infrastruktur dle zákona č. 181/2014 Sb.

21 Audit národní bezpečnosti. Praha: Ministerstvo vnitra České republiky, 2016. Dostupné z: 1url.cz/etEas, s. 95.

Příběh:

Webové stránky státních úřadů včetně Úřadu vlády a Ministerstva obrany jsou nedostupné z důvodu DDoS útoku.[22] Nedostupnost služeb hlásí některé banky a systém elektronické evidence tržeb. Ředitel NÚKIB vyhlašuje stav kybernetického nebezpečí a rozhoduje o provedení reaktivních opatření.

NÚKIB ve spolupráci s Ministerstvem vnitra a zpravodajskými službami intenzivně hledá zdroje nepřátelského působení. O pomoc jsou požádány mezinárodní instituce.

Intenzita nepřátelských útoků se stupňuje, je napadena elektrická rozvodná síť, a dochází k masivním výpadkům dodávky elektřiny ve velkých městech.

Zdroj nepřátelského působení je lokalizován do prostoru Ruska a států jižní části bývalého Sovětského svazu. Bezpečnostní rada státu a poté vláda, jednomyslně považuje kybernetický útok za ozbrojené napadení České republiky a vyhlašuje stav (kybernetické) nouze. Dále žádá NATO o aplikaci článku 5. NATO v rámci dohod vysílá svůj Rapid Reaction Team do ČR.

ČR aktivuje své obranné schopnosti. V součinnosti všech relevantních složek se částečně daří odrážet kybernetické útoky a vracet některé služby do alespoň omezeného provozu. Nepřátelské působení nepolevuje, je nutné eliminovat zdroj. Na mezinárodním poli vrcholí diplomatická a právní bitva, Rusko odmítá zodpovědnost za útoky či původ působení ze svého teritoria. Je rozhodnuto o provedení cílených kybernetických útoků na aktivní zdroje.

Koordinovaným působením všech složek včetně pomoci od NATO a některých spojenců je kybernetický útok zastaven, zasažená kybernetická infrastruktura je postupně zprovozňována a kybernetický prostor se vrací k normálu.

Cílový stav:

- služby obyvatelstvu jsou obnoveny,
- kritická infrastruktura státu je v provozu,
- důvěra ve schopnost vlády ochránit kritickou infrastrukturu před útoky z kyberprostoru je udržena.

Informační napadení

Scénář informačního útoku či spíše informačního působení[23] v kybernetickém prostoru je v poslední době stále aktuálnější. V Auditu národní bezpečnosti[24] se informační působení objevuje především v částech kybernetické hrozby, působení cizí moci a hybridní hrozby. Systematické informační působení v kybernetickém prostoru ČR ať státního či nestátního aktéra již nyní probíhá.[25] Ovlivňování veřejného mínění cestou nepřátelského informačního působení je hrozbou pro životní a strategické zájmy ČR.

22 DDoS útok (distributed denial-of-service attack) - útok na internetovou službu či webovou stránku zahlcením požadavky, jehož cílem je nedostupnost pro normální uživatele.

23 Působení lépe zdůrazňuje dlouhodobost a charakter hrozby.

24 *Audit národní bezpečnosti*. Praha: Ministerstvo vnitra České republiky, 2016.

25 Ibid, s 99-100.

Příběh:

Zpravodajské služby zvyšují své schopnosti pro získávání informací z kybernetického prostoru ať z otevřených či zakrytých zdrojů. V nepřátelské kybernetické špionáži zvyšují aktivitu Rusko a Čína. Důvěryhodnost zpravodajských serverů a tradičních médií klesá, obyvatelstvo se obrací spíše k alternativním zdrojům informací na internetu a sociálním sítím. Komunikační prostor se fragmentuje, což ovlivňuje i domácí politiku.[26]

Dochází ke krizi identity, což využívá Rusko k intenzivnímu informačnímu působení[27]. Cílem je upevnit a prohloubit antisystémové postoje[28] Schopnost lidí spolehlivě rozlišovat se snižuje vlivem zdokonalených dezinformačních metod. To vše snižuje důvěru v politické instituce a tradiční zdroje autority. Kybernetický prostor umožnuje i šíření idejí násilných extrémistických skupin. Šíří se nenávist, skupiny jako ISIL zde rekrutují bojovníky a získávají své podporovatele. Společnost se stále více polarizuje.

Rusko se snaží ovlivnit rozhodování vlád euroatlantického prostoru a zpochybnit důvěryhodnost a legitimitu vládnutí. Selektivně vybrané a kontextu zbavené informace získané kybernetickou špionáží cíleně uveřejňuje. Tlačí na rozpad západních demokratických struktur a především vnitřní jednoty NATO.

Demokratické státy se snaží reagovat na nepřátelské informační působení, posilují obranyschopnost a vnitřní soudržnost. Intenzivně pracují na skloubení svobody vyjadřování a zajištění bezpečnosti.

Cílový stav:

- jsou minimalizovány negativní dopady informačního působení,
- je zvýšena odolnost společnosti proti nepřátelskému informačnímu působení,
- svoboda a ochrana práv jednotlivce v rámci kybernetického prostoru je nedotčena.

Vedení společných operací v rámci Aliance

Scénář vedení společných operací je pro praktické použití u ozbrojených sil nejdůležitější. Použití ozbrojených sil v rámci alianční obrany je základním způsobem jejich nasazení, a jejich mírová struktura je takto koncipována.[29] V rámci scénáře není řešeno, jaký bude příspěvek ČR do konkrétní operace, ale spíše co bude potřebovat aliance jako celek. Popis scénáře se soustředí na aspekty dotýkající se kybernetického prostoru a působení v něm, to ale neznamená, že se neplní i jiné úkoly.

Příběh:

Bezpečnostní situace v baltských státech se zhoršuje. Ruské etnické menšiny se dožadují větší samostatnosti a podílu na moci, vznikají nepokoje. Intenzita kybernetických útoků na infrastrukturu se zvyšuje, dochází k výpadkům sítě. Baltské státy žádají konzultace dle čl. 4. a žádají o posílení jejich bezpečnosti, situace je nejasná.

---

26 DITRYCH, Ondřej. et al. *Scénáře vývoje mezinárodního bezpečnostního prostředí (2016)*. Praha: Ústav mezinárodních vztahů, 2016, s. 5.

27 Ibid, s. 31

28 Ibid, s. 5

29 *Audit národní bezpečnosti*. Praha: Ministerstvo vnitra České republiky, 2016, s. 134.

Do Pobaltí se přesouvají síly rychlé reakce NATO jako důkaz jednoty a odhodlání ke společné obraně. Manévr je narušován častými problémy ve spojení v důsledku napadání sítí velení a řízení NATO.[30] Rusko vydává prohlášení o ochraně svých etnických menšin v zahraničí a svém odhodlání je v případě potřeby podpořit. V Baltském moři dochází k incidentu, kdy je loď vybavená systémem AEGIS ohrožována ruskými letouny a snahou vyřadit naváděcí systémy prostředky elektronického boje. Dochází k odpalu raket a ruský letoun je sestřelen. Není jasné, proč došlo k odpalu raket.

Po sociálních sítích se v oblastech s převahou ruské národnosti šíří informace o násilnostech vojsk NATO. Pokročilé analytické systémy využívající prvky umělé inteligence v téměř reálném čase vytváří výraznou polarizaci nálad ve společnosti a ochotu k násilnému řešení. Ve městech vzniká panika, lidé se připravují na válku, dochází k rabování.

Rusko provádí prověrku pohotovosti svých vojsk v oblasti Kaliningradu a Petrohradu, v pohotovosti je 50 tisíc vojáků. Na operačním velitelství NATO se slaďují obranné plány ve všech doménách založené na společném působení všech sil a prostředků. Připravuje se manévr a systém paleb především na systémy velení a řízení. V kybernetickém prostoru dochází k intenzivnímu sběru a analýze aktuálních informací o zranitelnostech. Připravuje se série společných útoků vzdušných, námořních a kybernetických sil na místa velení a řízení.

Cílový stav:

- je zajištěna bezpečnost států NATO,
- nepřítel je odstrašen,
- systémy velení a řízení jsou nenarušeny.

Ochrana národních zájmů

Scénář použití ozbrojených sil ČR pro ochranu národních zájmů vychází z jednoho z typových plánů. ČR tedy předpokládá v určitých případech chránit své zájmy i za použití sil pod národním velením. Únosy občanů různých států, ať už z jakéhokoli důvodu poměrně často a výrazně zasahují do domácí politiky. ČR není hlavní cílovou zemí, ale přesto je nutné, aby ozbrojené síly na takovéto situace byly připraveny a poskytovaly vládě možnosti řešení situace.[31]

Příběh:

Při probíhajícím konfliktu na Předním východě jsou uneseni dva pracovníci humanitární organizace české národnosti. Zároveň jsou napadeny webové stránky humanitárních organizací ukazující, co se stane každému, kdo přijede pomáhat. Únosci se ozvou se svými politickými požadavky. V konfliktu jsou v rámci koalice nasazeny i jednotky AČR.

V průběhu vyjednávání se podaří Vojenskému zpravodajství lokalizovat polohu vyjednavačů do objektu v okrajové průmyslové části města. S pomocí taktických odposlechů, autonomních průzkumných systémů, sledování sociálních sítí a komunikátorů jsou získána potřebná data. Jejich zpracováním s využitím prvků umělé inteligence je potvrzena

30 MAZANEC, Brian M a Bradley A. THAYER. *Deterring cyber warfare: bolstering strategic stability in cyberspace*. ISBN 978-1-137-47617-3, s. 20

31 Článek neřeší právní aspekt.

i přítomnost rukojmí. Je rozhodnuto o provedení záchranné operace. Úkolové uskupení speciálních sil je posíleno o jednotku kybernetických operací a modul ISTAR.

Začala spolupráce s lokálními důvěryhodnými prvky, pro což je vytvořena ad-hoc zabezpečená komunikační a informační síť. Místní spolupracovník pronikl do objektu a infikoval systém zabezpečení objektu speciálně připraveným malware.

Odřad je při postupu k objektu chráněn napadením městského sledovacího systému kybernetickým útokem vedeným z ČR. Na sociálních sítích začíná diskuse nad pohybem činností koaličních sil v jiné části města, nepřítel je klamán a pozornost je odvedena od cíle operace. Při napadení objektu je vypnuto zabezpečení, a tak dosaženo momentu překvapení, rukojmí jsou téměř bez boje osvobozeni a odřad pokračuje na místo vyzvednutí. Systém sledování známých příslušníků teroristické skupiny ukazuje srocení na směru odchodu. Komunikace mezi základnou a odřadem je rušena a vede se boj o udržení spojení. Konvoj je odkloněn a bezpečně předá osvobozené občany.

Okamžitě začíná kampaň proti unášení civilistů a neschopnosti teroristů. V ČR vláda vydává prohlášení o záchraně humanitárních pracovníků a ujišťuje české občany o svém odhodlání a schopnostech zajistit jejich bezpečnost.

Cílový stav:

- rukojmí jsou osvobozena,
- je zachována důvěra ve schopnost ČR chránit své občany.

5.3 Úkoly vyplývající ze scénářů a jejich uspořádání

Analýzou možných úkolů vyplývajících ze scénářů je možné pro lepší přehlednost a pochopení úkoly shrnout do několika velkých skupin.

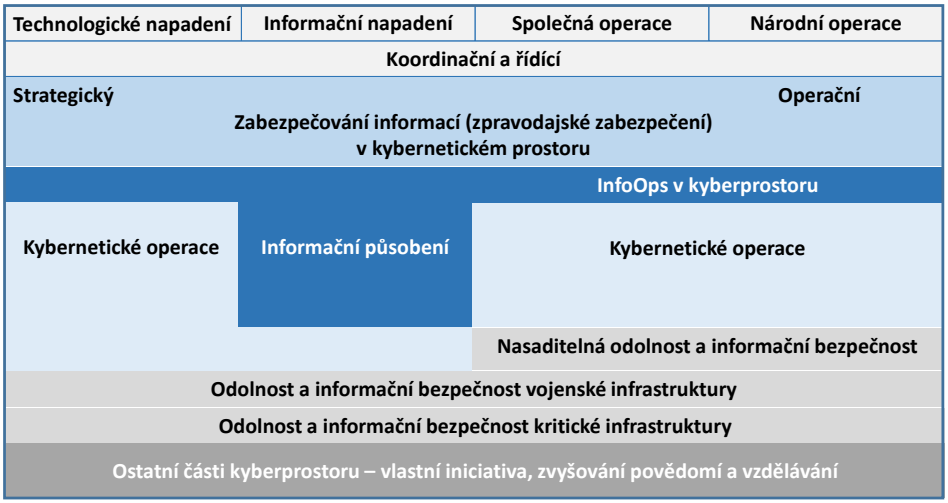
1. Odolnost a bezpečnost informací.
2. Zabezpečování informací v kyberprostoru.
3. Kybernetické operace.
4. Informační působení v kyberprostoru.
5. Koordinační a řídící.

Rozložení a uspořádání v rámci scénářů je možné vidět na obrázku č. 3. Dále budou rozpracovány jednotlivé skupiny úkolů podrobněji.

Odolnost a bezpečnost informací (Information Assurance)

Skupina úkolů zahrnující dva koncepty, odolnost a bezpečnost informací, ale s výrazným přesahem mezi sebou navzájem. Odolnost (Resilience) je „schopnost organizace, systému či sítě odolat hrozbám a čelit výpadkům.“[32] Z vojenského pohledu je nutno dodat, že se jedná o aktivity na vlastních systémech. Z nevojenského pohledu je zasahování do jiných, než vlastních systémů nezákonné, a proto se ani neuvažuje.

32 JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6., s. 78.



Obrázek č. 3: Úkoly vyplývající ze scénářů a jejich uspořádání

Bezpečnost informací je pak spíš pohled státních orgánů. V zákoně o kybernetické bezpečnosti je definována jako „zajištění bezpečnosti důvěrnosti, integrity a dostupnosti informací". Odolnost a bezpečnost informací jsou tak úkoly spojené s budováním, bezpečností a ochranou infrastruktury a informací **vlastních systémů**.[33] Z vojenského pohledu je ještě nutné rozčlenit tuto oblast na kritickou infrastrukturu, vojenskou kritickou infrastrukturu a nasaditelnou infrastrukturu[34].

Zabezpečování informací v kyberprostoru

Zpravodajské služby[35] mají za úkol „získávání, shromažďování a vyhodnocování informací … důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky"[36]. Informace zabezpečují i z kybernetického prostoru. V podstatě se jedná buď o získávání informací z otevřených zdrojů, nebo o kybernetickou špionáž. Na strategické úrovni se informace přímo vztahují k životním zájmům. Další jsou pak informace nutné pro vlastní činnost nebo vedení operací, tedy operační a taktické informace. Informace je možné zjišťovat cestou (skrz) kybernetického prostoru o skutečnostech mimo kybernetický prostor nebo o situaci a aktivitách v kybernetickém prostoru. Ve vojenské terminologii pak jde o strategické, operační a taktické zpravodajské zabezpečení. Úkoly v této skupině jsou úkoly plněny dedikovanými orgány, nejedná se tedy o každodenní získávání informací pro vlastní činnost.

33 Pro další pochopení dělení je nutné ještě jednou zdůraznit – aktivity na vlastních systémech.

34 infrastruktura a sítě pro potřeby nasazených jednotek.

35 Vojenské zpravodajství, Bezpečnostní informační služba, Úřad pro zahraniční styky a informace.

36 Zákon č. 153/1994 Sb., o zpravodajských službách České republiky. In: *Sbírka zákonů*. 1994, § 2.

Kybernetické operace

Skupina úkolů tvořící vlastní jádro úkolů působení v kyberprostoru z pohledu obrany. Souhrn opatření, přípravu a použití kybernetických prostředků ofenzivním nebo defenzivním způsobem, aktivního nebo pasivního charakteru.

Koordinace a řízení

Budoucí operační prostředí, i jeho vyjádření v předcházejících scénářích jasně ukazuje na stírání hranic mezi vnější a vnitřní hrozbou, neurčitostí, zda je nepřátelská aktivita vojenského typu, či kybernetická kriminalita. Není možné se tak na hrozby připravovat a čelit jim v jakýchsi oddělených bublinách, dle organizačních struktur. Bez vzájemné součinnosti, nebo hůře s rivalitou. Úkoly zahrnují koordinaci a vzájemnou synergii všech typů úkolů, vytváření struktur řízení a koordinace, s jasnou zodpovědností a pravomocemi zvláště pak při změnách krizových stavů od nebezpečí až po válečný stav. V čistě vojenské části pak zahrnují začlenění kybernetické domény do plánování a řízení operací, v rámci společného působení všech sil a prostředků k získání převahy nad nepřítelem.

Informační působení v kyberprostoru

Informační působení je zde nejširší pojem zahrnující veškeré aktivity v kyberprostoru. Z pohledu státu pak především vytváření informačně odolné společnosti, strategická komunikace a v jejím rámci pak při vedení operací ozbrojených sil informační operace.

ZÁVĚR

Analýza trendů za pomoci faktorové analýzy PESTLE slouží jako podklad pro aplikaci vojenského pohledu a zpřesnění charakteristik budoucího operačního prostředí.

Budoucnost je plná komplexity[37], rizik, nejistot, hrozeb a příležitostí. Rychlé změny v sociální, vědecké, technologické a environmentální oblasti, jejichž vliv je zvyšován všudypřítomným efektem globalizace, vytvářejí svět plný neznámých a nepředvídatelnosti. Globalizovaný a propojený svět umožňuje rychlé přelévání konfliktů a jejich dopadů i do vzdálených oblastí.[38] Zároveň rozpad bipolárního světa vytvořil prostor k realizaci ambicí i lokálních a nestátních aktérů. Roste význam a centralita informací a kybernetického prostoru a zároveň roste závislost společnosti na bezproblémovém fungování kyberprostoru.

Zpracované scénáře umožňují prozkoumat a rozpracovat možné úkoly, které bude nutné plnit při obraně kybernetického prostoru. Scénáře pokrývají situace od masivního kybernetického útoku v době míru, přes informační působení až po vedení bojových operací ve všech doménách, a tedy i kybernetické.

---

37 *Framework for Future Alliance Operations*. Norfolk, Virginia: North Atlantic Treaty Organisation, Supreme Allied Command Transformation, 2015.FFAO, s.5

38 Dlouhodobý výhled pro obranu 2030. Praha: Ministerstvo obrany, 2015, s. 3-4.

Analýza úkolů vyplývajících ze scénářů napomohla určit následující základní skupiny úkolů: (1) **odolnost a bezpečnost informací** ve vlastních sítích, zajišťujících infrastrukturu a informace v ní uložené. Úkoly (2) **koordinační a řídící** umožní propojit vše dohromady. (3) **Zabezpečování informací v kyberprostoru** přispěje svým dílem do všezdrojového zpravodajství. (4) **Kybernetické operace** a (5) **informační působení** pak přináší aktivní prvek do působení a obrany v kybernetickém prostoru. Na analýzu úkolů navazuje určení požadovaných schopností rezortu obrany a návrh rozdělení rolí, odpovědností a požadovaných schopností, což však přesahuje záměr tohoto článku.

Autoři: ***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.*

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. V současnosti pracuje ve funkci zástupce ředitele speciálních sil Armády České republiky.*

Jak citovat: FEIX, Miroslav and Dalibor PROCHÁZKA. Aktuální úkoly kybernetické obrany rezortu Ministerstva obrany. *Vojenské rozhledy* 2017, 26 (3), 31-50. DOI: 10.3849/2336-2995.26.2017.03.031-050. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz