Ing. Martin HAVLÍK, MBA, MSc.

Sdílení zpravodajských informací v rámci principu „potřeba sdílet“
Sharing of intelligence information in terms of process “need to share”

RECENZOVANÝ ČLÁNEK

Vojenské rozhledy, 2015, roč. 24 (56), č. 2, s. 83–91, ISSN 1210-3292 (tištěná verze), ISSN 2336-2995 (on-line).

Abstrakt:

Hlavním cílem tohoto článku je snaha pojednat o problematice sdílení zpravodajských informací v rámci takzvaného principu „potřeba sdílet – need to share“ a zdůraznit odlišnosti tohoto současného trendu, který měl nahradit princip sdílení informací „potřeba vědět – need to know“. Úvodní část je s ohledem na současné globální bezpečnostní hrozby věnována rozměru současného národního a nadnárodního zájmu ve zpravodajské oblasti, na který navazuje v další části samotná problematika sdílení zpravodajských informací dle principu „potřeba sdílet“. Cílem další části je provedení obecného rozboru sdílení zpravodajských informací v rámci organizace NATO a Evropské unie. Do této časti je zakomponován také popis možného sdílení informací charakteru SIGINT získaných národním taktickým prvkem začleněným do struktury úkolových uskupení v soudobých operacích. Závěrečná část shrnuje podstatu zhodnocení sdílení zpravodajských informací a nastiňuje určitou predikci dalšího vývoje v této oblasti.

Abstract:

The main goal of this article is to depict the issue of intelligence information sharing within the so called principle „need to share“ and highlight the differences of this current trend, which was to replace the „need to know“ principle. The first chapter in reference to current global threats depicts the extent of the present national and international interrest in the intelligence field which is followed by the issue of „need to share“ principle. The aim of the following chapter is briefly analyse the sfaring of intelligence information within NATO and the EU. This chapter also includes the possible sharing of SIGINT information obtained by national tactical element embedded in Task force during current day operations. The final part evaluates the intelligence information sharing and outlines certain prediction of future development in this field.

Klíčová slova:

Zpravodajství, sdílení informací, NATO, Evropská unie, Evropská bezpečnostní strategie, informační a komunikační technologie, sběr dat, hrozby, rizika, terorismus, SIGINT.

Keywords:

Intelligence, sharing of information, NATO, European Union, European security strategy, information and communication technologies, data collection, threats, risks, terrorism, SIGINT.

Úvod

V samotném úvodu je vhodné uvést, že sdílení zpravodajských informací začalo ve větší intenzitě až po teroristických útocích provedených v USA, ke kterým došlo dne 11. září 2001. Praktické zkušenosti se sdílením zpravodajských informací před tímto zlomovým datem měly pouze jednotlivé národní kontingenty (v dnešní době úkolová uskupení) působící v rámci mezinárodních operací, a to jak na území Kuvajtu (osvobozovací operace Pouštní bouře) a Iráku (humanitární operace UNGCI – United Nations Guards Contingent in Iraq), tak zejména na území bývalé Jugoslávie (mírové operace UNPROFOR – United Nations Protection Forces, UNCRO – United Nations Confidence Restoration Operation in Croatia, IFOR – Implementation Forces, SFOR – Stabilisation Forces, KFOR – Kosovo Forces). Zde docházelo již v minulosti v rámci plnění společných úkolů ke sdílení zpravodajských informací, a to zejména taktického a operačního charakteru s cílem naplnit společné cíle stanovené a vymezené mandátem jednotlivých misí. Po avizovaných útocích v září 2001 však vzešla nutnost sdílet zpravodajské informace nejen v prostředí společných nadnárodních misí, ale s ohledem na všude přítomný terorismus také v normálním běžném relativně mírovém prostředí. V této souvislosti vyvstala potřeba nastavit jednotlivé mechanismy sdílení zpravodajských informací mezi spojeneckými zpravodajskými službami, a to nejprve v rámci Evropské unie a NATO (North AtlanticTreaty Organization), později také mezi dalšími spojenci v boji proti světovému terorismu. Samotná problematika sdílení zpravodajských informací a v dnešní době také sdílení schopností se neustále rozvíjí do nových dimenzí a navyšuje se jejich intenzita, a to zejména na bázi organizace NATO a Evropské unie. Tento trend lze s velkou pravděpodobností očekávat i v budoucnu, v krátkodobém a střednědobém horizontu s vysokou určitostí.

„Žádná země nedokáže vyřešit složité problémy současnosti sama.“

Zdroj: [7]

Současné operační prostředí je charakterizováno především jako nestabilní, vyžadující intervenci mezinárodního společenství k opětovnému nastavení stability. Nestabilita je způsobována globalizačními trendy, rozvojem a zpřístupněním nových technologií, demografickými změnami, urbanizací rozsáhlých oblastí, rostoucími požadavky na energetické zdroje, změnami klimatu, přírodními katastrofami, proliferací zbraní hromadného ničení a zhroucenými nebo hroutícími se státy. Tyto trendy zapříčiňují neustálou změnu operačního prostředí, ve kterém se kontinuálně mění koalice, aliance, partnerské vztahy a klíčoví hráči. Změny v současném operačním prostředí s sebou přináší změněné rozhodovací problémy, které se dále promítají ve změněných požadavcích na informační podporu. Ve svém důsledku se změny promítají i v požadavcích na změny zpravodajského zabezpečení. K tomu, aby velitel dospěl ke správnému úsudku, potřebuje informace, které mu umožní provést analýzu operačního prostředí. Pokud bude zpravodajská organizace usilovat o „vlastní schopnost“ nezávisle na znalosti ostatních funkčních oblastí, nástrojů moci a jejich informačních procesech, tak dojde k tomu, že výklad informací (a potažmo také zpravodajských informací) bude rozdílný uvnitř

štábu i mezi organizacemi, zastupujícími ostatní nástroje moci. Tito aktéři si nebudou rozumět a bude docházet k nekoordinovanosti, k rozdílným závěrům a zdlouhavému rozhodovacímu procesu velitelů. Pro činnost zpravodajských orgánů to znamená, že musí zásadně změnit styl práce od separace a utajení, ke spolupráci, koordinaci a otevřenosti vůči ostatním prvkům úkolového uskupení i vnějším aktérům. [1]

Nejen v souvislosti s vývojem nových komunikačních a informačních technologií, ale také v souvislosti s digitalizací (nejen bojiště) je v posledních letech patrný nárůst počtu zdrojů dat a obecně i informací [2], a od toho se samozřejmě odvíjí také nárůst potencionálních zpravodajských informací, které mohou sloužit v rámci rozhodovacího procesu velitele a být taktéž sdíleny s dalšími zpravodajskými subjekty v národním i nadnárodním kontextu.

1. Rozměr národního a nadnárodního zájmu ve zpravodajské oblasti

Pokud budeme brát v potaz současné hrozby, kterým čelí vyspělé státy „západního světa“ a v obecném pohledu také mezinárodní společenství jako celek, je nutné v oblasti sdílení zpravodajských informací a v oblasti společného prosazování zájmů v oblasti bezpečnosti akceptovat pravidlo, že nadnárodní zájem nejen ve zpravodajské oblasti převyšuje v současné době zájmy národní, a to jak zejména s ohledem na rizika a hrozby vyplývající s celosvětového terorismu a možného vzniku Islámského státu, tak také s ohledem na společné úsilí při eliminaci nepokojů především v Africe (Mali, Demokratická republika Kongo), na Blízkém a Středním východě (Sýrie, Irák) a v Asii (Afghánistán). V této souvislosti je velmi důležitým procesem vzájemné sdílení zpravodajských informací mezi jednotlivými (především zpravodajskými) službami a státy a eliminovat případné třecí plochy mezi zájmy národními a nadnárodními (úmyslná konspirace vlastních zájmů, zajištění vlastní suverenity a ochrana národní kritické infrastruktury).

Přestože je z výše uvedeného patrný jasný trend prosazování nadnárodních zájmů na úkor zájmů národních v oblasti sdílení zpravodajských informací, lze i v současné době identifikovat mnohá úskalí a preferované postoje světových velmocí k této problematice (reprezentované zejména USA). Je zcela zřejmé, že se malé státy (včetně například České republiky) budou snažit v maximální možné míře sdílet své zpravodajské informace s cílem společného čelení hrozbám jako např. terorismus; nicméně USA se svými spojenci sdílejí téměř vždy pouze nejnutnější informace, a to pravděpodobně z důvodu udržení si jisté suverénnosti, nadhledu a konkurenční výhody v případných střetech s dosavadními spojenci v budoucnu. Důvodem může být také částečná konspirace vlastních možností získávání zpravodajských informací a také výše nastíněná konspirace oblastí zájmu konkrétních zpravodajských služeb a jednotlivých států. Tyto skutečnosti se nám jeví jako poměrně logické, nicméně popírají společnou snahu zpravodajských subjektů a vlád jednotlivých zemí v maximalizaci úsilí a společném boji právě například proti celosvětově diskutovanému terorismu, který v současné době zejména prostřednictvím takzvaného Islámského státu představuje jednu z nejprioritnějších a nejvážnějších hrozeb, a to nejen pro státy NATO a Evropské unie.

V oblasti nadnárodního zájmu v rámci sdílení národních zpravodajských informací je nutno si uvědomit, že zde vyvstává určitá omezující podmínka týkající se samotného praktického řešení informačních toků a taktéž kompatibility informačních a komunikačních kanálů a systémů. Jak je z uvedeného patrné, existence funkčního informačního a komunikačního systému pro sdílení zpravodajských informací mezi jednotlivými subjekty (zpravodajskými službami, organizacemi, státy) je velmi potřebná. Pokud bereme v potaz nejvyšší, tedy strategickou úroveň, je možné na této úrovni sdílet zpravodajské informace v rámci specifických systémů jako NIWS (NATO Intelligence Warning System) nebo BICES (Battlefield Information Collection and Exploitation System) [3], kde je však už pravděpodobně patrná vyšší limitovanost národními zájmy. Z hlediska institucionálního je možným společným prostorem (subjektem) pro sdílení zpravodajských informací například NIFC (NATO Intelligence Fusion Center), vytvořené v roce 2006 [4][5].

2. Sdílení zpravodajských informací dle principu „potřeba sdílet“

Po ukončení „studené války“ a s ohledem na teroristické útoky v USA v září 2001 došlo v myšlení mnoha významných autorit, předních světových politiků a také v myšlení mnoha zpravodajských důstojníků (analytiků) ke komplexnímu procesu změny s cílem přejít od principu sdílení zpravodajských informací „potřeba vědět – need to know“ k principu sdílení „potřeba sdílet – need to share“. Podle vrcholných představitelů USA se sdílení zpravodajských informací dle principu „need to share“ stalo nutností pro ochranu zejména národní bezpečnosti, a to ihned po avizovaných útocích 11. září 2001. Kultura zpravodajské komunity dle principu „need to know“, důležitá a nutná především v průběhu „studené války“, se v posledních letech a taktéž v současnosti stala výrazným hendikepem ohrožujícím národní schopnosti odhalit, působit a ochránit před terorismem a dalšími asymetrickými hrozbami. Mezi hlavní cíle a záměry v oblasti sdílení zpravodajských informací patří v současné době dle schváleného strategického záměru pro sdílení informací pro období 2011 až 2015 pro DNI (Director of National Intelligence) především:

- Optimalizace a sdílení informací a zpravodajských činností v rámci zpravodajské komunity (IC – Intelligence Community) a také s dalšími partnery a zákazníky s cílem uplatnit výhody v procesu rozhodování.
- Maximalizace a sjednocení schopností zpravodajské komunity s cílem nalézt, zpřístupnit, udržet, uchovat, sdílet a využít informace.
- Maximalizace a sjednocení schopností zpravodajské komunity v oblasti ochrany a zabezpečení informací.
- Zhodnocení, uspořádání a posílení kontrolního systému (mechanismu) k optimalizaci a odpovědnosti v oblasti sdílení informací, a to při dodržení ochrany občanské svobody a soukromí.
- Posílení kultury odpovědnosti v oblasti sdílení informací. [6]

Přestože došlo na základě výše uvedených potřeb ke změně principu sdílení zpravodajských informací, je nutné si uvědomovat také rizika s tímto spojená. Nadále lze ve zpravodajské komunitě očekávat úmyslnou konspiraci vlastních národních zájmů,

a to zejména u světových velmocí. Dalšími zájmy limitujícími rozsah a způsob sdílení informací v principu „need to share“ jsou snahy o zajištění vlastní národní suverenity a ochrana národní kritické infrastruktury. Určitou obavu při sdílení informací může iniciovat také riziko možné ztráty kontroly nad samotným tokem sdílené národní zpravodajské informace v nadnárodních informačních systémech, do kterých jsou stále rozšířenější přístupy v rámci členských států.

V rámci samotného sdílení zpravodajských informací je nutné také reflektovat odlišnosti ve sdílení jednozdrojových informací specifických zpravodajských disciplín a sdílení informací typu „All Source Intelligence“. Zde je potřeba brát v potaz určitá omezení například při sdílení informací typu SIGINT, případně HUMINT (Human Intelligence), kde je snaha o zakrytí samotného původu zdroje těchto informací a v případě sdílení mohou tyto informace vykazovat určitá obsahová zkreslení způsobená provedenou sanitizací. Další úskalí vzniká v posledních letech velmi často u posuzování takzvaných cirkulujících zpravodajských informací, kdy je mnohdy všezdrojovým analytikem potvrzena jedna dílčí informace toutéž informací, jejíž původ se však jeví od jiného zdroje, ač to mu tak ve skutečnosti není a jedná se v podstatě o tutéž informaci (případně částečně obsahově zmutovanou) získanou zprostředkovaně jinými komunikačními kanály, ne však původem z jiného zdroje. Na tyto skutečnosti je nutno brát zřetel zejména v případech, kdy určité potvrzování získaných zpravodajských informací jinými zdroji může mít za následek iniciaci úderných akcí v rámci plnění operačního úkolu, a to nejen v bojových operacích. Přestože bývá původci informací a zpravodajských informací často potlačován samotný zdrojový rámec v rámci určité (úmyslné) ochrany zdrojů, je vhodné pro všezdrojové analytiky produkující výstupní zpravodajské informace sloužící pro rozhodovací proces samotných velitelů uvádět alespoň obecný popis zdroje informací, což může eliminovat právě výše zmiňovanou problematiku cirkulujících (duplicitních) informací a jejich následné vzájemné potvrzování. Mezi další dílčí problémy v oblasti sdílení zpravodajských informací mezi jednotlivými národy (státy) může být také používaný jazyk komunikace, což však v současné době je poněkud na ústupu a jsou dodržovány přijaté konvence v oblasti používání jednotných (světových) jazyků, kdy za prioritní je považována angličtina, následována francouzštinou. Taktéž došlo v posledních letech ke sjednocení (standardizaci) používaných datových formátů (dokumentů), pomocí nichž jsou v rámci společných informačních systémů sdíleny národní zpravodajské informace.

3. Sdílení zpravodajských informací v rámci NATO a EU

V předcházejících částech byla popsána základní potřeba sdílení zpravodajských informací (oddíl 1) a také význam nadnárodního zájmu v této oblasti (oddíl 2), který v současné době (a dá se s určitostí tvrdit, že také v budoucnu) převyšuje zájem národní. Tyto skutečnosti jsou také potvrzeny přechodem od principu sdílení zpravodajských informací „need to know“ k modernějšímu a efektivnějšímu principu „need to share“, kterým se blíže věnuje oddíl 3. V této části bude problematika sdílení zpravodajských informací rozpracována ve smyslu členství České republiky v NATO a Evropské unii,

jakožto dvou významných společenství států s obdobnými zájmy nejen v oblasti kolektivní obrany a bezpečnosti.

Sdílení zpravodajských informací v rámci Evropské unie a NATO dílčím způsobem vymezují zejména *Evropská bezpečnostní strategie* z roku 2003 [7], dále v rámci NATO jsou to *Souhrnná politická směrnice NATO* z roku 2006 [8] a *Strategická koncepce NATO* z roku 2010 [9]. *Evropská bezpečnostní strategie* se primárně věnuje problematice vnějšího rozměru bezpečnosti Evropy.

Evropská bezpečnostní strategie mimo jiné zdůrazňuje, že systematické využívání sdružených a sdílených prostředků může omezit duplicitu, provozní náklady a ve střednědobém horizontu i zvýšit schopnosti. Dále je zde uvedeno, že nejlepším základem pro společné akce Evropské unie jsou společné analýzy rizik, k nimž je zapotřebí kvalitnějšího sdílení zpravodajských informací mezi členskými státy a také s dalšími partnery [7].

Zmiňovaná strategická koncepce NATO upřesňuje mimo jiné také svoji vizi, v závislosti na vývoji bezpečnostního prostředí, poslání a úkolech NATO, včetně záměrů použití sil členských států. Tato koncepce je nepravidelným (neperiodickým) dokumentem, který bývá aktualizován zejména při zásadních změnách bezpečnostního prostředí. Zmiňovaná koncepce z roku 2010 byla sestavena převážně ze závěrů summitu konaného v roce 2009 ve Štrasburku [10][11][12].

V rámci NATO je problematika sdílení zpravodajských informací rozvíjena na všech úrovních (taktické, operační i strategické). Na taktické úrovni jde například o sdílení informací týkajících se improvizovaných výbušných zařízení IED (Improvised Explosive Device) v Afghánistánu. Z uvedeného je pravděpodobné, že nejen tyto společné hrozby vytváří tlak na skutečně funkční systém sdílení informací a taktéž samotné sdílení informací je v této oblasti považováno za prospěšné.

Mnohonárodnostní princip se musí šířit rovnoměrně stádii řízení, shromažďování, zpracovávání a šíření v rámci zpravodajského procesu (zpravodajského cyklu). To bude zahrnovat oblasti jako například vytvoření mnohonárodnostní organizace managementu shromažďování a mnohonárodnostního zapojení do fáze zpracovávání v rámci zpravodajského cyklu [13].

3.1 Praktický příklad možného sdílení zpravodajských informací:

Sdílení informací charakteru SIGINT (Signals Intelligence) získaných národním taktickým prvkem začleněným do struktury úkolových uskupení v soudobých operacích lze pro lepší pochopení znázornit například níže uvedeným grafickým schématem. V této souvislosti je nutné upozornit, že se nejedná o žádné dogmatické znázornění, ale pouze o nastínění možného získávání a sdílení informací charakteru SIGINT, včetně nastínění určitých informačních toků v rámci zasazení taktického segmentu SIGINT do struktury národního úkolového uskupení v soudobých a budoucích operacích. Je nutné si v této spojitosti také uvědomit, že ze strany nadnárodních zájmů v oblasti sdílení zpravodajských informací získaných prostředky signálového zpravodajství je stále větší tlak na sdílení informací na operační úrovni, a to přímo v rámci konkrétní operace, kdy bývá pro tyto potřeby vytvořeno specifické místo označované jako SEWOC (Signals Intelligence Electronic Warfare Operations Center). Zde by mělo docházet ke sdílení

informací získaných prostředky signálového zpravodajství (SIGINT) a elektronického boje (EW – Electronic Warfare) [14]. V současné době si však doposud jednotlivé národní elementy signálového zpravodajství a elektronického boje udržují své určité *know how* a sdílejí pouze velmi omezené množství zpravodajských informací, které jsou navíc značně sanitizované – tedy upravené do takové podoby, aby nebylo možné identifkovat původce a charakter samotného získání tohoto typu informací. Lze tedy v tomto případě tvrdit, že pouze velmi zřídka dochází ke sdílení zdrojových dat, případně i informací, ale dochází pouze k částečnému sdílení finálních (sanitizovaných) zpravodajských informací.

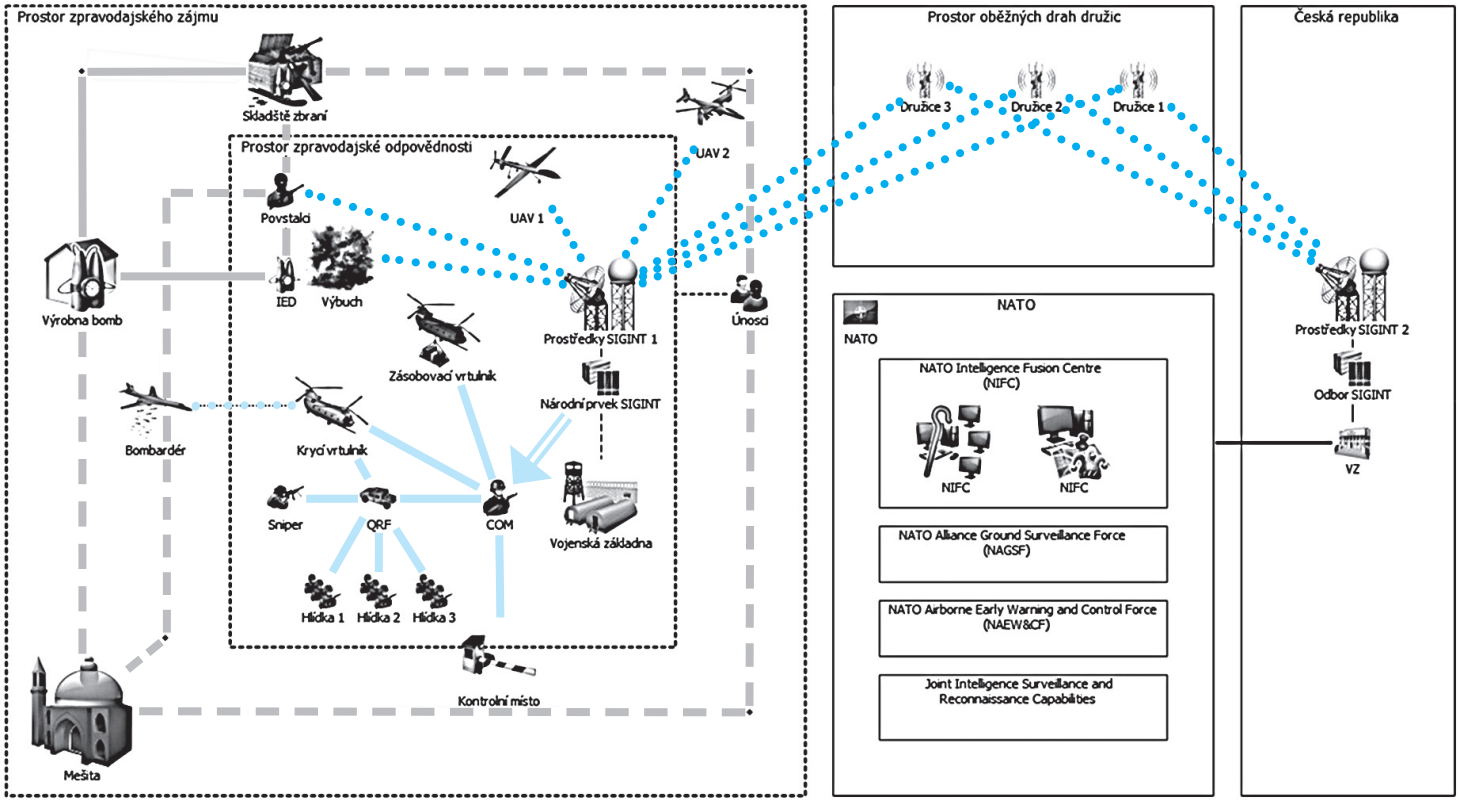
Na schématickém obrázku č. 1 jsou nastíněny možné informační vazby dotýkající se výhradně taktického národního prvku SIGINT začleněného do struktury úkolových uskupení v soudobých operacích s výjimkou úkolových uskupení speciálních sil, kde by pravidla samotného informačního toku byla v současné době nastavena poněkud odlišněji. Začlenění národního taktického prvku SIGINT do sestavy úkolového uskupení speciálních sil, respektive popis této možné varianty přesahuje rozsah tohoto článku. Vzhledem k provedené reorganizaci k 1. lednu 2015, kdy české speciální síly přešly z podřízenosti Vojenského zpravodajství, respektive z podřízenosti Ředitele Vojenského zpravodajství, do podřízenosti Náčelníka generálního štábu (NGŠ), lze však s velkou pravděpodobností usuzovat, že případné zapojení národního taktického prvku SIGINT do struktury úkolových uskupení speciálních sil v budoucích operacích bude v oblasti informačních toků založeno na velmi podobném organizačním schématu, jak je nastíněno výše, s tím, že zde bude kladem větší důraz na sdílení informací v rámci principu „need to share“ s přímou intenzivnější podporou rozhodovacích procesů velitele konkrétního úkolového uskupení speciálních sil.

Legenda k obr. č. 1 (na následující stránce)

Potvrzené a pravděpodobné vazby monitorovaných objektů nepřítele v rámci sledovaného prostoru zpravodajského zájmu (AoII – Area of Intelligence Interest) včetně prostoru zpravodajské odpovědnosti (AoIR – Area of Intelligence Responsibility).

Komunikační vazby mezi velitelem určitého úkolového uskupení (COM – Commander) a jednotlivými prvky konkrétního úkolového uskupení, včetně prostředků zabezpečující podporu těmto prvkům.

Možné komunikační kanály využívané taktickým národním prvkem SIGINT, a to jak k monitorování sledovaných zájmových objektů v rámci prostoru zpravodajského zájmu, tak rovněž ke komunikaci s ústředím v České republice, případně s prvky a prostředky podpory v rámci konkrétních operací.



Obrázek č. 1: Možnosti informačních toků u taktického národního prvku SIGINT v soudobých operacích.

Zdroj: Vlastní zpracování autora s využitím softwarového produktu IBM i2 Analyst's Notebook 8.

Závěr

V této závěrečné části je nastíněna problematika sdílení zpravodajských informací v budoucnosti, a to zejména v souvislosti s nárůstem objemu sdílených informací, kdy je patrný trend související obecně s růstem dat, potažmo informací a také zpravodajských informací ve společném boji bezpečnostních subjektů s aktuálními i budoucími hrozbami. Trend růstu obejmu informací je v přímé korelaci s poznatky z oblasti fenoménu Big Data, kde mimo nárůst objemu informací je sledován také vývoj v oblasti informačních a komunikačních systémů a také v oblasti digitalizace. S tímto problémem souvisí také nárůst počtu zdrojů samotných dat (v budoucnu také ve spojení s oblastí kybernetických činností všeho druhu), a od toho se samozřejmě odvíjí také nárůst potencionálních zpravodajských informací, kterou mohou sloužit v rámci rozhodovacího procesu velitele a být v jakékoliv fázi sdíleny.

Smyslem v následujících letech bude stále efektivněji nahrazovat velmi nákladné lidské zdroje a urychlit proces jednotlivých zpravodajských analýz specifických zpravodajských disciplín, a to primárně v návaznosti na všezdrojové zpravodajství (All Source Intelligence). Správně interpretovaná data budou v budoucnu předpokladem k tomu, aby zpravodajské subjekty lépe porozuměly vnitřním procesům a hledaly nové způsoby, jak minimalizovat všechna související rizika, efektivněji hospodařit a zejména věrohodněji a v reálném čase predikovat budoucí vývoj bezpečnostního prostředí se všemi zájmovými faktory a ukazateli. Budoucí cesta ve sdílení a využívání dat velkého objemu (včetně zpravodajských informací) je v hledání trendů a aspektů, které tyto trendy přímo či nepřímo ovlivňují, a poté se těchto trendů držet (pokud prezentují příležitosti) nebo se jich vyvarovat (pokud prezentují hrozby). Hlavní přínosy nových trendů pro ovlivněné zpravodajské disciplíny (zejména SIGINT, ELINT, COMINT, IMINT a FISINT) lze do budoucna spatřit v samotném novém propojení dat do souvislostí (vizualizace událostí a aktivit zájmových zpravodajských subjektů), což přináší dle nejnovějšího zjištění narůstající možnosti nových pohledů na sledované subjekty a také výše avizované snížení nákladů na lidské zdroje. Do budoucna lze dále očekávat, že se bude stále více rozvíjet sdílení dat velkého objemu z veřejných datových zdrojů (rejstříky státní správy, informační databáze a služby nejrůznějšího charakteru, apod.). Nejdůležitějším záměrem pro zpravodajské služby by mělo být to, abychom se nevěnovali hlavním úsilím popisu stávajících jevů (to, co se v oblastech zpravodajského zájmu událo), ale naopak výhradně predikci toho, co může v budoucnu nastat v nejrůznějších pravděpodobnostních variantách, a jak na tyto možnosti reagovat v rámci řízení možných rizik.

Na významu budou nabývat také citlivá data sdílená prostřednictvím moderních sociálních sítí (Facebook, Twitter, Google+, LinkedIn, Naymz, Xing, MySpace, Orkut, Bebo, Classmates, Friendster, Hi5, Blackplanet atd.). S nárůstem objemu dat bude v budoucnu také narůstat potřeba na vysoký výpočetní výkon počítačů a změnu základní počítačové architektury, kdy bude využíváno sdíleného výkonu, pozornost bude věnována zrcadlení diskových polí, vzdáleným úložištím a podobně. Mezi nejrozšířenější metody bude pravděpodobně patřit Data Mining, simultánní zpracování dat (Massively Parallel Processing, MPP), strojové učení (Machine Learning) a prediktivní modelování v návaznosti na rozhodovací procesy velitelů (nejen v oblasti zpravodajských služeb) [15].

Pokud budeme chtít v budoucnu efektivně sdílet zpravodajské informace, budou muset jednotliví partneři (státy, zpravodajské služby) minimalizovat rozdíly v zavedených

a používaných doktrínách, operačních postupech, technickém vybavení a zbraňových systémech, sjednotit komunikační a informační systémy ve smyslu vzájemné kompatibility a minimalizovat rozdíly v jazykových znalostech a kulturních odlišnostech. Jen takto lze společným úsilím efektivně využívat sdílené zpravodajské informace a také sdílet vlastní schopnosti ve společném boji proti současným globálním i regionálních hrozbám reprezentovaným zejména terorismem. Ve světě globálních hrozeb, globálních trhů a globálních médií je nutná mnohostranná spolupráce, dobře fungující národní i nadnárodní instituce a společný mezinárodní řád.

Poznámky k textu a použitá literatura

[1] HORÁK, O. *Zpravodajská informace a zpravodajský cyklus.* Skripta, VA Brno, 2004. 175 s.
[2] AAP-6, NATO Glossary of Terms and Definitions (English and French). NATO Standardization Agency, 2010. 451 s.
[3] KRIENDLER, J. 2002. *Předjímání krizí* [on-line]. NATO Review. [cit. 2015-01-15] Dostupné z: http://www.nato.int/docu/review/2002/issue4/czech/art4.html
[4] CRS Report for Congress. *Intelligence and Information Sharing Elements of S.4 and H.R.1.* [on-line]. 2007 [cit. 2015-02-10] Dostupné z: http://fas.org/sgp/crs/intel/RL34061.pdf
[5] MIXON, L. M. 2007. *Requirements and Challenges Facing The NATO Intelligence Fusion Center* [on-line]. Air War College, Air University. [cit. 2015-02-01] Dostupné z: https://www.afresearch.org
[6] Office of the Director of National Intelligence. 2011. *Strategic Intent for Information Sharing 2011–2015* [on-line]. [cit. 2015-02-03] Dostupné z: http://www.dni.gov/files/documents/Strategic%20Intent%20for%20Information%20Sharing.pdf
[7] *Evropská bezpečnostní strategie* [on-line]. 2003 [cit. 2015-01-08] Dostupné z: http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIICS.pdf
[8] *Souhrnná politická směrnice NATO* [on-line]. 2006 [cit. 2015-01-10] Dostupné z: http://www.mocr.army.cz/scripts/detail.php?id=146
[9] *Strategická koncepce NATO* [on-line]. 2010 [cit. 2015-01-10] Dostupné z: http://www.mocr.army.cz/scripts/detail.php?id=146
[10] AJP-2.1 (A), Intelligence Procedures. Brusels: NATO Standardization Agency, 2005, 231 s.
[11] NATO. NATO‘s new Strategic Concept. Why? How? [on-line]. 2010 [cit. 2015-01-15] Dostupné z: http://www.nato.int/strategic-concept/what-is-strategic-concept.html
[12] RAŠEK, A. *NATO připravuje novou strategickou koncepci.* Vojenské rozhledy, 2010, roč. XIX (LI), č. 2, s. 3–21. ISSN 1210-3292.
[13] OTŘÍSAL, P. *Vnímání bezpečnostních hrozeb v oblasti CBRN – historie a výzvy.* Vojenské rozhledy, 2013, roč. 22 (54), č. 1, s. 00-00, ISSN 2010-3292.
[14] Pub-20-63-03, *Elektronický boj v AČR*. 1. vyd. Vyškov: Odbor doktrín VeV-VA, 2010. 58 s.
[15] JARED, D. *Big Data, Data Mining, and Machine Learning.* Wiley, 2014, 288 s. ISBN 978-1-118-92069-5.