Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Diplomová práce

2007 **Bc. Václava Hammerová**

Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Studijní program: informační studia a knihovnictví

Studijní obor: informační studia a knihovnictví

Bc. Václava Hammerová

Veřejně přístupné informační zdroje pro oblast vojenství

Diplomová práce

Praha 2007

Vedoucí diplomové práce: PhDr. Richard Papík, Ph.D.

Oponent diplomové práce:

Datum obhajoby:

Hodnocení:

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracovala samostatně a že jsem uvedla všechny použité informační zdroje.

V Praze 17. srpna 2007

……

podpis diplomanta

Poděkování:

Ráda bych poděkovala vedoucímu své diplomové práce PhDr. Richardu PAPÍKOVI, Ph.D. za vstřícný přístup při jejím zpracování a také za podnětné náměty. Zároveň bych ráda poděkovala Ing. Martě LUKAČOVSKÉ za ochotu, cenné rady a konzultace.

Identifikační záznam

HAMMEROVÁ, Václava. *Veřejně přístupné informační zdroje pro oblast vojenství [Public Open Information Sources in Defence and Military Areas*]. Praha, 2007. 83 s. Diplomová práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví 2007. Vedoucí diplomové práce PhDr. Richard Papík, Ph.D.

Abstrakt

Tématem diplomové práce je problematika veřejně přístupných informačních zdrojů pro oblast vojenství. Práce si klade za cíl základní analýzu současných informačních systémů pro oblast vojenství z veřejně dostupných zdrojů a jejich vyhodnocování. V úvodu se práce zabývá vývojovými tendencemi ve vojenství a legislativními východisky pro informační systémy. Hlavní pozornost je zaměřena především na informační zdroje využívané armádami, zejména armádou České republiky. V další části práce provádí srovnávací analýzu, která poskytuje ucelený přehled o informačních zdrojích v oblasti vojenství. Vymezuje význam informací a organizace informačních systémů, podává základní informace o současném stavu a vysvětluje požadavky na informační systémy ve státní správě. Je v ní poukázáno na možná bezpečnostní rizika při poskytování informací v rámci veřejných zdrojů. V závěru práce jsou, na základě zkušeností, úvah a názorů autora, navržena obecná doporučení pro optimalizaci využívání informací ve vojenském výzkumu, vojenském školství a vojenské praxi.

Klíčová slova

Informační zdroje, informační systémy, databáze, vojenství, Ministerstvo obrany, armáda České republiky

OBSAH

PŘEDMLUVA

Tématem mé diplomové práce je problematika veřejně přístupných informačních zdrojů pro oblast vojenství. Toto téma jsem si zvolila zejména z důvodu, že mi je oblast vojenství profesně blízká, vzhledem k mé dlouholeté praxi na Ministerstvu obrany. Problematika informačních zdrojů mě zaujala již v rámci studia na Ústavu informačních studií a knihovnictví, kde jsem se mimo jiné v rámci výuky seznámila s některými otevřenými informačními zdroji.

Téma považuji za významné, neboť přístup k veřejným informačním zdrojům z oblasti vojenství je v poslední době uživateli velmi žádaný. Vyhledávání v těchto systémech nabízí armádě možnost oslovit širokou veřejnost a poskytnout informace o své činnosti. Současný stav informačních systémů ve vojenství je v České republice málo zmapovaný a z tohoto důvodu jsem považovala zpracování tohoto tématu za výzvu, ale i za možnost obohatit si své znalosti a zkušenosti.

Práce je vypracována v souladu se schváleným zadáním. Jejím cílem je provést základní analýzu informačních systémů pro oblast vojenství z veřejně dostupných zdrojů s jejich vyhodnocením a názorem na optimalizaci jejich využívání.

Diplomovou práci jsem si pomyslně rozčlenila do dvou částí. Práce je dále dělena na kapitoly a podkapitoly. První část je věnována základní analýze současného stavu informačních systémů pro oblast vojenství. Jsou zde uvedeny a analyzovány informační systémy, které jsou Ministerstvem obrany České republiky v současné době využívány. V druhé části jsem zúročila svou praxi, a vlastní poznatky získané při využívání veřejně přístupných informačních zdrojů a použila jsem metodu zobecnění problému a na základě toho jsem se snažila doporučit postup pro optimalizaci využívání informací ve vojenském výzkumu, vojenském školství a vojenské praxi.

Při psaní diplomové práce jsem informace čerpala pouze z otevřených zdrojů, právních norem, odborných knih, periodik, internetu a z vlastních praktických zkušeností.

Použitá literatura je citována v souladu s normami ISO 690 a ISO 690-2.

1. ÚVOD

Obsahová orientace práce je soustředěna na skutečný stav zavádění moderních informačních technologií v oblasti veřejné správy a vojenství. V textu práce jsou zařazena četná definiční vymezení pojmů, které jsou očíslovány a vysvětleny i v poznámce pod čarou.

Diplomová práce je rozdělena do pěti kapitol, které představují hlavní okruhy problematiky veřejně přístupných informačních zdrojů pro oblast vojenství. Kapitoly jsou dále členěny do podkapitol, ve kterých je pak daný problém podrobněji rozebrán.

Kapitola první řeší úvod práce, otázky cílů při zpracování diplomové práce.

Ve druhé kapitole je analyzován současný stav informačních systémů pro oblast vojenství. Samostatná podkapitola je věnována pojetí vojenství a jeho vývojovým tendencím, legislativním východiskům pro informační systémy veřejné správy, významu informací a znalostí, systému integrované společnosti a e-Governmentu. Značná pozornost je věnována srovnávací analýze některých veřejně přístupných informačních zdrojů zaměřených na činnosti v oblasti vojenství..

Třetí kapitola je zaměřena na obecné a specifické požadavky na informační systémy ve státní správě a v podmínkách vojenství, a na zvláštní odpovědnost na úseku informační bezpečnosti. Samostatnou podkapitolou je dále systém odborných vědeckých vojenských informací v ČR.

Výsledky diplomové práce – doporučení pro optimalizaci využívání informací ve vojenském výzkumu, vojenském školství a vojenské praxi je obsaženo ve čtvrté kapitole. Samostatné podkapitoly řeší moderní telekomunikační technologie, průběh informatizace vojenství a efektivnost vojenských činností při nasazování moderních informačních technologií.

Pátá kapitola – závěr řeší celkové shrnutí diplomové práce a možnost její využití v praxi.

Masové nasazení výpočetní techniky v mnoha oborech lidské společnosti dalo v průběhu posledních let vzniknout velkému množství údajů v elektronické podobě. V souvislosti s tím vzniká v rostoucí míře problém jejich dlouhodobého uložení, přenositelnosti, dlouhodobé čitelnosti a využitelnosti v nejrůznějších prostředcích. Tento problém se týká mnoha oborů a to od počátku vzniku informace, vyhledávání

a využívání až po archivnictví, oboru, jehož úkolem je uchovávat a zpřístupňovat široké veřejnosti údaje o archiváliích a archiválie samotné. Všechny archivy v ČR disponují již zhruba deset let programem PevA[1], vyvinutým odborem archivní správy a spisové služby MV. Jeho zjednodušenou verzi využívají občané od roku 2001 v podobě webové databáze Archivní fondy a Sbírky ČR[2] na webových stránkách ministerstva vnitra (dále jen MV) http://www.mvcr.cz/archivnictvi/. S uchováním a zpřístupněním archiválií souvisí zákon č. 499/2004 Sb., o archivnictví a spisové službě a prováděcí vyhlášky k tomuto zákonu č. 645/2004 Sb., a č. 646/2004 Sb., které předepisují státním a dalším subjektům zajistit odbornou správu dokumentů vzešlých z jejich činnosti nebo v souvislosti s ní, včetně dokumentů právních předchůdců a dokumentů přijatých od jiných osob, tzn. vykonávat spisovou službu písemnou formou nebo elektronickou formou za použití výpočetní techniky. Tyto subjekty musí dbát o řádnou evidenci dokumentů, jejich bezpečné uložení a při skartačním řízení o dodržení zákonných postupů. Uvedený zákon zavádí v **§** 3 pojem **veřejnoprávní původce**[3] a **soukromoprávní původci**[4] dokumentů, § 63 pak zpřesňuje, kdo má povinnost vykonávat spisovou službu v rozsahu podle tohoto zákona a tyto subjekty označuje jako určené původce dokumentů. Určeným původcům zákon stanoví v § 83 povinnost vydat do 6-ti měsíců ode dne nabytí účinnosti zákona vnitřní směrnici pro výkon spisové služby, jejíž součástí bude Spisový a skartační řád, který bude v souladu se zmíněným zákonem a dále Spisový a skartační plán. Povinnosti podnikatelského subjektu v oblasti spisové služby dále významným způsobem precizuje speciální legislativní úprava např. v oblasti vedení účetních záznamů, daňovém řízení, správním řízení, trestním řízení, občanském soudním řízení a dále pro účely sociálního zabezpečení, veřejného zdravotního pojištění a ochrany autorských práv. Tato speciální legislativní úprava zasahuje

[1] **PevA** – program vytvořený odborem archivní správy MV ČR, ve kterém archivy vedou základní evidenci archiválií. Jakýkoli badatel se tak může dozvědět, kde se nalézá příslušný archivní fond nebo archivní sbírka.

[2] Evidence archiválií publikovaná formou databáze na webových stránkách MV ČR.

[3] **§ 3 , odst. 1: veřejnoprávní původci** - organizační složky státu, státní příspěvkové organizace, státní podniky, územní samosprávné celky, organizační složky a právnické osoby založené nebo zřízené územními samosprávnými celky, pokud vykonávají veřejnou správu nebo zaměstnávají více než 25 zaměstnanců, školy a vysoké školy, právnické osoby zřízené zákonem, zdravotnická zařízení.

[4] **§ 3 , odst. 2: soukromoprávní původci** - podnikatelé zapsaní v obchodním rejstříku, pokud jde o dokumenty uvedené v příloze č. 1 k zákonu, politické strany, politická hnutí, občanská sdružení, odborové organizace, organizace zaměstnavatelů, církve a náboženské společnosti, profesní komory; členové profesních komor jen v případech, pokud dokumenty vzniklé z jejich činnosti jsou veřejnými listinami, nadace a nadační fondy, obecně prospěšné společnosti, likvidátoři v případě dokumentů

zejména do délky skartačních lhůt vyplývajících z obecné legislativní úpravy a v určitých případech je výrazně prodlužuje.

Archivnictví a spisová služba velice úzce souvisí se zákonem č. 257/2001 Sb., o knihovnách a podmínkách provozování veřejných knihovnických a informačních služeb (knihovní zákon). Archivy a knihovny zpřístupňují široké veřejnosti oficiální dokumenty jednak o historii i současnosti, čímž představují bohaté veřejné informační zdroje pro každého jedince, ale i pro vývoj i výzkum.

Při vyhledávání informací se můžeme rozhodnout, zda chceme využít stovky a tisíce různorodých zdrojů na internetu pomocí vyhledávacích nástrojů nebo zájmových témat prostřednictvím klíčových slov, anebo zda chceme pracovat se zdroji pokud možno soustředěnými do jednoho místa - pomocí databázových center, která jsou téměř vždy založená na profesionálních a komerčních základech.

Orgány veřejné správy poskytují informace na internetu v souladu se zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (dále jen ISVS) v rámci projektu Portál veřejní správy (dále jen PVS).

Se získáváním informací z veřejných informačních zdrojů souvisí počítačová gramotnost, která se šíří od dětí v základních školách až po kluby seniorů. V posledních 5 letech zažívá Česká republika (dále jen ČR) boom rozvoje internetu. Svět internetu je stále bohatší a nabízí svým uživatelům nejen nepřeberný oceán informací formou veřejně přístupných informačních zdrojů, ale také stále více zajímavých služeb. Těžko bychom hledali úřad, veřejnou instituci nebo město bez webové stránky. Tento pozitivní trend na jedné straně skýtá nečekané možnosti získávání informací, e-learingu, v komunikaci veřejné správy s občany apod. Na druhé straně však přináší i jistá rizika v oblasti bezpečnosti elektronické komunikace.

Přístup k veřejnému internetu zabezpečují internetové kavárny nebo infocentra za stanovený poplatek. Asi úplně nejjednodušší je vyhledat místní knihovnu, kterou najdeme v každém městě a skoro v každé obci, protože knihovní

---

původce, který je v likvidaci, a správci konkursní podstaty v případě dokumentů původce, na kterého byl prohlášen konkurs.

zákon uložil knihovnám a jejich provozovatelům zabezpečit do konce roku 2007 připojení k internetu. Podle dostupných informací nabízí 4000 knihoven a jejich poboček přístup k veřejnému internetu a to bez poplatků, internet zde je opravdu pro všechny. Navíc - knihovna je příjemné a neutrální místo, kam můžeme zajít se svým dítětem, nebojí se tam chodit senioři nebo ženy z domácnosti. Kladem je, že při práci s počítačem rádi poradí pracovníci knihoven.

Současným trendem je bezpochyby automatizace a elektronizace zavedených procesů a agend, které v tištěné podobě s sebou přinášejí výraznou administrativní zátěž ve všech oborech společnosti. Věřím, že ve velmi blízké budoucnosti bude zavedena i elektronická veřejná správa, tzv. e-Government, čímž překročíme pomyslný práh mezi elektronickou informovaností a plně elektronickým výkonem státní správy. Připravovaný zákon o e-Governmentu zrovnoprávní listinné a elektronické formy úředních dokumentů a výrazně zefektivní práci samotných úřadů, zejména v nakládání s dokumenty. Zavede bezpečnou a jednoznačnou identifikaci subjektů a v konečném efektu zjednoduší, zrychlí a přiblíží veřejnou správu občanům a podnikům. Nahradí papírové dokumenty za elektronické, zefektivní jejich oběh, vyhledávání a vytvoří vazby spisové služby, archivu a knihovnictví.

Elektronizace ukáže občanům i firmám viditelné a využitelné výsledky. Umožní efektivně pracovat, výhodně podnikat a důstojně žít. Praxe ukazuje, že právě občané čím dál tím víc upřednostňují elektronickou podobu minimálně při jednoduchém vyplňování.

Přístup k elektronickým informacím veřejně přístupných informačních zdrojů by měl ovšem probíhat bez zbytečných komplikací s využitím moderních informačních technologií (dále jen IT), které zajistí nejen všechny klíčové parametry, ale poskytnou i komplexní nabídku dalších služeb.

2. ZÁKLADNÍ ANALÝZA SOUČASNÉHO STAVU INFORMAČNÍCH SYSTÉMŮ PRO OBLAST VOJENSTVÍ

Základní analýza současného stavu informačních systémů bude vycházet z aktuální situace vojenství a probíhajících projektů v rámci informační společnosti.

2.1 Pojetí vojenství, jeho omezení a vývojové tendence v 21. století

Se vstupem do 21. století se v myslích mnoha lidí, a to platí samozřejmě i pro ty, kteří se zabývají otázkami bezpečnosti, vynořila otázka, co nás v tomto století čeká. Jaká bude povaha ozbrojených sil a válek budoucnosti? Jaká bude forma ekonomického zabezpečení? Budou ozbrojené síly, ekonomické zabezpečení a války jen obdobou toho, co jsme dosud poznali? Z vlastní zkušenosti můžeme říci, že i oblast vojenství se v rámci globalizace radikálně mění. Zdrojem technologického rozvoje moderních prostředků využitelných pro vojenské účely již není, na rozdíl od období studené války, výhradně uzavřený sektor vojenského výzkumu, vývoje a výroby, nýbrž otevřená civilní komerční sféra. Z výše uvedených důvodů je účelné se společně zamyslet nad některými klíčovými problémy, které s touto budoucností bezprostředně souvisejí, a to hlavně proto, aby se staly předmětem společného hledání konsenzu ve sféře státní bezpečnostní politiky, občanské a vojenské veřejnosti.

Není sporu o tom, že moderní válka se bude týkat téměř všech občanů ať přímo nebo nepřímo; že bude vedena výzbrojí, jež se bude používat v množství daleko menším než v předcházejících světových konfliktech. Celá řada poznatků hovoří ne o mobilizaci lidských zdrojů pro vedení války, ale ve prospěch vojenských akcí, operací, konfliktů a úderů. Úroveň masové mobilizace nelze udržet bez moderní, industrializované a vysoce produktivní ekonomiky a bez ekonomiky v rukou nebojujících složek populace. Změna charakteru světového hospodářství změnila i armády, které byly vytvořené především pro ochranu země. Žádná armáda není schopna dobývat vědu nebo kyberprostor. Zkušenosti dokazují, že pokud jsou v dnešní době povoláni k řešení bezpečnostního incidentu vojáci, musí umět něco víc než jen bojovat. Mírové operace ukazují, že kromě schopnosti bojovat vojáci

potřebují řadu dalších dovedností, aby mohli obsáhnout široké spektrum namáhavých a náročných rolí. Musí mít dovednosti od diplomata přes policistu a vyjednavače, pracovníka první pomoci, ředitele nemocnice nebo pracovníka městské správy – tzn. voják profesionál. V přípravě vojenských profesionálů dochází k výkladu problémů krize, pokroku a humanismu, úlohy morálky a etiky ve vývoji společnosti, pojetí bezpečnostní politiky a ekonomických otázek národní bezpečnosti. Důležité místo má také otázka poznání dějinných souvislostí vývoje společnosti. To vše předpokládá výklad filozoficko-metodologických principů vědeckého myšlení a vojensko-vědeckého poznání. Vojáci musí být pružnější, lépe vycvičení a vzdělanější. To vyžaduje jak změny v bezpečnostním uvažování, tak změny v celkových bezpečnostních investicích.

Největším nedostatkem je udržování bojových dovedností v případě, že struktury sil jsou omezeny. V uplynulých letech s tím, jak se zbraně a technika zdokonalovaly, rostly náklady na jejich modernizaci velmi rychle. Pokud je procento hrubého domácího produktu vyčleněné na obranu konstantní ve stanovené výši, a pokud HDP každoročně neroste v reálných hodnotách o značnou částku, vedou náklady na nákupy nevyhnutelně k redukci sil. Jestliže nás nutí k redukci armády náklady, nebudeme moci udržovat špičkové síly a udržovat vyváženou armádu schopnou všech funkcí. Již Xenofon v díle Oeconomicus, hovoří o nutnosti slaďovat a koordinovat všechny záležitosti od vedení státu až po vedení armády.

Problémy vojenství jsou dnes pro všechny země velké a naléhavé zároveň. Ačkoliv neexistují hotové odpovědi, je zřejmé, že cesta vpřed bude vyžadovat zvýšenou transparentnost v obranném plánování a společný přístup. Ať už strategie bezpečnosti století budou jakékoliv, myšlenka bezpečnosti zajišťované společnými silami je jediný rozumný přístup. Všechny mezinárodní instituce (NATO, Evropská unie a Organizace pro bezpečnost a spolupráci v Evropě) mají zájem na spolupráci v oblasti vojenství..

2.1.1 Vývojové tendence ozbrojených sil České republiky

Reforma ozbrojených sil citlivě postihuje současné tendence ve vojenství a rozvoj nových technologií. Moderní vojenství pružně reaguje na požadavky

společnosti a její vývoj. Z toho důvodu se ve vojenství klade čím dál větší důraz na preventivní úlohu ozbrojených sil a je vůle, aby se jejich ničící síla v bojových operacích využívala jen v případech, kdy prevence selhala. Spektrum vojenských operací se rozšiřuje i o operace nebojové (stabilizační a podpůrné). Současně se zvyšuje podíl ozbrojených sil v záchranných operacích a v asistenčních činnostech. Toto pojetí operací ozbrojených sil však vyžaduje přesně rozpoznat klíčová strategická místa protivníka a vytvořit vlastní schopnosti působit proti nim. Do popředí se dostává význam získávání, vyhodnocování, využívání a distribuce informací, zejména zpravodajskými orgány. Schopnost aktivní komunikace s veřejností, spolupráce se sdělovacími prostředky, civilně-vojenská spolupráce, ale i informační a psychologické operace, se stávají významnou součástí bezpečnostního systému. Dokonalé informace umožňují ještě před vznikem konfliktu získat a využít varovací dobu, v které se ozbrojené síly mohou na případný konflikt připravit.

Současný stav Armády ČR je výsledkem téměř deseti let reorganizací, transformací a postupných změn. Základním cílem současné reformy ozbrojených sil ČR je zvýšit schopnosti ozbrojených sil při zabezpečování obrany našeho státu s využitím zdrojů, které má ČR na obranu k dispozici ve střednědobém i dlouhodobém horizontu. Počítá s maximálním využitím přínosu našeho členství v NATO, ale zároveň předpokládá, že ČR bude plnit závazky, které z členství vyplývají. Reforma vychází z obecně platného faktu, že ani sebedokonalejší a sebesilnější stát a jeho bezpečnostní a obranný systém nemůže svými schopnostmi eliminovat veškeré hrozby, které jsou součástí bezpečnostního prostředí. Počítá tedy programově s tím, že je vždy nutné přijmout určitou úroveň rizika. Hlavním úkolem reformovaných ozbrojených sil ČR zůstane rozvíjet schopnosti čelit vojenským hrozbám a podílet se na celkových schopnostech bezpečnostního systému státu vypořádat se i s nevojenskými hrozbami. Toto poslání plní profesionální ozbrojené síly, které jsou méně početné, ale lépe vyzbrojené, mobilní a operativnější.

Důležitým předpokladem pro definici požadavků dlouhodobého koncepčního rozvoje je stanovení úrovně vojensko-politických ambicí. ČR jako stát, který chce sehrávat určitou roli v bezpečnostním prostředí dnešního světa, má své vojensko-politické ambice rozpracovány ve třech variantách:

a) bude schopna zúčastnit se všemi svými vojenskými silami v operaci, která bude součástí společné obrany členských států Aliance podle článku 5 Washingtonské smlouvy; v silách mohou být zahrnuty i zálohy;
b) bude schopná vyslat do jedné operace na prosazení míru kontingent, který bude odpovídat brigádě pozemních sil v počtu do 5000 osob nebo podobnému prvku vzdušných sil (avšak až od roku 2007), na dobu maximálně šesti měsíců (bez rotace); současně bude schopná přijmout síly Aliance na vlastním teritoriu a také zabezpečit aktivní účast AČR v systému ochrany vzdušného prostoru (NATINEADS);
c) bude schopna dlouhodobě se účastnit jedné operace na podporu, resp. udržení míru tím, že vyšle kontingent, který bude odpovídat praporu pozemních sil v počtu do 1000 osob nebo podobnému prvku vzdušných sil; současně bude schopna vyslat druhý kontingent v síle do 250 osob po dobu maximálně šesti měsíců (bez rotace, po dosažení počátečních operačních schopností s rotací) do další následně vzniklé a současně probíhající operace (humanitární pomoc, odstraňování následků katastrof apod.); dále bude schopna přijmout síly Aliance na vlastním teritoriu a zabezpečit aktivní účasti AČR v systému ochrany vzdušného prostoru (NATINEADS).

Ve všech variantách si zachová schopnost plnit úkoly, které vyplývají ze zákonů ČR, na teritoriu státu. Svým složením, ale i kvalitou, bude plně srovnatelný s kontingenty vyspělých zemí světa. K jeho vyslání nebude zároveň třeba přijímat žádná zvláštní nesystémová opatření, zejména pokud se týká přidělování dalších zdrojů mimo rozpočtovou kapitolu Ministerstva obrany. Po dosažení cílových operačních schopností, to znamená po celkovém dokončení reformy v dalším časovém horizontu, budou ozbrojené síly schopny plně zabezpečit stanovené úkoly a cíle. Ty se promítnou v úrovni vojensko-politických ambicí v rámci rozpočtové kapitoly Ministerstva obrany včetně eventuálního využití systému předběžných a mobilizačních opatření v případě stavu ohrožení státu nebo válečného stavu v ČR.

Výzkum a vývoj je zaměřen do oblastí koncepce, politiky a strategie bezpečnosti, obrany, výstavby, přípravy a činnosti ozbrojených sil, ekonomiky obrany, sociálních a etických aspektů bezpečnosti a obrany.

2.2 Legislativní východiska pro informační systémy veřejné správy

Legislativní normy ČR vychází z **Ústavního zákona**, do kterého byla zapracována Listina základních práv a svobod, a od kterého se odvíjí všechny právní normy ČR. Z obecného hlediska dělíme právní normy na:

a) **Primární právní normy** jsou tvořeny zákony k bezpečnosti informací, které mají celorepublikovou působnost; v odborných publikacích jsou rovněž nazývány pojmem „*zákonné normy*".

b) **Sekundární právní normy** jsou tvořeny vyhláškami NBÚ, nařízeními vlády, apod., které se váží k bezpečnosti informací. Zvláštní skupinu tvoří interní normativní akty (dále jen INA), např.: Odborné pokyny bezpečnostního ředitele MO (dále jen BŘ MO), Odborné instrukce BŘ; Rozkazy ministra obrany (dále jen RMO) apod. V odborných publikacích jsou rovněž nazývány pojmem „*podzákonné normy*". Podrobněji rozpracovávají danou problematiku na konkrétní podmínky, nesmí být v rozporu s primárními právními normami, ale musí z nich vycházet.

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění zákona č. 119/2007 Sb., definuje druhy[5] zajištění ochrany utajovaných informací (dále jen OUI), které řeší následující právní normy přičemž:

- **Personální bezpečnost** tvoří výběr fyzických osob, které mají mít přístup utajovaným informacím (dále jen UI). Legislativně je administrativní bezpečnost zakotvena v právní normě:

- *Vyhláška NBÚ č. 527/2005 SB., o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti).*

- **Průmyslovou bezpečnost** tvoří systém opatření k zajišťování a ověřování podmínek pro přístup podnikatele k UI. Legislativně je administrativní bezpečnost zakotvena v právní normě:

[5] **Druhy zajištění OUI**: personální, průmyslová, administrativní a technická bezpečnost, bezpečnost informačních nebo komunikačních systémů a kryptografická ochrana.

- *Vyhláška NBÚ č. 526/2005 Sb., o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti).*

- **Administrativní bezpečnost** tvoří systém opatření při tvorbě, příjmu, evidenci, zpracovávání, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s UI. Legislativně je administrativní bezpečnost zakotvena v právní normě:

- *Vyhláška NBÚ č. 529 Sb., o administrativní bezpečnosti a o registrech utajovaných informací.*

- **Fyzickou bezpečnost** tvoří systém opatření k zabránění přístupu neoprávněné osoby k UI. Legislativně je technická bezpečnost zakotvena v právní normě:

- *Vyhláška NBÚ č. 528 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.*

- **Bezpečnost informačních a komunikačních systémů** tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost UI, odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému (dále je IKS). Legislativně je administrativní bezpečnost zakotvena v právní normě:

- *Vyhláška NBÚ č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.*

- **Kryptografickou ochranu** tvoří systém opatření na ochranu UI použitím kryptografických metod a materiálů při zpracování, přenosu nebo ukládání UI. Legislativně je administrativní bezpečnost zakotvena v právních normách:

- *Vyhláška NBÚ č. 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací,*

- *Vyhláška NBÚ č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací.*

Mezi další související právní normy zabezpečující administrativní bezpečnost patří:

- zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti,
- zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů,
- zákon č. 227/2000 Sb., o elektronickém podpisu a změně některých dalších zákonů, ve znění pozdějších předpisů,
- zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů;
- zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů, stanoví skutkové podstaty trestných činů postihujících porušení pravidel pro nakládání s informacemi,
- zákon č. 500/2004 Sb.,správní řád, ve znění pozdějších předpisů,
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů,
- nařízení vlády č. 522/2005 Sb., kterým se stanoví seznamy utajovaných informací.

Problematika INA resortu MO je podrobně specifikována ve vojenském předpisu Vševojsk-15-1 „Vydávání interních normativních aktů v působnosti resortu MO.“ Mezi INA, které řadíme k sekundárním právním normám, patří např.:

- vojenské předpisy,
- RMO, nařízení náčelníka generálního štábu (dále jen NNGŠ), rozkazy příslušných velitelů (náčelníků),
- nařízení a směrnice velitelů jednotlivých velitelských stupňů.

V rámci začlenění ČR do Severoatlantické aliance resort obrany dodržuje normy NATO, mezi které patří:

- NATO: C-M(2002) 49 - Bezpečnost v rámci organizace Severoatlantické smlouvy,
- NATO: AD 70-1 „ACE SECURITY DIRECTIVE“ - Bezpečnostní směrnice velitelství spojeneckých sil v Evropě,
- NATO: AC/35-D/1015 (Revised) „Guidelines for the Development of Security Requirement Statements“ - Směrnice pro vypracování přehledu bezpečnostních požadavků,

- NATO: AC/35-D/1021 „Guidelines for the Accreditation of ADP Systems and Networks“ - Směrnice pro akreditaci systémů automatického zpracování dat a sítí,
- STANAG 4406 v. 3 - Systém pro zpracování vojenských zpráv (hlášení),
- AC/35-D2005 INFOSEC „Management Directive for Communication and Information Systems (CIS)“ – Směrnice pro řízení bezpečnosti KIS.

Z hlediska českého právního řádu bylo oficiálně přistoupeno k některým mezinárodním standardům, mezi které patří:

- ČSN ISO/IEC 15408 - Common Criteria (CC) Obecná kritéria hodnocení bezpečnosti IS,
- ČSN ISO/IEC TR 13335 - Směrnice pro řízení bezpečnosti IT,
- ČSN ISO/IEC 17799 - Řízení informační bezpečnosti,
- ISO/IEC 11801 - mezinárodní standard vhodný pro návrhy sítí s rozsahem 3.000 m, 1.000.000 m^2 prostoru a 50 ti až 50.000 osobami; zaměřeno na široký okruh aplikací (data, video, hlas),
- EN 50173 - evropská obdoba standardu ISO/IEC 11801,
- TIA/EIA-568-B – standardy telekomunikační kabeláže v komerčních budovách.

2.3 Význam informací a znalostí pro vojenskou oblast

Význam informací a znalostí pro oblast vojenství spočívá ve faktu, že dnešní moderní bojiště s jeho dynamickým charakterem a z toho vyplývajícího značného množství neurčitostí, zvyšuje nároky na potřebu informační převahy v celém prostoru boje. Cílem je získání informační nadvlády. Budování schopností v ozbrojených silách zabezpečí velitelům a individuálním bojovníkům informace, které potřebují, aby mohli činit klíčová, časově kritická rozhodnutí v celém rozsahu vojenských operací.

Schopnost získat kvalitní **informace** a využívat je, se stala kritickým faktorem úspěšnosti ve veškerém dění společnosti. Zejména ve vojenství musí být informace cílená, včasná, přesná, musí jí být přiměřené množství a musí být srozumitelná, tzn. prezentována vhodnou formou. V současnosti se informace staly výrobním zdrojem stejně jako pracovní síla, suroviny, výrobní zařízení či peníze. Je proto potřebné

informace efektivně získávat a využívat je. Informační procesy jako je získávání informací, jejich přenos, zpracování a využití je nutno řídit a to nejlépe procesně.

Kvalita informací závisí na faktu, zda jsou k dispozici na potřebném místě, v potřebný čas, v žádoucí struktuře, rozsahu, významu, se všemi podstatnými vazbami, se správnou úrovní agregace a možností zjistit detail. Samozřejmě nutnou podmínkou kvality je jejich pravdivost. Použitelnost je většinou závislá na formě (způsobu uložení/prezentace) a dostupnosti. Toto bývá složitý problém, z důvodu existence dvou přístupů získávání informací:

- sběr informací,
- příjem informací

Ve druhém případě je faktorem kvality také redundance přijímaných informací. Pokud nejsou jasné informační požadavky (které údaje jsou kdy potřebné), nemohou být v žádném případě informace kvalitní (je jich buď mnoho nebo málo). Žijeme v nové době, ve které se staly **znalosti**[6] klíčovým faktorem výkonnosti firem. Když si položíme a zodpovíme několik otázek např.:co jsou to znalosti, jaká je ekonomická efektivnost znalostí,nebo co je to management znalostí, obecně zjistíme, že:

- znalost je soubor zobecnělých informací obohacených o kontext (např. zkušenost), který lze v konkrétních podmínkách aplikovat,
- proti informaci je znalost schopná vytvářet v novém kontextu novou kvalitu (přidanou hodnotu), tedy i nová fakta či dosud nepoznané vazby,
- znalosti jsou tedy využité informace, které slouží ke zvýšení produktivity a efektivity jakékoliv činnosti a dávají schopnost najít řešení pro dosud neznámé.

Definice ve slovníku jazyka českého vymezuje znalosti jako souhrn vědomostí z určité oblasti. Širší informatické pojetí rozšiřuje tento pojem o kognitivní schopnosti, tedy informace včetně poznávacích funkcí. To je pravděpodobně velice výstižné, jelikož se jedná o získání vědomostí (*tento pojem bychom mohli chápat jako „zařazené“, resp. použitelné informace*) a současnou změnu kvalitativní úrovně (*pravděpodobně skok související s kvantitou informací*), která umožňuje tyto

[6] Drucker P. vnímá znalosti jako něco, co rozhoduje o produktivitě práce jednotlivce, firmy i hospodářského celku.

informace efektivně a účelně využívat k analýze a pochopení nových skutečností. Právě poznávací funkce zřejmě dělá z vědomostí „znalosti“. Nakonec co máme na mysli, když o někom říkáme, že „***to zná***“? Nejčastěji právě to, že se vyzná, že je v dané oblasti „doma“, že tomu rozumí a chápe problém hlouběji než většina ostatních. Navíc anglický originál „know” znamená daleko víc „znát“ či „umět“ než „být informován“. Proto je dobré rovněž odpovědět na otázky:

- Co je nejčastěji myšleno správou či managementem znalostí?
- Kdo a proč dané téma otevírá?

Nejlépe srozumitelná je definice T. H. Davenporta, který definuje ***management znalostí*** jako systematický proces hledání, vybírání, organizování, destilování a prezentování informací způsobem, který zlepšuje porozumění pracovníka specifické oblasti zájmu. ***Správu znalostí*** vnímá v jistém smyslu jako mechanický systém, který má zajistit získání informací „z hlav lidí“. Dokonce mechanismy pro sběr znalostí uvádí do spojitosti s propouštěním zaměstnanců, kteří žádoucí znalosti vlastní. ***Audit znalostí*** chápe nikoli jako mapování míst, kde mají být zlepšeny informační a kognitivní schopnosti systému, ale jako průzkum ochoty pracovníků sdílet informace. Zde je možné vidět zásadní rozdíl mezi škatulkovým a účelovým přístupem.

- Účelový přístup se snaží především najít a využít skryté rezervy ke zvýšení podnikového potenciálu. Je mu jedno, jestli se navrhovaným opatřením bude říkat strategický marketing, správa příležitostí nebo management znalostí. Jednoznačně definujeme to, co vnímáme jako nedostatek či slabou stránku. Snažíme se navrhnout, jakým opatřením by se tato možnost zvýšení podnikového výkonu dala využít. Většinou to bude vyšší kvalita informací a změna organizace práce, která k této vyšší kvalitě povede a která ji umožní využít. Velmi důležité je to, že neshromažďujme informace pro ně samotné, ale definujeme informační strukturu s konkrétním záměrem, jako pracovní nástroj a způsob zdokonalení rozhodování.
- Škatulkový či přesněji školometský přístup vidí hlavní smysl shromažďování informací v tom, aby jich bylo „co nejvíc“. Jistě, toto je hrubé zkreslení – je také myšleno zcela obrazně. Ale v jistém smyslu se tak výše uvedená definice dá chápat. Navíc u tohoto přístupu je typickým znakem, že si autoři nedělají

příliš velké starosti s rozlišováním toho, co jsou znalosti, co vědomosti a co informace či dokonce data uložená v souborech. Jediné starosti jsou s tím, jak co nejlépe vymyslet mechanismus, který zajistí, že všechny údaje, se kterými se pracuje, budou nějakým způsobem uloženy v podnikové databázi.

Pokud se chceme zabývat znalostmi, je bezpochyby nutné zajistit odpovídající systém pro získávání, zpracování a zpřístupnění informací. Nutno se ztotožnit s názory, že o problematice ***řízení znalostí*** panuje řada zmatených představ, velmi často podporovaných subjekty, které mají zájem na zisku plynoucím z implementace nástrojů pro podporu správy explicitních formálních znalostí a souvisejících procesů. Proto se může v úvahách o tom, jak řízení znalostí funguje, objevit internet, elektronický podpis či e-learning.

Pokud má být jakákoli nová myšlenka prospěšná, musí být použitelná a to snadno. Proto je důvod zamyslet se nad tím, jestli je potřeba rozlišovat mezi informacemi a znalostmi. Jaký je tedy ten rozdíl mezi znalostmi a informacemi? Má to nějaký vliv na konkurenceschopnost? Co se tím, že máme správu znalostí, změnilo? Stačí skutečně pro využití znalostí ke zvýšení výkonnosti organizace odstranit ty staré známé zjevné chyby ve zpracování informací? Je nutno počítat s tím, že k tomu, aby se z informací staly znalosti, jsou potřeba *manažerské schopnosti*, značné *metodické know-how*, *uplatnění zásadních metod* jako je systém řízení pomocí cílů, fungující strategické řízení atd. To jsou náležitosti, které se jen málokdy vyskytují všechny pohromadě. Znalosti by totiž měly umožnit nejvyšší dosažitelnou kvalitativní úroveň rozhodnutí. Musí organizaci umožnit správně chápat, co se děje kolem a uvnitř ní, pomoci včas nalézt postupy a zdroje, se kterými na tento vývoj může účinně reagovat.

Znalosti, které obsahují zobecněné, rozpracované zkušenosti a zohledňování komplexních souvislostí, pomohou modelovat dopad navrhovaných opatření a korigovat vypočítané výsledky. A to všechno komplexně, tedy tak, že rozhodnutí přijaté u jednoho problému neohrozí fungování jiné části podniku, resp. spíše dokážeme najít takové řešení, které ostatní aktivity pokud možno podpoří. Znalosti tomu budeme říkat proto, že to nejsou jenom informace. Je to uspořádání informačních zdrojů, přístup a motivace lidí tyto zdroje tvůrčím způsobem využívat. Když to budeme brát takto, tak se možná rýsuje nejdůležitější funkce správy znalostí.

Správa znalostí (knowledge management) se občas prezentuje jako počítačová disciplína, ale fakticky se jedná o jistou stránku procesního přístupu, kde jsou postupy striktně stanoveny. Dodatečné (*většinou nejdůležitější*) informace (*typicky zdůrazňováno v CRM*[7]) nesmí být „vlastnictvím" konkrétních osob (*jednotlivců*), ale je nutno pro ně najít odpovídající techniky formalizace (*převedení do strukturované/strojově zpracovatelné podoby*) a řídící pracovníky (*vlastníky procesů*) pověřit tím, aby zajišťovali maximální mírů zachycení/transformace (*uložení*) těchto informací (*v kterémžto procesu mají velmi aktivní roli*).

Pokud se podíváme na roli IT v libovolné organizaci, dojdeme k jednoznačnému závěru, že *hlavním úkolem je automatizovat efektivně hlavní, vedlejší a podpůrné podnikové procesy, vytvořit informační základnu, která slouží pro realizaci těchto procesů, pro podporu rozhodování a poskytnout služby pro interní a externí komunikaci* (elektronickou, hlasovou či obrazovou). Pod pojmem IT rozumíme veškeré přístroje a projekty, které mají souvislost s informacemi, jejich tvorbou, analýzou, zpracováním nebo přenosem. Mezi IT patří telekomunikace, internet, počítače, přístroje na analýzu dat ve vědě, v lékařství, satelity, televize a mnoho dalšího. Tyto přístroje nám ulehčují manuální i duševní práci a díky nim máme všeobecný přehled. Komplexnost IT v dnešních organizacích vyplývá z rozsáhlosti nasazení a vzájemné provázanosti jednotlivých systémů. Základem budování IS by v každé organizaci měla být informační strategie, která definuje, jak za pomoci odpovídajících prostředků informačních a komunikačních technologií podporovat dosahování cílů a realizovat strategii organizace. Páteří IT každé firmy je hlavní provozní systém, který slouží k automatizaci hlavních procesů. Z pohledu IT a organizace jde o systémy např.:

- **Back-office systémy -** serverové systémy pro podporu a automatizaci podnikových procesů.

[7] **CRM** … řízení vztahů se zákazníky (Customer Relationship Management). Sice stále přežívá představa, že se jedná především o počítačovou aplikaci, ale ve skutečnosti je to spíše podnikatelská filozofie. Informační systémy pro CRM podporují prodejní činnosti včetně organizace práce prodejců, marketing, někdy elektronické obchodování, servis a zákaznickou podporu. Včetně analytických funkcí nad získanými daty. CRM je ve své podstatě silně procesní záležitost ("... konkrétní vztah se zákazníkem je instance procesu ..."), proto by mělo být pravidlem, že CRM systémy obsahují vlastní nebo alespoň podporují připojení externího workflow.

- **Business Automation systémy (BA) -** obecné označení aplikací pro automatizaci firemních procesů. Většinou se jedná o zakázkově vytvářené aplikace pro podporu specifických firemních procesů.
- **Distribuovaný systém -** IT systém, jehož jednotlivé části (aplikace nebo jejich moduly) jsou provozovány na různých systémech nebo v různých lokalitách, ale pro uživatele se tváří jako integrovaná aplikace. Jsou tvořeny pro maximálně efektivní využití infrastruktury.
- **Portál** - označení, se kterým se můžeme v IT setkat téměř na každém kroku. Pod pojmem se skrývá celá řada méně či více odlišných významů (enterprise portal, employee portal, business portal atd.). Ve všech případech je základní premisa stejná – *portál je systém či produkt sloužící jako prostředek pro vizuální či nevizuální integraci širšího spektra aplikací, informací (metadata) nebo procesů, které umožňují snadnou správu, zajištění bezpečnosti a flexibilitu*. Hlavním smyslem využití portálu je zjednodušení administrace portfolia aplikací a informací a zvýšení komfortu pro uživatele, kteří mohou přes jednotný konfigurovatelný interface přistupovat ke všem relevantním částem podnikových IS nebo dokonce k externím aplikacím a informacím.

Podoba jednotlivých částí IT systémů může být odlišná (samostatný systém, komponenta, balíková aplikace, modul integrovaného systému) v závislosti na zvoleném přístupu té či oné organizace. Také názvy těchto aplikací a jejich funkcionalita se mohou mírně odlišovat podle pojetí konkrétního dodavatele.

V oblasti administrativy a podpůrných procesů existuje velká rozmanitost používaných aplikací. Přínosy nasazení v této oblasti jsou obtížněji definovatelné, a proto také patří nasazování IT mezi nižší priority. Hlavní cílovou oblastí je digitalizace, archivace a správa fyzických (papírových) dokumentů, automatizace některých schvalovacích procesů a front-office systémy, které zná každý uživatel PC, neboť mezi ně patří textové editory, e-mailové programy atd. Pro základní orientaci uvedu některé administrativní systémy v návaznosti na uživatelské požadavky:

1) **Poskytování služeb** (procesů) si dnes bez silné IT podpory nelze vůbec představit. Je často formována právě hlavním IT systémem (*provozní systém, transakční systém, systém pro automatizaci poskytování služeb*), který definuje podobu a kvalitu těchto procesů. Klíčovou součástí systémů je správa

uživatelů služby společně s měřením užívání služeb a s následným zpoplatněním (billing systémy). V případě, že podkladem pro poskytování služeb je určitá infrastruktura, je pak jeho součástí také plánování, řízení, údržba a případně i budování této infrastruktury. Patří sem např.:

- **Expertní systémy (ES) -** znalostní automatizované systémy, které na základě specifikace problému ve své bázi známých problémů a jejich řešení hledají adekvátní postupy.
- **Grafický informační systém (GIS)** - pracuje nad grafickými daty popisujícími geografický kontext. Jsou součástí IT podpory pro plánování, údržbu a správu infrastruktury pro poskytování těchto služeb.
- **Knowledge management (KM) -** velmi široká definice, která vymezuje nejen IT systémy. V podstatě se jedná o vědní obor, tzn. KM je většinou chápán jako systém pro správu expertních znalostí, případně se může jednat o systémy uchovávající organizační znalosti (směrnice, postupy, integrované workflow atd.).

2) **Administrativa, podpora hlavních procesů** - způsob pokrytí administrativních a podpůrných procesů IT se u jednotlivých firem liší a právě v této oblasti narazíme na největší rozmanitost používaných aplikací. Jedná se o systémy:

- **Document Managment systémy (DMS)** - systém pro digitalizaci, archivaci, správu a práci s elektronickou formou dokumentů, které buď vnikly již v elektronické podobě, nebo měly původně papírovou podobu. V současné době se prosazuje širší pojetí DMS, které je nazýváno ECM.
- **Enterprise Content Management (ECM) -** systém pro správu podnikových dokumentů a toku informací (zahrnuje práci s dalšími typy informací, jako jsou e-mail, obrazová data apod.). ECM systémy jsou integrovány s dalšími aplikacemi, které využívají v nich uložené dokumenty a naopak ECM systémy je využíván obsah uložený v jiných systémech.
- **Document Imaging System (DIM)** - slouží pro digitalizaci, archivaci a správu dokumentů, které obsahují jak hardwarové, tak softwarové prvky, jsou součástí DMS nebo jsou na ně napojeny.
- **Elektronické kolaborační systémy -** aplikace určené pro týmovou spolupráci.

- **Elektronické komunikační systémy -** aplikace pro elektronickou komunikaci (e-mailové servery, faxové servery, voice mail systémy).
- **Elektronické publikační systémy -** skupina aplikací pro elektronické publikování a práci s dokumenty (textové editory, DTP aplikace, kopírovací systémy).
- **Image Processing System (IPS) -** aplikace pro zpracování obrázků, do které kromě grafických editorů patří také multimediální systémy či systémy pro vytváření prezentací.
- **Office Management Systems (OMS) -** systémy pro podporu plánování času, správu a distribuci úloh.
- **Workflow systémy -** systémy pro řízení a správu toku dokumentů spojených s podnikovými procesy.

3) **Řízení organizace** - klíčovým IT nástrojem jsou systémy poskytující agregované údaje (analytického charakteru) z jednotlivých provozních systémů, které umožňují ideálně v reálném čase sledovat výkonnost, chování a stav společnosti a adekvátně reagovat. Tyto nástroje se souhrnně označují jako **systémy pro podporu rozhodování** nebo *business intelligence systémy*. Další skupinou jsou specializované aplikace nebo taková součást interních systémů, jež *umožňují řídit a spravovat proces přípravy strategie společnosti, systémy pro strategické plánování společnosti a také např. rozpočtové systémy v neziskových organizacích*. Patří sem např.:

- **Decision Support System (DSS) -** označení pro software pro podporu rozhodování poskytující souhrnné informace z provozních systémů umožňující kvalifikovanější rozhodnutí řídících nebo odborných složek organizace.
- **Business intelligence (BI) -** zpracovává informace z interních provozních systémů, případně externích informací a poskytuje výstupní informace pro řízení společnosti na různých úrovních. Částečně shodné s DSS, BI systémy jsou však širším pojetím a nemusí nutně sloužit jako podpůrný nástroj, ale přímo jako součást procesů.

- **Data mining (DM) -** většinou interaktivní práce nad agregovanými daty (analyzovanými), které pochází z jednoho nebo více podnikových systémů umožňující odhalit nestandardní souvislosti.
- **Data warehouse (DW) -** systém pro analytické zpracování a uložení dat z jednoho nebo více provozních systémů, případně i nástroje pro zobrazení výstupů z takového zpracování.
- **Enterprise Information System (EIS) -** označení pro vrcholové IS sloužící pro strategické rozhodování managementu.

Ze zkušenosti se potvrzuje, že při aplikaci bude vždy nutné firemní produkt přizpůsobit potřebám armády. Problematika armádního řešení SW produktu je natolik složitá, že ji nelze řešit nákupem jakéhokoliv komerčního SW produktu a jeho případnou drobnou úpravou speciálních funkcí. Vyřešení problému sběru informací na teritoriu ČR (natož pak i pro zahraniční mise) vyžaduje samostatný systémový pohled, důkladnou analýzu toku dokumentů, analýzu uživatelských a bezpečnostních požadavků, atd. Technické řešení je velice finančně náročné a lze je realizovat pouze ve spojení s kapitálově a technologicky silnou firmou zakázkovým způsobem.

V oblasti vojenství pražský summit NATO ukázal, že Network Centric Warfare (NCW) bude klíčovou strategií pro 21. století. Někteří evropští spojenci v NATO začínají budovat schopnosti síťového vedení operací. NATO Network Enabled Capability (NNEC) je dalším krokem podporujícím „síťový“ přístup. Používání jiného názvu (NNEC místo NCW) nemá pouze symbolický charakter. Evropské země nemají stejné ambice jako USA a nejsou ochotny věnovat finanční zdroje v takovém rozsahu, aby vyvinuly a vybudovaly obdobně širokou síťovou architekturu. Hledají spíše levnější řešení využitím těch stávajících kapacit, které mají, nebo budují, případně jejich přizpůsobením potřebám síťového vedení války.

Idea NCW je sbírat informace pro rychlé zpracování, analýzy a interpretace a sdílet v čase informace o bojišti mezi těmi co rozhodují na všech úrovních velení a individuálními bojovníky. NCW slibuje nadvládu v efektivnosti zbraňových systémů pomocí rychlé distribuce informací na každé místo na válčišti. Distribuované informace jsou získávány pomocí různorodých, vysoce kvalitních senzorů, umístěných na různých platformách.

Jednotlivé země mají rozdílný přístup k budování schopností NCW, který vyplývá z rozdílného rozsahu a úrovně prvků jejich současných systémů, stupně digitalizace a finančních prostředků vyčleněných na modernizaci ozbrojených sil. Základním požadavkem však je, aby budované kapacity byly interoperabilní a použitelné ve společných koaličních operacích.

Aplikovat NNEC v podmínkách ČR a AČR předpokládá:

- zpracovat koncepci v podmínkách OS ČR a zabudovat ji do všech určujících bezpečnostních a obranných dokumentů a zejména plánů resortu,
- zapojit se úměrně do prací na koncepci a studii proveditelnosti NNEC (PSS-významný prvek sítě senzorů),
- zvýšit informovanost a dosáhnout pochopení problematiky NNEC na všech stupních velení a řízení,
- analyzovat dopady změn operačních a organizačních aspektů NNEC,
- analyzovat potřebné změny lidských aspektů NNEC, změny ve vzdělávání a výcviku,
- posoudit technologické aspekty NNEC, ověřit interoperabilitu budovaných OTSVŘ,
- zaměřit obranný výzkum ke všem uvedeným aspektům (nejen k aspektům technologickým),
- zhodnotit stávající kapacity v oblasti C4I a jejich využitelnost, případně přizpůsobitelnost pro koncepci NNEC,
- usměrnit již započatý vývoj relevantních technologií a systémů tak, aby byly využitelné pro NNEC,
- vyhodnotit případnou potřebnost budování zcela nových zatím chybějících schopností, nezbytných pro tuto koncepci.

Dále jsou uvedeny příklady významnějších aktivit, které v současnosti probíhají v některých evropských zemích a jsou příspěvkem k budování schopností NCW.

a) **Švédské ozbrojené síly** - Švédové rozpoznali potenciál NCW velice brzy a budují tyto schopnosti, aby napomohli změně od stávající obranné koncepce k pružnějším a rozmístitelným silám s vysokou pohotovostí. Vzhledem k rozpočtu, spoléhají více na vlastní technologie, což by mohlo způsobit

problémy při propojování se spojenci.

b) **Francouzská Network-Centric vize** - Francouzi jsou pravděpodobně jedinou evropskou zemí, která investuje do celého rozsahu net-centric technologií včetně vesmírných, bezpilotních prostředků, velení a řízení a komunikačních systémů. Výrobci vedeni firmami EADS, Thales, MBDA a Sagem přecházejí od prodeje jednotlivých zařízení k nabídce integrovaných systémů a řešení.
c) **Nizozemský přístup** - kromě kooperace s Francií investuje Holandsko do systému ISIS – Integrated Staff Information Systém.
d) **Německý přístup** - Německé ozbrojené síly zkoumají různé přístupy a systémům řízení boje (Battle Management Systems - BMT) z hlediska zavedení struktury net-centric sil použitím různých platforem, senzorů a zařízení. To povede ke zlepšení řízení boje v čase blízkém reálnému a zabezpečí přenos údajů o cílech a video výstupů, prostřednictvím spojů systému C3I k podpoře všech úrovní velení, v rozsahu vojenské operace.
e) **Britský přístup** - Britové v oblasti NCW usilují zejména o zachování interoperability s USA. Proto značnou část technologií pro NEC buď přímo kupují (BOWMAN, ASTOR), nebo kooperují s americkými výrobci (UAV WATCHKEEPER).

Z výše uvedeného vyplývá, že ozbrojené síly evropských zemí si začínají uvědomovat důležitost sil, které jsou založeny na znalostech a jsou schopné pracovat v soustředěných sítích. NCW umožní budoucím bojovníkům zjistit cíl a přenést informace o něm na odpovídající místo velení, což umožní rychlejší sdílení informací a reagování na ohrožení.

2.3.1 Organizace informačních systémů MO ČR

Resort obrany ČR disponuje značným počtem relativně nezávislých informačních systémů dle odborností, které jsou v různém stadiu výstavby a jsou určeny pro stanovený okruh uživatelů. Jejich vzájemné nepropojení způsobuje, že nejsou uspokojeny operační požadavky a potřeby uživatelů. Zásadním nedostatkem budování těchto systémů byla nedostatečná koordinace řízení jejich výstavby. Proto byl koordinací, dalším rozvojem a prosazováním jednotné strategie informatizace pověřen jediný orgán. Pro potřeby velení vojskům v operaci byla zahájena výstavba

mobilních komunikačních a informačních systémů (dále jen KIS). Stacionární KIS jsou prvkem k zabezpečení spojení na teritoriu.

Po vstupu naší země do NATO a zahraničními misemi AČR vyvstal problém elektronizace spisové služby. Jako reakce na tento stav byly sice zavedeny v různých klíčových lokalitách SW produkty pro ulehčení a nastartování spisové služby, ale jejich rozšíření do celého resortu bránila poměrně vysoká pořizovací cena. I zde se nakonec narazilo na problematiku komunikační infrastruktury.

V současné době resort obrany v rámci automatizace spisové a archivní služby (dále jen ASAS), nebo-li knihovnictví využívá systém InfoLive, Archid a ESAS. Systémy jsou opět určeny pro úzký okruh uživatelů, nepatří mezi veřejně přístupné informační zdroje.

Systém InfoLive poskytuje informační podporu evidenci dokumentů NATO, EU a ostatních smluvních stran. Zabezpečuje informační podporu pro procesy manipulace, správy, řízení a kontroly a současně poskytuje informační služby uživatelům v resortu MO. Vytvořený systém je nasazen na zahraničních pracovištích, na vybraných pracovištích MO ČR, MZV ČR na základě meziresortní dohody v rámci vyčleněného informačního systému. Architekturu tvoří čtyři registrační místa - *Registr MO, Registr SD ČR v Bruselu, Registr Mons a Registr MZV ČR*. Propojení NBÚ je řešeno přístupem k databázi Registr MO pro jednoho uživatele v rámci celoarmádní datové sítě.

Systém ESAS – elektronická spisová a archivní služba zabezpečuje jednotné prostředí pro evidenci, manipulaci, zpracování, bezpečné ukládání a vyhledávání informací, předávání a přijímání úkolů a s tím související kontrolovaný pohyb dokumentů jak v elektronické i listinné podobě.

Systém Archid je využíván pro procesy související s archivní péčí ve Vojenském ústředním archivu. Zajišťuje informační podporu při přebírání dokumentů do archivu a podporu pro komplexní archivní péči.

2.3.2 Veřejně přístupné informační zdroje MO ČR

Základ veřejně přístupných zdrojů MO ČR tvoří **Webová aplikace**, tzn. technologie, která zpřístupňuje dílčí funkčnost podnikového IS. Jde o prostředek, který zajišťuje přístup do IS prostřednictvím standardní - zcela obecné, primitivní funkčnosti klienta, typicky webového prohlížeče, pro poskytování přístupu k datům a funkcím rozsáhlých IS vzdáleně. Jedná se o IT technologii typickou pro poskytování IS jako služby.

Veřejným informačním zdrojem v rámci resortu obrany je **Vojenský historický archiv** (dále jen VHA) Praha, který využívá k zpřístupňování informací program pro Počítačovou evidenci Archivu – PEvA vytvořen archivní správou MV pro vedení základních evidencí v síti archivů ČR. Hlavním úkolem VHA Praha je péče o muzejní sbírky podle zákona č. 122/2000 Sb. O ochraně sbírek muzejní povahy, odborně zpracovává sbírky a zpřístupňuje je veřejnosti ve stálých expozicích a příležitostných výstavách. Ze zákona je garantem udílení povolení k vývozu militárií. Je zároveň garantem ochrany v oblasti vojenské historie v rámci AČR i mimo ní, poskytuje odborné služby státním orgánům a právnickým a fyzickým osobám, zpracovává vědecké studie a expertízy. Vědecko výzkumná činnost je zaměřena především na problematiku I. II. a III. odboje a zpracování personálií předních vojenských osobností. Dlouhodobě je zkoumáno české a československé vojenství zejména ve 20. století. Další zdroje vojenských informací lze vyhledat na www stránkách internetu jednotlivých útvarů a zařízení AČR a muzeí, jako je např.: [61]

Letecké muzeum - založeno v roce 1968 v areálu historického vojenského letiště Praha - Kbely, které bylo první leteckou základnou vybudovanou po vzniku Československa v roce 1918. Prezentuje vojenské, výrobní, dopravní a sportovní tradice českého a československého letectví. V současné době je vystaveno více než 100 letounů, z nichž některé patří k světovým unikátům. Expozici dále tvoří letecké motory, výzbroj, výstroj, řády, vyznamenání a řada dalších památek. Část expozice je věnována čs. účasti na kosmickém výzkumu. [36]

Armádní muzeum - je umístěno v Praze na Žižkově v historických budovách Památníku národního osvobození. Muzeum je věnováno historii prvního a druhého odboje v letech 1914 - 1918 a 1939 - 1945 a historii československé armády 1918 - 1939. Vedle zbraní je vystavena řada unikátních dobových stejnokrojů, praporů, řádů, vyznamenání a rovněž osobních památek na čs. presidenty a přední představitele čs. armády. [37]

Vojenská historická knihovna - je rozsáhlá odborná knihovna, která soustřeďuje více než 250 000 svazků knih a časopisů, věnovaných především vývoji vojenství. Ojedinělý fond vojensko-historické literatury z 19. a 20. století zpřístupňuje četné monografie a periodika k vývoji vojenského umění, průběhu válečných konfliktů, k vývoji výstroje, výzbroje a vojenskému stavitelství. Zvláště cenné jsou fondy starých tisků a map odborně vojenského charakteru a velká mapová díla 19. století. [38]

Vojenský historický ústav Praha - vydává **odborný** časopis Historie a vojenství. Další nalezené stránky na http://www.militarymuseum.cz. Časopis je jediným specializovaným vědeckým a odborným časopisem v oblasti vojenské historie s celostátní působností. Publikovány jsou studie a materiály především k dějinám českého a československého vojenství s důrazem na 19. a 20. století, dále archivní dokumenty, informace o nových knihách, výstavách, konferencích apod. Do roku 1998 včetně vycházel časopis 6 x ročně, každý sešit byl číslován samostatně, od roku 1999 vychází 4x ročně, číslování je průběžné. [39]

V rámci mezinárodních vztahů vojenskou historii reprezentuje v zahraničí Česká komise pro vojenské dějiny, která je členem Mezinárodního komitétu pro vojenské dějiny (CIHM). Vojenský historický ústav Praha je současně členem komisí Mezinárodního výboru muzeí (ICOM) a Mezinárodní asociace muzeí zbraní a vojenské historie (IAMAM) při UNESCO. [39]

2.4 Systém integrované společnosti

S využíváním IKS nabývá na významu budování informační společnosti. Za informační společnost je považována společnost, ve které hlavní roli hrají informace

společně s informačními a komunikačními technologiemi, jež přispívají lidem k zlepšení kvality jejich života. Určujícími faktory informační společnosti jsou:

- informace,
- vědomosti,
- znalosti.

Informace ovšem musíme chránit před vnějšími i vnitřními hrozbami. Současná doba je ale čím dál více prezentována vnitřními i vnějšími útoky na počítače (dále jen PC) a počítačové sítě. Jde o výrazný nárůst útoků zaměřených na krádež důležitých dat či identit, s cílem vymáhat peníze nebo zcizené informace prodat. Proto je nezbytně nutné urychleně ochránit jak PC tak sítě a především data v nich uložená proti neoprávněnému přístupu. Existuje mnoho různých technologií a produktů, jak tento požadavek splnit. Řešením je spojení bezpečnostních systémů v jeden celek – integrace IT bezpečnosti s objektovou bezpečností s návazností na další systémy. Cílem není jen zvýšení bezpečnosti, ale i zjednodušení práce administrátorů, správců, uživatelů a snížení role lidského faktoru (zapomnětlivost, nedůslednost, špatný úmysl apod.). K tomu je nutné kombinovat různé technologie a prostředky, které jsou k dispozici:

- proti fyzické krádeži PC nebo disku - důsledným zálohováním dat a šifrováním,
- proti virovým útokům - nasazením antivirového programu,
- proti spamu - nasazením antispamového programu používající kombinovanou technologii ochrany,
- proti spywaru - nasazením antispywarového programu,
- proti průniku do systému - nasazením firewallu, PKI a automatickým updatem systému,
- proti průniku do aplikací - nasazením technologií PKI a Single Sing-On,
- proti neoprávněnému přístupu k našim datům a komunikaci - šifrováním,
- proti odposlouchávání komunikace - šifrováním komunikace.

Vlastní ochranu dat nutno řešit kombinací hardwarových, softwarových produktů a technologií k bezpečnému uložení autentizačních dat a ochraně citlivých informací v PC a počítačových sítích včetně komunikace.

Mezi nejdůležitější projekty podporující rozvoj informační společnosti patří:

- bezpečná města,
- metropolitní sítě měst a obcí,
- znalostmi řízený přístup ke službám občanů,
- softwarová architektura IS hmotné nouze a sociálních služeb – IS vznikl v roce 2006 v souladu se zákony č. 111/2006 Sb., o pomoci v hmotné nouzi a zákonem č. 108/2006 Sb., o sociálních službách. IS je určen pro pověřené obecní úřady, obce s rozšířenou působností, krajské úřady a Ministerstvo práce a sociálních věcí,
- jednací místnosti pro státní správu a jejich vybavení audiovizuální technikou pro efektivní sdílení informací,
- a další.

Ministerstvo informatiky ČR dále zpřístupnilo na portálu veřejné správy (dále jen PVS) bezplatné samostudijní e-learningové kurzy pro širokou veřejnost. Nyní je nabízeno několik (cca 9) kurzů, které jsou zaměřené na počítačovou gramotnost. Kurzy mohou využít ti, kteří:

- se chtějí s počítačem něco nového naučit,
- kteří si chtějí procvičit, co se naučili během kurzů Národní počítačové gramotnosti nebo
- kteří si chtějí otestovat své znalosti nutné pro získání tzv. evropského řidičáku na počítač.

Počet registrovaných aktivních uživatelů v září 2006 přesáhl 10 000 a počet prostudovaných kurzů přesáhl 9 800. Z výše uvedeného je zřejmé, že nové technologie umožňují překonat časová a prostorová omezení v šíření informací a umožňují rychlý přenos a zpracování informací v datové, zvukové či audiovizuální podobě do nejrůznějších oblastí každodenního života, čímž se stávají neodmyslitelnou součástí dnešní společnosti. Míra rozšíření a především pak způsob využití moderních informačních a komunikačních technologií (dále jen ICT) a na ně navazujících procesů, stejně jako znalosti a dovednosti s nimi související, ve stále větší míře ovlivňuje způsob práce, komunikace, ale i trávení volného času čím dál většího počtu jednotlivců společnosti. Přístup k informačním a komunikačním zdrojům (dále jen IKZ), který tyto moderní technologie umožňují a jejich efektivní

využívání jsou považovány za klíčový faktor ekonomického a sociálního rozvoje společnosti. Rozdíly v možnosti k přístupu a využívání nových IT mohou způsobit nový druh sociálních rozdílů a prohloubit dosavadní, založené na přístupu ke vzdělání, pohlaví, věku, rodinného zázemí, finanční situaci apod. Při identifikaci těchto rozdílů má nezastupitelné místo statistika. Od roku 2003 Český statistický úřad (dále jen ČSÚ) zavádí do svého programu šetření o využívání ICT v podnikatelském sektoru, v domácnostech/mezi jednotlivci a ve veřejné správě, která přinášejí srovnatelné údaje se zeměmi EU. Dostupné statistické informace, dokumenty a materiály, a to včetně mezinárodních o informační společnosti, nalezneme pod odkazy např.:

- Domácnosti a jednotlivci: [51]
  http://www.czso.cz/csu/redakce.nsf/i/domacnosti_a_jednotlivci
- Veřejná správa: [52]
  http://www.czso.cz/csu/redakce.nsf/i/verejna_sprava
- ICT ve školství: [53]
  http://www.czso.cz/csu/redakce.nsf/i/ict_ve_skolstvi_e_education.

Kromě výše uvedených webových stránek je nutné vzpomenout i brožuru „Informační společnost v číslech 2007“, která obsahuje nejen nejaktuálnější informace o stavu informační společnosti ČR, ale i o jeho vývoji v posledních 3 letech.

2.4.1 Informační společnost a e-Government

Teorie říká – „změny obecně označované jako e-Government předsazují přeměnu a inovaci veřejné správy za využití IT a znamenají:

- inovaci organizačního modelu a kontrolních instrumentů,
- re-design administrativních procesů ve světle efektivnosti a hospodárnosti,
- re-design rozhodovacích procesů a zlepšení jejich transparentnosti pro veřejnost,
- podporu většího zapojení veřejnosti na správě „věcí veřejných“.

Porovnáme-li tuto definici se skutečností, pak musíme říci, že e-Government u nás ještě nezačal v plném rozsahu. Bohužel stále převládá přístup „legislativa nám to neumožňuje“ namísto „je nutné změnit legislativu. Co tedy dnes máme u nás?

- Elektronizace úřadu - je v současné době na dobré úrovni. Zaostává však úroveň v menších obcích. Problém je komunikace např. mezi městskými částmi a detašovanými pracovišti v rámci měst.
- Elektronizace komunikace mezi úřady – jedná se o zcela zásadní předpoklad pro širší zavedení e-Governmentu. Chybí mnohde infrastruktura, nejsou implementovány vhodné aplikace, není dopracovaná legislativa.
- Komunikace občana a veřejné správy (dále jen VS) – řeší se (např. PVS). Snaha o centralizaci a zjednodušení především pro malé obce, které na to nemají vybavení, kapacitu a technickou způsobilost. Otázka je, zda se tento bod nepřeceňuje a první dva nepodceňují. Proč? Protože je to prosté líbivé, zdánlivě jednoduché a proto zdánlivě efektivní. A zcela upřímně – občan chce komunikovat s VS co nejméně.

Vhodné IT jsou bezesporu k dispozici, ale využívání nových IT ve VS i veřejností však zdaleka zatím nedosahuje očekávání, která se do informačních a komunikačních technologií vkládá, zejména pokud jde o její aktivní využívání. Příčina ovšem není v samotných IT, které se osvědčili v komerční sféře, ale je nutné ji hledat v úrovni ICT vzdělávání a úrovni investic do IT.

2.4.2 Využívání služeb e-Governmentu jednotlivci

Jak je výše uvedeno, e-Government můžeme charakterizovat jako využívání informačních a komunikačních technologií a různých IS ve VS, s cílem optimalizovat činnost VS a nabídnout občanům a firmám profesionálnější, rychlejší a méně komplikované služby. Rozvoj e-Governmentu je dlouhodobý a náročný proces, jehož klíčovým prvkem je elektronizace vnitřních agend ve VS. Elektronizace agend však není jediným předpokladem efektivního fungování e-Governmentu. Dalšími jsou:

- dostatečná vybavenost orgánů VS IT,
- zpřístupnění on-line služeb klientům,
- dostatek úředníků schopných pracovat s náročnými IS,

- rozvinutá informační společnost, kde jednotlivci mají přístup k internetu a zcela běžně internet využívají.

Již jsme hovořili o skutečnosti, že ČSÚ realizuje od roku 2003 pravidelné šetření o využívání IKT v domácnostech a mezi jednotlivci. Šetření probíhá jednou ročně na vzorku cca 10 000 jednotlivců a je reprezentativní pro dospělou populaci (16 a více let) ČR. Jako metoda sběru dat se používá osobní interview. Dotazník je rozdělen do 4 základních modulů:

- přístup k vybraným IT,
- použití osobního počítače,
- použití internetu,
- nákup přes internet.

K nejpopulárnějším činnostem na internetu patří vyhledávání informací a komunikace. Podrobnější informace o využívání služeb e-Governmentu jednotlivci najdeme na webových stránkách ČSÚ : http://www.czso.cz v sekci „Informační technologie“. [59]

Při plnění bezpečnostních úkolů státu je výzkum a vývoj v působnosti Národního bezpečnostního úřadu. Je prováděn a zabezpečován v souladu s požadavky a potřebami státu při naplňování úkolů obsažených v zákoně č. 412/2005 Sb. Při plnění úkolů výzkumu a vývoje dalších oblastí je v kompetenci ministerstev dle daného oboru.

V oblasti vojenství ČR provádí výzkum a vývoj **Ústav strategických studií** (dále jen Ústav), který je vysokoškolským ústavem Univerzity obrany (dále jen UO). Posláním ústavu je provádět vědecko - výzkumnou a vzdělávací činnost ***v oblasti obrany a bezpečnosti***, která přispěje k lepšímu pochopení komplexního a nejistého vývoje bezpečnostního prostředí a jeho důsledků pro formulování efektivní obranné politiky a vojenské strategie státu. Svým posláním reaguje na trend zvyšujícího se zájmu rezortu obrany o vědecko-výzkumnou podporu strategické úrovně řízení a na prohlubující se internacionalizaci vzdělávání v globální postindustriální společnosti založené na znalostech a informacích. Za tímto účelem jsou rozvíjeny tři základní pilíře okruhů strategických studií:

- strategické studie vývoje bezpečnostního prostředí, které zahrnují regionální a globální bezpečnostní vztahy, hrozby a rizika, ohniska napětí,
- strategické studie vývoje ve vojenství se zaměřením na trendy vývoje vojenské strategie a operačního umění, soudobé ozbrojené konflikty, armáda v různých typech bojových a nebojových operací, operační požadavky na budoucí ozbrojené síly v pravděpodobném operačním prostředí,
- strategické studie vývoje zdrojů a technologií s důrazem na vývoj obranných zdrojů, schopnosti ozbrojených sil a jejich budování, ekonomické aspekty obrany, informatika ve vojenství, revoluce ve vojenských záležitostech.

Integrujícím prvkem mezi jednotlivými pilíři strategických studií jsou strategické synergické studie pro obranu a bezpečnost (*prognózování a trendové analýzy*), které vytvářejí alternativní metody a návrhy možných řešení se zaměřením na výstavbu a použití ozbrojených sil ČR. Vytváří představu o pravděpodobné podobě prostředí, ve kterém budou ozbrojené síly působit, jejich úkoly, schopnosti a zdrojové možnosti.

V teoretické rovině je ústav primárně zaměřen na rozvoj ***vojenské strategie*** a zprostředkovaně ***na související vědní obory*** zejména politologii, mezinárodní vztahy a vojenskou ekonomii.

Ústav dále provádí konzultační, poradenské a expertizní činnosti v otázkách obrany a bezpečnosti. Vydává odborný časopis „Obrana a strategie“, který je zaměřen na publikaci textů z oblasti strategických a bezpečnostních studií, vojenství a příbuzných oborů. Časopis vychází dvakrát ročně v tištěné i elektronické verzi a je otevřen přispěvatelům z české i mezinárodní bezpečnostní komunity. Od roku 2007 vychází jako recenzovaný časopis.

Podrobné informace včetně struktury a členů Ústavu najdeme na internetových stránkách UO. [54]

2.5 Srovnávací analýza některých veřejně přístupných informačních zdrojů

WORLDWIDE GOVERNMENT AND DEFENCE DIRECTORY

Producent: WORLDWIDE GOVERNMENT DIRECTORIES

Databáze poskytuje široký záběr informací o světových vládních organizacích a jejich představitelích. Vychází ze tří základních zdrojů:

- WORLDWIDE GOVERNMENT DIRECTORY

obsahuje jména a kontaktní informace o klíčových hráčích světové legislativní a diplomatické komunity a také nejvyšší představitele více než 100 mezinárodních organizací jako jsou OSN, Světová banka nebo Rada Evropy. Jsou zde informace o ministrech, jejich náměstcích, poradcích, klíčových legislativních představitelích a soudech, diplomatických misiích apod. pro 195 zemí.

- WORLDWIDE DIRECTORY OF DEFENCE AUTHORITIES

je rozsáhlý zdroj kontaktních informací vojenských a obranných organizací celého světa. Záznam o každé zemi začíná přehledem obranné struktury a odpovědnosti různých agentur a ministerstev včetně údajů o počtech pracovníků a ročním rozpočtu. K dispozici jsou adresy vedoucích pracovníků ministerstev obrany, předních důstojníků a struktur taktického velení.

- PROFILES OF WORLDWIDE GOVERNMENT LEADERS

poskytují detailní biografie hlav států a ministrů vlád z celého světa. Informace jsou získávány z řady zdrojů, velvyslanectví, vlád a vlastní sítě korespondentů po celém světě.

AV-DATA (Aviation Data)

Producent: INFORMATION HANDLING SERVICES

Webová kolekce technických dokumentů týkajících se leteckého provozu a bezpečnosti letectví.

DMS/FI CONTRACT AWARDS

Producent: FORECAST INTERNATIONAL/DMS

Vychází ze státních dokumentů a mapuje státní kontrakty nad 25 000 USD z oblasti vojenství, obrany, dopravy, energie, administrativy, letectví a astronautiky. Retrospektiva od roku 1981 (aktualizace nepravidelná, cca 3,5 mil.položek).

ESDU - FOR ENGINEERS BY ENGINEERS

Producent: INFORMATION HANDLING SERVICES

Sbírka validovaných inženýrských dat, metod a softwaru pro vývoj a konstrukci, zejména v leteckém sektoru. Jde o více než 1300 dokumentů a příslušných programů.

GALE MILITARY AND INTELLIGENCE DATABÁZE

Producent: THOMSON GALE

Databáze obsahuje kolekci plných textů z více než 600 titulů časopisů s více jak 7 mil. článků, z nichž na 80% je dostupných v plném textu, zaměřených na oblast vojenství a zpravodajských služeb včetně přesahu do souvisejících oblastí jako je letectví, strojírenství, logistika aj.

GLOBAL DEFENSE INFORMATION

Producent: UNITED COMMUNICATIONS GROUP US NAVAL INSTITUTE TELDAN INFORMATION SY

Obsahuje abstrakty článků, zpráv, rozhovorů a mezinárodních kontraktů z předních světových periodik v oboru obrany za posledních 12 let od roku 1986. Pokrývá přes 9900 společností a dalších organizací a 35 000 produktů.

INFORMATION WARFARE

Producent: JANE'S

Zabývá se měnícími se principy vojenských informačních technologií a otázkami informační dominance na informačních bitevních polích.

MARKET INTELLIGENCE

Producent: FORECAST INTERNATIONAL/DMS

Patří k nejdůležitějším informačním zdrojům o trhu s vojenskou a dopravní technikou. Obsahuje plné texty analýz a popisů více než 3 000 civilních a vojenských

programů, včetně obrany a leteckého průmyslu v celosvětovém měřítku. Zabývá se též vojenskou výzbrojí, komerčními leteckými společnostmi, helikoptérami, leteckými motory a jejich kontrolou. Specialitou FI/DMS jsou detailní a časem dobře prověřené předpovědi vývoje každé oblasti v nejbližších 10 letech!
Aktualizace online v Dialogu je týdenní.
Konkrétní produkty
DMS/FI MARKET INTELLIGENCE REPORTS
MCGRAW-HILL AEROSPACE & DEFENSE

MILITARYnetBASE

Producent: CRC PRESS

Databáze pokrývá všechny otázky vojenství - historii, výzbroj, politiky, boj proti terorizmu a další.

NOUVELLES ATLANTIQUES / ATLANTIC NEWS

Producent: AGENCE EUROPE

Od roku 1967 jediný věstník přinášející systematicky zpravodajství a analýzy politických, obraných, technologických a ekonomických aktivit zaměřených na bezpečnost a obranyschopnost Evropy a západních států v rámci organizací jako jsou NATO, WEU, OSCE a Evropská unie jako celku.

PROQUEST MILITARY COLLECTION

Producent: PROQUEST

Kolekce časopisů poskytuje informace z oblasti vojenství, mezinárodních vztahů, politologie, kriminologie, obrany, letectva, vesmírných letů, komunikace, stavebnictví a další. Počet titulů sledovaných v kolekci je více jak 520, přičemž více jak 370 je plnotextových. Zpřístupňuje časopisy od roku 1991.

UNITING EUROPE

Producent: AGENCE EUROPE

Týdeník přináší každé pondělí (s výjimkou měsíce srpna) analýzy procesu slučování evropských států a zároveň vysvětluje význam rozšiřování Evropské unie na následujících úrovních:

- Stavy vyjednávání o možnostech přístupu mezi Evropskou unií a Polskem, Maďarskem, Českou republikou, Slovenskem, Estonskem, Bulharskem, atd.
- Vzájemné vztahy mezi Evropskou unií na jedné a státy střední a východní Evropy a zeměmi bývalého Sovětského svazu na druhé straně. Sledovány jsou přitom politické, ekonomické, finanční, kulturní a další aspekty.

JANE'S DEFENSE & AEROSPACE NEWS / ANALYSIS

Producent: JANE'S

Plné texty různých druhů primárních pramenů vydávaných u Jane's IG se zaměřením na novinky v oblasti armády, námořních a vzdušných sil, včetně výzkumu, vývoje, vojenského průmyslu a vybavení armády různými prostředky a obrannými systémy. Retrospektiva od 1982, aktualizace týdně, cca 92 000 zázn. (od r. 1993).

Konkrétní produkty:

JANE'S DEFENSE & AEROSPACE NEWS/ANALYSIS [587]

JANE'S WORLD DEFENCE INDUSTRY

Producent: JANE'S

Na CD-ROM poskytuje informace o 300 špičkových společnostech světového vojenského průmyslu. Společnosti nemusí být nutně největšími, ale jsou nejdůležitějšími vzhledem ke své pozici na trhu, produktům nebo technologiím, které vyvíjejí. Každý záznam poskytuje informace o obchodu dané společnosti a jeho struktuře prostřednictvím úplné analýzy aktivit, produktů, důležitosti, poboček, personálu a finanční výkonnosti.

Konkrétní produkty:

JANE'S WORLD DEFENCE INDUSTRIES

JANE'S WORLD INSURGENCY AND TERRORISM

Producent: JANE'S

Zdroj nepředpojatých a spolehlivých informací a profilů každé důležité teroristické skupiny včetně údajů o typech výzbroje, analýzy taktiky, počtu přívrženců a politických spojeních. Podává biografické informace o vedoucích představitelích včetně popisu vzhledu, známých společnících, politických aktivitách a jejich vojenských zkušenostech a výcviku. Poskytuje deník událostí podle jednotlivých

zemí s detailními popisy za posledních 12 měsíců. Pokrývá také nejnovější nebezpečí informačního věku, kybernetický terorismus.
Konkrétní produkty:
JANE'S WORLD INSURGENCY AND TERRORISM

JANE'S CHEMICAL-BIOLOGICAL DEFENCE GUIDEBOOK

Producent: JANE'S
Příručka poskytující veškeré dostupné informace o světových organizacích a metodách boje s chemicko-biologickými zbraněmi. K dispozici online.
Konkrétní produkty:
JANE'S CHEMICAL-BIOLOGICAL DEFENCE GUIDEBOOK

JANE´S ALL THE WORLD´S AIRCRAFT

Producent: JANE'S
JAWA představuje nejrozsáhlejší zdroj informací o leteckých programech v rámci celého světa. Obsahuje množství technických detailů k více jak 1 000 vojenských i civilních letadel, která jsou v současné době ve výrobě nebo se nacházejí ve fázi vývoje. Rovněž zpřístupňuje detailní profily několika set výrobců z 50 zemí.

JANE´S ARMOUR AND ARTILLERY

Producent: JANE'S
Nejnovější informace o systémech dělostřelectva a obrněných jednotek armád celého světa. Od posledního vydání přibyly nové sekce o obrněných transportérech a samohybných ostřelovacích systémech. Dále bylo zařazeno přes 400 nových obrázků.
Konkrétní produkty:
JANE´S ARMOUR AND ARTILLERY
JANE´S ARMOUR AND ARTILLERY UPGRADES

JANE´S COUNTER TERRORISM

Producent: Jane'sZdroj informací vážících se k vytváření anti-teroristických strategií. Příručka provede uživatele veškerými informacemi potřebnými pro plánování odvetných strategií, zpracovávání nepředvídaných událostí a přípravu bezpečnostních opatření.

JANE´S DEFENCE WEEKLY

Producent: JANE'S

Jane´s Defence Weekly představuje nejpřednější světový týdeník ve svém oboru, s největším množstvím technických detailů a informací ze zákulisí. Poskytuje pravidelné zprávy díky světové síti renomovaných korespondentů a unikátní skupině vlastních novinářů a technických redaktorů. V časopise kromě jiného najdete hloubkové zprávy ze zbrojního průmyslu, profily jednotlivých států, příležitosti na trhu, novinky z oblasti technologického vývoje, rozhovory s klíčovými osobnostmi. Online verze se aktualizuje dvakrát týdně, takže uživatel má přístup k opravdu nejaktuálnějším informacím.

JANE´S EXPLOSIVE ORDNANCE DISPOSAL

Producent: JANE'S

Je rozsáhlý průvodce identifikací a posuzováním nepoužité munice a výbušnin. Žádný jiný zdroj neposkytuje tak obsáhlé informace o technických parametrech společně s detaily o příbuzných zařízeních a službách. Průvodce poskytuje také důležité informace sloužící k přesné identifikaci munice a výbušnin - pestrou paletu barevných kódů, značek, názvů a označení.

JANE´S FIGHTING SHIPS

Producent: JANE'S

Jane´s Fighting Ships představuje nezávislý, vysoce aktuální zdroj informací o možnostech námořnictva jednotlivých zemí, o flotilách a zbraňových systémech. Obsahuje přes 4 000 fotografií (většina je barevných a pořízených v současnosti). Podrobné nákresy lodí umožní uživateli snadno identifikovat lodě válečného námořnictva 163 zemí světa.

JANE´S LAND AND SYSTEMS LIBRARY

Producent: JANE'S

Konkrétní produkty:

JANE´S LAND AND SYSTEMS LIBRARY

JANE´S LAND SYSTEMS IMAGE LIBRARY

Kompletní knihovna vyobrazení všech světových pozemních systémů:

- opevnění a dělostřelectvo
- transportéry a výzbroj
- přemosťovací systémy
- prostředky minové války

JANE´S POLICE AND SECURITY LIBRARY

Producent: JANE'S

Množství důležitých informací z oblasti policejních a bezpečnostních služeb.

JANE´S RADAR AND ELECTRONIC WARFARE SYSTEMS

Producent: JANE'S

Obsáhlý zdroj informací o pozemních, námořních a leteckých radarových, zpravodajských a komunikačních systémech.

JANE´S SENTINEL COUNTRY RISK ASSESSMENTS

Producent: JANE'S

Informační služba pokrývající bojovou připravenost, zbrojní průmysl, očekávané možnosti a nebezpečí a obranné schopnosti dané země nebo regionu.

JANE´S TERRORISM WATCH REPORT

Producent: JANE'S

Nejaktuálnější informace o teroristických a povstaleckých aktivitách po celém světě. Databáze dále umožňuje uživateli přístup k celému archivu předchozích bulletinů, takže má neustále přehled o pozadí aktuálních událostí. [48]

2.5.1 Vědecké a výzkumné instituce

Instituce uvedené na seznamu jsou celé přístupné veřejnosti nebo alespoň jejich části. Jedná se však o analytické informace, strategické a dlouhodobého charakteru. Proto je nelze využít pro vytvoření aktuálního situačního přehledu, tzn. nejsou vhodné pro operační a taktickou úroveň. Jsou vhodné pro vytváření informačních podkladů pro nejvyšší představitele MO ČR.

- CrisisWeb – International Crisis Group
- Central Asia – Caucasus Analyst
- International Relations and Security Network
- Congressional Research Service (US Department of State)
- Federation of American Scientists (FAS): Secrecy News
- Center for Strategic & International Studies
- Conflict Studies Research Centre
- The Jamestown Foundation
- Strategic Studies Institute of the U.S.Army War College
- Arms Control Association
- Institute of Peace & Conflict Studies
- International Policy Institute for Counter-Terrorism
- Jaffee Center for Strategic Studies
- Center for Nonproliferation Studies (Monterey Institute of International Studies)
- Institute for National Strategic Studies
- NTI – Nuclear Threat Iniciative
- Inteligence and Terrorism Information Center and the Center for Spoecial Studies
- České Centrum Strategických Studií
- Middle East Intelligence Bulletin
- Middle East Forum
- Country Indicators for Foreign Policy
- World´s Dictionary of Think Tanks
- Institute of Defense and Strategic Studies
- The Power and Interest News Report
- The Global Politician
- Defense Industry Daily
- Federal Research Division
- EIA- Energy Information Administration
- RFE – Resources for Economists on the Internet
- Global Health Reporting
- Profaca Mario´s Cyberspace Station: The Inteligence News Portal
- Open Source Solution

- Stockholm International Peace Research Institute
- SITE Institute Inteligence Subscription Service
- USAF Counterproliferation Center
- The Terrorism Research Center
- University of Military Intelligence
- RAND

2.5.2 Využitelné české placené databáze

ČESKÁ TISKOVÁ KANCELÁŘ

Možnost nastavení filtrů, např. zprávy z vojenství nebo zprávy o terorismu, zbrojení obecně atd.

ALBERTINA DATA - ANOPRESS

Není přímo vojenský zdroj, monitoring českých médií (okrajová záležitost).

INTERFAX – AGENSTVO VOJENNYCH NOVOSTEJ

Stěžejní faktografická databáze, která pokrývá Rusko a společenství nezávislých států. Pokrývá vojensko politickou oblast, tzn. personální a organizační změny v ruských silových strukturách, tzn. ministerstvo obrany, ministerstvo vnitra a zpravodajské služby, jmenování nových ředitelů, odvolání, povyšování, případně početní stavy, pokud se nejedná o utajovanou skutečnost.

V technické oblasti přináší zprávy o veškerých nových projektech, které organizují podniky ruského obranného průmyslu, je možné zjistit z hlediska technologického o co se tam jedná, co se bude vyvíjet, jaká bude nová technika, kdy bude zařazená do výzbroje, jaké jsou finanční náklady a s tím je následně spojená i ekonomická oblast tzn. vývoz, co kam Rusko vyváží jaké množství, v jaké hodnotě a jaké jsou plány, vyčleňování financí na obranu obecně, ale i na jednotlivé projekty.

Dále pokrývá veškerou činnost ruských ozbrojených sil tzn. cvičení na území ruské federace, může to být buď s kontrolou bojové připravenosti, nebo v souvislosti se zaváděním nové techniky do výzbroje a nebo společná cvičení s jednotkami jiných států např. Indie, Čína ale i státy NATO.

Je to faktografická databáze, proto zde nelze najít analýzy nebo predikce, což si z toho musí uživatel odvodit sám. Má ruskou i anglickou verzi. Ruská je lepší, pokrývá dění u ozbrojených sil. Anglická verze v porovnání s ruskou je redukovaná tzn. zkrácené články, které nejsou úplné, některé z článků chybí zcela. Úplně přesný nebývá ani překlad do angličtiny. [44]

STATFOR – STRATEGIC FORECAST

Komerční americký zdroj. Údajně ho založili bývalí příslušníci zpravodajských služeb. Je celosvětově uznávaný, využívají ho ozbrojené sily všech evropských států. Nezaměřuje se na faktické články, ale na analýzy a predikce budoucího vývoje, zejména v krizových oblastech. Jejich analýzy se vyznačují tím, že vždy mají krátký úvod a závěr, takže uživatel v případě, že chce rychle pročíst co nejvíce jejich analýz, se může podívat na jejich úvod a závěr a nemusí se prokousávat 2-3 stránkovým textem.

Zabývají se veškerou tématikou od terorismu přes ekonomiku související se zbrojním obchodem až po humanitární krize např. v Africe nebo v Asii. Rovněž jejich analýzy předpovídají možnosti budoucího vývoje v prostorech nasazení koaličních sil tzn. v Iráku a v Afganistánu.

INDIGO PUBLICATIONS

Komerční databáze pro armádu, která má více produktů např.: Inteligence online - analýzy týkají se zpravodajství a zpravodajských služeb.

UNITED PRESS INTERNATIONAL

Pro armádu jsou zajímavé dva produkty:

- International Intelligence – terorismus, mezinárodní zpravodajství a bezpečnost,
- Security and Terrorism - analýzy, nejsou to faktografická data. [46]

MIDDLE EAST NEWSLINE

Monitoruje oblast blízkého a středního východu. Sleduje problematiku obrany, strategie a vyzbrojování. Zaměření na faktografické články, faktografická data, mohou se vyskytnou i kratší analýzy. Denně jsou produkovány nové články.

Přístupný komerčně, pokud tam vstoupí veřejný uživatel, tak uvidí jenom část článků a bude to redukovaný text. Úplné články nezpřístupňuje bezplatně vůbec a pokud jde o kvantitu článků, tak jenom část. Pokrývá např. Libanon, palestinskou Gazu, otázku Palestiny, Sýrii, Jordánsko, Irák, Irán a samozřejmě i obchody těchto států s ostatními zeměmi, převážně s Ruskem. [43]

DEBKA FILE

Izraelský zdroj. Nejedná se o faktografickou databázi, jde o analýzy. Verze je placená i neplacená. V neplacené části sou přístupné buď zkrácené články, minimum analýz. V kterémkoliv článku je i názor zpracovatele, nebo predikce budoucího vývoje.

Protože je to zdroj izraelský, monitoruje oblast blízkého a středního východu. Je zde jiný pohled na dění, než mají Evropané. To vyplývá z toho, že to píšou Izraelci. Evropanům se mohou zdát např. některé články o terorismu, pronikání al-Káidy tendenční. Oblast blízkého východu však pokrývá téměř bezkonkurenčně. [45]

UNMIK – LOCAL MEDIA MONITORING

Služba mezinárodní mise v Kosovu, která se zabývá monitoringem místního tisku se zaměřením na bezpečnostní situaci, vojenský a politický vývoj v provincii. Přebírá články z místních sdělovacích prostředků, překládá je do angličtiny, nepřidává k nim žádný vlastní komentář.

SEE SECURITY MONITOR

Komerční instituce, která monitoruje veškeré události, včetně bezpečnostní situace v prostoru Balkánu. Pro ozbrojené síly jsou přínosné informace ze Srbska, Kosova, Černé Hory a Makedonie.

KOSOVA LIVE

Kosovská zpravodajská agentura. Spíše doplňkový zdroj, anglická verze je stručnější než albánská.

AFGHAN NEWS NETWORK

Monitoruje afgánská média, zaměřuje se na bezpečnostní situace a na politické a ekonomické události, které by mohly vývoj bezpečnostní situace ovlivnit.

Kromě toho přebírá zprávy od renomovaných světových agentur, jako např. AFP, Associated Press, týkající se Afghánistánu. Má anglickou verzi, lze považovat za doplňkový informační zdroj.

PAK TRIBUNE

Pakistánský zdroj (deník). Zaměřuje se na problematiku bezpečnosti jak Afghánistánu, tak v Pákistánu. Právě události v Pákistánu jsou pro úspěšné pokračování mise ISAF důležité. Jde o veřejně přístupný, doplňkový zdroj.

OPEN SOURCE CENTER

Více naznačí jeho dřívější název Foreign Broadcast Information Service (Informační služba zahraničního vysílání). Jde o americký zdroj, není dostupný ani veřejně ani komerčně. Poskytuje se členským státům NATO na základě mezivládní dohody.

Má celosvětový záběr, monitoruje s výjimkou amerických, veškeré hlavní světové a regionální deníky i další periodika ve všech jazycích. Podle neoficiálních zdrojů má tato služba několik desítek tisíc zaměstnanců. Zprávy z regionálních deníků (i ty, které jsou třeba v originále ve farsí, nebo v regionálních nářečích) se objevují maximálně s 2-3 denním zpožděním (přepsané samozřejmě do angličtiny).

Kromě deníků monitoruje i zahraniční regionální rozhlasové a televizní vysílání u kterého provádí transkripci do angličtiny.

Zpracovává i vlastní analytické zprávy z krizových a zájmových oblastí. Ty se mohou týkat např. aktuální bezpečnostní situace v Afghánistánu, aktivit čínských zpravodajských služeb nebo zbrojních kontraktů Venezuely.

Zveřejňuje i pravidelné souhrnné informační materiály jako např. Iraqi Mosquito.

DEFENSE NEWS

Americký zdroj, monitoruje hlavně oblast technologií a vývoje nových systémů. Pokrývá všechny druhy vojsk. Zvláštní součást má zaměřenou na systémy velení a řízení. Má část placenou, která není přístupná veřejnosti a část neplacenou. Část neplacená je redukovaná, články nejsou celé. Část placená je přístupná uživatelům, kteří si objednají např. tištěnou verzi Defense News. Vyhledávání funguje pomocí klíčových slov s využitím booleovské algebry. [42]

2.5.3 Hlavní zdroj MO – Jane´s

Klíčový informační zdroj pro Ministerstvo obrany České republiky. Poskytuje informace využitelné k aktuální informovanosti velitelů v oblasti vyzbrojování. Informace dlouhodobého charakteru slouží k odhadu dlouhodobé predikce.

JANE´S

Přibližně před dvěma měsíci změnily uživatelské rozhraní. Je zajímavostí, že v katalogu produktů je poskytují jako jednotlivé databáze, jejich seznam je vytvořen:

- podle abecedního pořádku,
- podle tématu.

Je pouze na uživateli, který přehled si zvolí. Uživatel si může každou databázi pořídit zvlášť (online, nebo na DVD). V případě, že se jedná o akvizici více databází, které

jsou svým zaměřením podobné, je vhodné si pořídit tzv. Library (knihovnu), nebo-li ucelený soubor příbuzných databází nabízený jako jeden komerční produkt.

Knihovna je stručně popsána, respektive její obsah, co všechno jednotlivé databáze pokrývají. V případě, že by si uživatel nevybral z nabízených knihoven, může si sestavit vlastní. Cena nestandardní knihovny však bude záležet na dohodě s poskytovatelem.

Přehled nabízených knihoven:

DEFENCE EQUIPMENT LIBRARY

Zahrnuje 23 jednotlivých databází Jane´s, poskytujících informace, novinky a analýzy o vojenské technice. Pokrývá vzdušnou, leteckou, pozemní, námořní techniku a zabývá se i problematikou obranného průmyslu.

DEFENCE MAGAZINES LIBRARY

Zahrnuje 10 produktů, pokrývá problematiku obrany a bezpečnosti. Některé z elektronických dokumentů (zejména technika) mají doprovod ve formě obrazových příloh.

MARKET INTELLIGENCE LIBRARY

Portfolio tvoří 17 jednotlivých databází Jane´s. Týká se obranného průmyslu, ale i komerčního průmyslu, nebo civilního sektoru v souvislosti se zakázkami pro ozbrojené síly nebo silové složky.

SECURITY LIBRARY

15 dílčích databází Jane´s. Pokrývá ozbrojené síly, tzn. jejich strukturu, jejich výzbroj, případně jejich nasazení, oblast bezpečnosti, terorismus a krizové oblasti v souvislosti s gerilovým a povstaleckým hnutím a odbojem. Kromě armády pokrývá i policii, pohraniční stráž a bezpečnostní agentury.

SENTINEL LIBRARY

15 produktů Jane´s. Poskytuje informace o globální bezpečnosti, hodnocení rizik a hrozeb pro jednotlivé státy, včetně všeobecné databáze zhodnocující rozsah hrozeb

a rizik v globálním měřítku. Důležité je, že poskytuje profil daného státu, zpravidla analýzu vnitropolitické a vnitřní situace se vztahem k bezpečnosti, a o externích faktorech ovlivňujících bezpečnost daného státu. Pro rychlý přehled poskytuje tzv. produkty Executive Summary. Zde se uživatel dozví nejdůležitější základní informace o aktuální bezpečnostní situaci v dané zemi (není to vystihující produkt, slouží k náhledu, uživatel se dozví základní informace a získá představu).

TRANSPORT LIBRARY

Tvoří ji 18 produktů Jane´s. Informace o problematice dopravy. Jsou to faktografické informace pokrývající všechny druhy dopravy (letecká, pozemní, námořní). Jedná se zejména o novinky (zprávy) typu: „společnost ALENIA přišla s novým dopravním letounem, s určitou kapacitou, nosností, bude vyrábět civilní i vojenskou verzi. Vojenskou verzi si objednala italská armáda a kontrakt zvažuje i Ministerstvo obrany Polska“. Kromě toho má Jane´s na své stránce „Products“ stručný přehled pro uživatele z oblasti bezpečnosti - jak kterou oblast pokrývají, tzn. kolik produktů Jane´s se zabývá letectvem, pozemním vojskem, námořnictvem a kolik všemi druhy vojsk dohromady a které produkty se zabývají obranným průmyslem. Pro uživatele je k dispozici i návod, jak si produkty objednat, včetně jejich cen. V případě, že se uživatel přesto špatně v nabídce orientuje, může se obrátit na poradenskou službu Jane´s, která poskytuje mj. konzultační služby.

Režim vyhledávání je v databázích Jane´s jednoduchý a pokročilý. V pokročilém je možné si nastavit určitá omezující kritéria (období; databáze; prohledávání textu, nebo pouze nadpisů; atd.). Nevýhodou je, že nelze kombinovat dva a více dotazů, jako např. v Dialogu. Proto v případě, že je vyhledáno příliš mnoho dokumentů, dotaz se musí zpřesňovat. To může samozřejmě činit potíže a hrozí možnost nevyhledání relevantních zpráv. [48]

3. POŽADAVKY NA INFORMAČNÍ SYSTÉMY VE STÁTNÍ SPRÁVĚ

Požadavky na IS ve státní správě ČR, *práva a povinnosti, které souvisejí s vytvářením, užíváním, provozem a rozvojem IS*, stanoví zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů. Provozovatelé jsou povinni při provozování IS zajišťovat ochranu a bezpečnost informací v rámci provozovaného IS v rozsahu stanoveném prováděcím předpisem, který stanoví minimální bezpečnostní požadavky k zajištění důvěrnosti, integrity a dostupnosti zpracovávaných informací. IS se navzájem propojují do sítí lokálních (LAN), rozsáhlých (WAN), metropolitních (MAN) nebo celosvětové sítě internet. Dochází k omezení vlivu časových a prostorových bariér, nabízí se nám možnost využívání široké studnice informací a znalostí prostřednictvím informačních sítí. V oboru IT se pod pojmem síť (určitý počet bodů, síťových prvků – uzlů navzájem propojených za účelem vzájemné komunikace) rozumí skupina bodů navzájem propojených komunikačními kanály. Sítě mohou být navzájem propojeny s jinými sítěmi a mohou obsahovat podsítě, ve kterých jsou uloženy informační zdroje s různou možností přístupu. Úkolem sítě je tedy zajistit přenos informací mezi komunikujícími uzly. Vzájemné propojování se subjekty a pracovišti vytváří prostředí pro efektivní hlasovou a datovou komunikaci a přístup k centrálním i regionálním informačním zdrojům. Tomuto procesu obecně říkáme budování komunikační infrastruktury (dále jen KI).

3.1 Obecné požadavky na Informační systémy veřejné správy

Prováděcím předpisem, který stanovuje minimální požadavky na bezpečnost ISVS je vyhláška NBÚ č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. Pro všechny systémy, které zpracovávají utajované citlivé informace, musí být nasazen celistvý komplex bezpečnostních opatření, který umožňuje splnit bezpečnostní cíle, zajistit ochranu informací a podpůrných systémových služeb a zdrojů. Porušení bezpečnostních provozních opatření záměrným nebo náhodným způsobem jednání vede ke

skutečnému nebo možnému kompromitování informací v KIS nebo podpůrných systémových služeb a zdrojů (např. ztráta informací během jejich přepravy, ponechání informací bez dozoru v nezabezpečené zóně, přístup neprověřených osob do objektu bez doprovodu, ztráta uložených dokumentů, neoprávněné modifikace, zničení neoprávněným způsobem nebo odmítnutí služby KIS).

3.2 Obecné bezpečnostní požadavky na Informační systémy veřejné správy

Na bezpečnost lze nahlížet z několika stran. Bezpečností systému se rozumí obvykle to, že data v IS jsou bezpečně uložena a že k nim nemá přístup neoprávněný uživatel. Bezpečnost IS však znamená i to, že je schopen své služby poskytovat pokud možno nepřetržitě. Je samozřejmé, že žádný systém nelze vybudovat jako naprosto spolehlivý, je však třeba zvolit takovou míru rizika, která je pro daný systém přijatelná a současně z finančního hlediska ještě únosná, protože se stoupajícími nároky na bezpečnost prudce rostou i náklady na její zajištění.

Zavádění nových IT vyvolává kromě obecných bezpečnostních požadavků i zvýšený zájem o bezpečnost sítí a přenášených informací. Mezi základní požadavky komunikační bezpečnosti patří zajištění **důvěrnosti** (ochrana proti nepatřičnému rozkrytí informací - utajení), **integrity** (správnost a celistvost informací a komponent), **dostupnosti** (informace jsou přeneseny a jsou k dispozici pro použití ve stanoveném časovém limitu) a **odpovědnosti** (jakákoliv činnost v systému je prováděna identifikovaným a oprávněným uživatelem, nebo správcem).

3.2.1 Zajištění důvěrnosti

Při zajištění důvěrnosti informací musí být přijaty takové bezpečnostní funkce, které dokáží zabránit odposlechu nebo přesměrování dat z komunikačních linek (kontrola nad sdělováním utajovaných a citlivých informací, přístup k informacím a k podpůrným systémovým službám a zdrojům). Bezpečnostní funkce zajišťující důvěrnost bývá typicky implementovaná vhodným šifrovacím mechanismem a administrativními předpisy pro zacházení s kryptografickými algoritmy. Kryptografický mechanismus je tvořen nejen kryptografickým algoritmem, ale i kryptografickým klíčem, tzn. dvěma vstupními parametry algoritmů

pro šifrování a dešifrování. Pokud komunikující partneři používají stejný kryptografický klíč k šifrování (K_E) a dešifrování (K_D), tzn. $K_E = K_D$, pak hovoříme o modelu **symetrické kryptografie** nebo také o *kryptografii se sdíleným tajným klíčem.* Znalost tajného klíče může sloužit i jako důkaz identity. Symetrickou kryptografii mimo služby zajištění důvěrnosti lze použít i pro identifikaci a autentizaci (ověření totožnosti vzdáleného adresáta). Bezpečnostní funkce může být implementována ověřováním znalosti tajné informace (heslo nebo osobní identifikační číslo - PIN), ověřováním vlastnění určitého předmětu (klíč, magnetická[8] nebo čipová karta[9]) nebo ověřováním fyzických charakteristik (otisk prstu, vzorek oční duhovky). Pokud se kryptografické klíče komunikujících partnerů vzájemně liší, tzn. $K_E \ddagger K_D$, jde o model **asymetrické kryptografie**. Typickým příkladem aplikace asymetrické kryptografie je *kryptografie s veřejným klíčem*, přesněji řečeno dvojicí *veřejný klíč* (V_K - všeobecně známý) *a soukromý klíč* (T_K - tajný). Kdokoli může srozumitelný (otevřený) text zprávy použitím V_K zašifrovat, šifru však může převést zpět do srozumitelného textu pouze ten, kdo vlastní dešifrovací T_K. Jedinečnost znalosti soukromého klíče umožňuje použít asymetrický model pro implementaci nejen důvěrnosti a autentizace, ale i pro implementaci nepopiratelnosti aplikací digitálního podpisu.

3.2.2 Zajištění integrity

Jedním z nejdůležitějších bezpečnostních požadavků, kladených na proces zpracování, ukládání a přenášení informací je požadavek na zajištění **integrity** těchto dat, tzn. požadavek na zabránění neoprávněné modifikace dat. Integrita utajovaných a citlivých informací a podpůrných systémových služeb a zdrojů musí být chráněna minimálním souborem opatření zaměřených na zajištění celkové ochrany proti úmyslným a neúmyslným hrozbám. U samostatných dokumentů je toho obvykle dosahováno tím, že se k datům připojí jistá informace, která příjemci *autentizuje,* tzn. prokazuje totožnost odesílatele nebo tvůrce dat, a to pouze v tom případě, že ji

[8] Hanáček P., Staudek J., Úřad pro státní informační systém 2000, Bezpečnost IS: **Magnetické karty** se používají poměrně dlouho a v mnoha aplikacích (bankomaty, placení v obchodech, řízení přístupu do zabezpečovaných prostorů).

příjemce přijal spolu s daty neporušenou. V případě, že příjemce musí autentičnost přijatých dat prokázat nezávislé třetí straně, hovoříme o vlastnosti *nepopiratelnost autora elektronického podpisu*, tzn. autor dokumentu nemůže popřít autorství dokumentu ani jeho obsah. Technická realizace zajištění autentičnosti dat vychází z předpokladu, že u dat na papírových médiích je autentičnost zajišťována pomocí manuálního podpisu. To přináší potřebu spolehlivé a efektivní náhrady manuálního podpisu podpisem elektronickým (digitálním), který může být stejně jako manuální podpis použit pro identifikaci a autentizaci původce informace. Elektronický podpis může být také použit pro kontrolu, že informace nebyla po podepsání změněna, čímž lze zajistit integritu informace. Na rozdíl od manuálního podpisu však nelze pomocí elektronického podpisu rozlišit originál informace od její kopie.

3.2.3 Zajištění dostupnosti

Zajištění **dostupnosti** utajovaných a citlivých informací a podpůrných systémových služeb a zdrojů znamená, že informace a služby musí být na vyžádání dostupné oprávněným uživatelům. IS musí být vybaven funkcí *tolerance k chybám* (poskytuje ochranu proti nedostupnosti kapacit způsobených výpadkem IS), *prioritou služeb* (zajišťuje, že zdroje budou přednostně přidělovány důležitějším nebo časově kritickým úlohám a že si je nebudou moci monopolizovat úlohy s nižší prioritou) a *alokací zdrojů* (zajišťuje limity na využití dostupných zdrojů, a tím zabraňuje uživatelům v monopolizaci zdrojů). Organizace jsou povinny připravit plány pro případ výskytu neočekávaných situací, podle nichž by byla organizována ochrana nebo likvidace utajovaných a citlivých informací a zdrojů v mimořádných situacích s cílem zabránit neoprávněnému přístupu, prozrazení a ztrátě jejich dostupnosti. Maximální prioritu v těchto plánech mají nejcitlivější informace, informace kritické z hlediska plnění úkolu nebo informace kritické z hlediska času. Aby bylo možné zabraňovat incidentům, které mají dopad na důvěrnost (únik utajovaných informací), integritu (porušení důvěrnosti, modifikace dat) a dostupnost (vyřazení určité funkce ze systému - účtovatelnost, ztráta auditních záznamů a pod.) utajovaných a citlivých informací a podpůrných systémových služeb a zdrojů, je nutné předcházet jim,

[9] Tamtéž: **Čipové karty** (smart cards) jsou karty s mikroprocesory, pamětmi RAM a ROM, poskytují větší paměťovou kapacitu než magnetické karty a navíc poskytují zpracovatelský výkon přímo na kartě. Umožňují uložená data fyzicky chránit.

detekovat je a zajišťovat obnovení původního stavu. Musí fungovat bezpečnostní řídící mechanismy a procedury, a to včetně oznamování bezpečnostních incidentů. Jako podklad a důkaz pro vyšetření záměrné nebo náhodné kompromitace důvěrnosti, integrity a dostupnosti informací slouží **účtovatelnost**, která zahrnuje zodpovědnosti uživatelů za akce, které v systému provádějí. Jde o bezpečnostní funkce *audit* (zajišťuje detekci, zaznamenávání a pozdější analýzu událostí důležitých z hlediska bezpečnosti, tzn. mechanismus protokolování událostí), *identifikace a autentizace* (zajišťuje zjištění a bezpečné ověření identity uživatele IS) a *důvěryhodná cesta* (umožňuje uživateli bezpečnou a přímou komunikaci s centralizovaným IS). Tam, kde bylo na základě vyhodnocení rizik zjištěno, že utajované a citlivé informace jsou v důsledku zvláštních hrozeb a výskytu zranitelných míst vystaveny zvýšenému riziku, musí být přijata doplňující opatření přiměřená okolnostem v rámci personální, fyzické (objektové) a informační (INFOSEC) bezpečnosti.

3.2.4 Specifické požadavky na Informační systémy ve státní správě v podmínkách vojenství

V mnoha zemích již po několik let probíhá přeměna průmyslové společnosti ve společnost informační. Tento proces je určován informační a komunikační technikou, jakož i stoupající potřebou komunikace nejen civilních, ale i vojenských institucí. Využívání informací ve vojenství vždy hrálo důležitou úlohu. Za rozhodující veličinu v budoucích konfliktech je považována schopnost pokud možno optimálně zasadit jako určujícího činitele informace. Zásadním cílem je ovlivňovat rozhodujícím způsobem proces nepřátelského rozhodování tvořeným prvky zjišťování a hodnocení situace, přijetím rozhodnutí a jednáním. K tomu je především nutná elementární znalost nepřátelských informačních toků a procesů zpracování informace. Vedení války proti nepřátelské informační a komunikační infrastruktuře je označováno jako informační válka. Zabývá se v nejširším smyslu získáváním, zpracováním a využíváním informací, jakož i ovlivňováním lidí a strojů a jejich rozhodování. Informační válka je definována jako souhrn opatření k :

- ochraně vlastních informací a procesů na nich založených,
- ochraně informační techniky,
- působení na nepřátelské informace a procesy na nich založené,

- působení proti nepřátelské informační technice.

Úvahy o informační válce se nevztahují na konflikt s nepřítelem používajícím nevyspělou technologii, protože v těchto případech bude schopnost vedení tradičního boje pro moderní armádu důležitější. V návaznosti na informační válku je nezbytné zaujmout i nový přístup ke státní bezpečnosti a stanovit specifické požadavky na IS v dané lokalitě. Je žádoucí a účelná kooperace a koordinace vojenských a civilních aktivit pro ochranu před útoky informační války.

Reálná představa předpokládaného rozvoje celosvětových bezpečnostních struktur bude ovlivněna variantností vývoje hlavních prvků světového vývoje. Strategické bezpečnostní prostředí ČR bude výrazně ovlivněno mezinárodní a vojenskopolitickou situací v zemi, v okolních státech, v Evropě a ve světě. Významným prvkem utvářejícím evropské bezpečnostní prostředí je Organizace pro bezpečnost a spolupráci v Evropě.

Jednou z klíčových podmínek pro zajištění fungování celé struktury AČR jak v mírových, tak i ve válečných podmínkách je funkční KI. V rámci zajištění KI jsou komplexně řešeny technické, síťové, aplikační, bezpečnostní a organizační problémy související s hlasovou i datovou komunikací. Důležitým požadavkem na KI je schopnost jejího dalšího rozvoje a otevřenost vůči novým požadavkům na jednotlivé poskytované služby. KI musí operativně reagovat na začlenění ČR do politicko-ekonomických (Evropská unie) a vojenských (NATO) uskupení. Řešení KI musí být natolik otevřené, aby umožnilo kompatibilitu IT a produktů používaných u jednotlivých útvarů a zařízení resortu obrany. Důraz musí být kladen na sjednocení komunikačního prostředí na základě celostátně platných právních norem včetně interních normativních aktů (dále jen INA) pro připojování do KI AČR.

3.2.5 Zvláštní odpovědnost na úseku informační bezpečnosti

Odpovědnost na úseku bezpečnosti utajovaných informací vyžaduje na národní úrovni existenci některých ústředních úřadů. Pro tyto účely byl v souladu se zákonem

č. 148/1998 Sb.,[10] zřízen **Národní bezpečnostní úřad**, který je bezpečnostní autoritou ČR. K ochraně utajovaných informací musí být používány kryptografické prostředky certifikované NBÚ, nebo organizací, kterou NBÚ pověřil. Právním předpisem jsou stanoveny způsoby použití, nasazování, evidence kryptografických prostředků, používání klíčových materiálů a zjišťování odborné způsobilosti pracovníků kryptografické ochrany utajovaných informací. Distribuci kryptografických materiálů (šifrových materiálů), tzv. kryptoklíčů, kryptozařízení, kryptopublikací předávaných do ČR výbory a agenturami NATO pro vojenskou i civilní sféru zajišťuje **Národní Distribuční Agentura** (NDA), která je delegovaná z NBÚ na MO ČR.

K 1. 1. 2003 vzniklo **Ministerstvo informatiky ČR** (dále jen MI ČR) na základě novely tzv. kompetenčního zákona, které převzalo kompetence v oblasti *telekomunikací* (od úseku spojů), v oblasti *informační společnosti* (v plném rozsahu působnosti dřívějšího Úřadu pro veřejné informační systémy, který byl se vznikem MI ČR zrušen) a v oblasti *elektronického podpisu* (od Úřadu pro ochranu osobních údajů). Působnost MI ČR je dána zejména zákonem č. 365/2000 Sb., o informačních systémech veřejné správy (dále jen ISVS) a zákonem č. 151/2000 Sb., o telekomunikacích. MI ČR zpracovává návrhy strategických dokumentů v oblasti ISVS, vytváří a spravuje Portál veřejné správy, koordinuje, vytváří podmínky pro podporu rozvoje elektronického obchodu a hodnotí projekty, které mají meziresortní dopady na ISVS. Zodpovídá za tvorbu legislativních návrhů a politiky v oblasti telekomunikací, stanovení principů a hlavních zásad regulace telekomunikačního trhu. Schvaluje plán přidělování kmitočtových pásem a uděluje akreditace k působení jako akreditovaný poskytovatel certifikačních služeb v oblasti elektronického podpisu. V roce 2007 MI ČR zaniklo a kompetence byly převedeny na **Ministerstvo vnitra ČR**.

MO ČR je pro účely zákona orgánem státu s postavením ústředního úřadu, jehož statutárním orgánem je **Ministr obrany ČR**, který jmenuje ***bezpečnostního ředitele*** (dále jen BŘ MO**)** v rámci Odboru bezpečnosti MO (dále jen OB MO). BŘ MO je přímo podřízen MO ČR a je pověřen plněním povinností, které zákon v oblasti OUI ukládá. OB MO vykonává koncepční, normotvornou, plánovací,

[10] V současné době je zákon zrušen a nahrazen zákonem č. 412/2005 Sb., o ochraně UI a bezpečnostní způsobilosti

organizátorskou, koordinační, kontrolní a analytickou činnost v oblasti OUI. Metodicky řídí činnost orgánů bezpečnosti informací v resortu MO, které zabezpečují OUI na jednotlivých stupních velení v organizační struktuře resortu MO.

Můžeme tedy říci, že určujícími faktory informační společnosti a bezpečnosti informací jsou informace, vědomosti a znalosti. A právě zde zkušenosti ukazují, že lidský faktor je tím nejvíce rizikovým v oblasti bezpečnosti. Proto je velmi důležité věnovat se vzdělávání, kontrole a přípravě personálu.

3.2.6 Lidské zdroje v informační společnosti

Za informační společnost je považována společnost, ve které hlavní roli hrají informace společně s informačními a komunikačními technologiemi. Informační a komunikační technologie vytváří globální informační společnost, která zakládá své bohatství na lidském kapitálu. Úspěch společnosti je dán schopnostmi jedinců určit relevantní informační zdroje, informace z nich získat, analyzovat a využívat pro rozhodování, řešení úkolů a problémů ke zvýšení efektivity práce a soukromého života.

V informační společnosti pojem informační gramotnost (*schopnost rozezenat potřebu informace, umět ji vyhledat, vyhodnotit a efektivně využít*) zastřešuje gramotnost funkční a počítačovou.

3.3 Systém odborných vědeckých vojenských informací v ČR

Odborné vojenské informace v ČR poskytuje AČR, která je hlavní složkou ozbrojených sil ČR. Dále zahrnuje Vojenskou kancelář prezidenta republiky a Hradní stráž. Hlavním posláním armády je a vždy bude co nejefektivnější a nejlepší zabezpečení obrany území ČR s využitím zásad kolektivní obrany v souladu s článkem 5 Washingtonské úmluvy. Je zapojena do integrované vojenské struktury NATO, do systému obranného, operačního a civilního nouzového plánování, do procedurálních a organizačních aspektů jaderných konzultací a do společných cvičení a operací.

Jednotnou realizaci vydavatelské a nakladatelské činnosti v resortu MO ČR zabezpečuje vojenské zařízení - Agentura vojenských informací a služeb (dále jen AVIS), které odpovídá za:

- vydávání a distribuci periodických a účelových publikací,
- dodržování a realizaci ustanovení zákona o právu autorském, knihovního, tiskového zákona a zákona o archivnictví a spisové službě v oblastech své odborné působnosti,
- audiovizuální a fotodokumentační tvorbu,
- práci s vojenskovědeckým knihovním fondem,
- hospodaření s filmovým archivem,
- propagaci a prezentaci resortu obrany na veřejnosti při tematických výstavách a vojenských i společenských akcích.

AVIS dále plní povinnosti, které vyplývají z členství v Evropské asociaci vojenského tisku (dále jen EMPA), a úkoly vyplývající z členství v systému mezinárodního standardního číslování seriálových a neseriálových publikací (dále jen ISSN, ISBN). Pracoviště sídlí v Praze 6 - Dejvicích v budově bývalého Vojenského zeměpisného ústavu, v jeho čele je ředitel, kterého jmenuje a odvolává ministr obrany.

Odborné vojenské informace jsou dále publikovány na internetových stránkách http://www.army.cz, jejichž vlastníkem a provozovatelem je Ministerstvo obrany ČR, se sídlem Tychonova 1, 160 01 Praha 6, zapsaná v Obchodním rejstříku, vedeném u Městského soudu v Praze, oddíl B, vložka 6941, IČ: 60162694, DIČ: CZ60162694. [58]

Důležitým zdrojem odborných vojenských informací je vědecká konference CATE (Community – Army – Technology – Enviroment, v českém překladu *Společnost – Armáda – Technika – Životní prostředí*), která tvoří nosný pilíř odborného doprovodného programu Mezinárodního veletrhu obranné a bezpečnostní techniky IDET, konané každoročně na výstavišti v Brně. Po odborné stránce je CATE setkáním armádních specialistů a specialistů z obranného průmyslu. Je pevnou součástí systému vědeckých konferencí pořádaných v AČR a proto nad jejími dílčími

částmi přebírají pravidelně záštitu vedoucí funkcionáři resortu obrany. Vysokou odbornou úroveň konference garantuje Univerzita obrany v Brně.

4. DOPORUČENÍ PRO OPTIMALIZACI VYUŽÍVÁNÍ INFORMACÍ VE VOJENSKÉM VÝZKUMU, ŠKOLSTVÍ A PRAXI

V současné době pokračuje transformace v rámci rezortu obrany s cílem optimalizovat řídící struktury, organizaci a administrativu. Dochází ke snižování počtů osob v armádě a procesu technizace a informatizace vojenství, který přináší velmi pozitivní efekt v potenciálu obranných prostředků, získávání informací v reálném čase a přijímání optimálních rozhodnutí v oblasti velení a řízení. Víme, že žádný komunikační a informační systém (dále jen KIS) nelze navrhnout bez zranitelných míst, lze však snížit pravděpodobnost uplatnění vnitřních[11], vnějších[12] a fyzických[13] hrozeb použitím vhodného řešení, které uvažuje přiměřená bezpečnostní opatření. Zranitelnost svou povahovou může být technická, procedurální nebo provozní. Využívání zranitelných míst je rozhodující pro důvěrnost, integritu a dostupnost informací uložených v KIS. Z pohledu vojenských specifik, pro které jsou vojenské KIS určeny, je potřebné hodnotit hrozby i z hlediska specifických vojenských požadavků. Dnes rozeznáváme celé spektrum možných hrozeb s nejrůznějšími motivacemi. Mezi nejzávažnější patří:

- zpravodajské služby států se zaměřením na průmyslovou, politickou a vojenskou špionáž s cíli zabezpečit politické a ekonomické zájmy svých vlád,
- zpravodajské služby firem s orientací na získání a udržení odbytišť, zakázek a technologického „knot how“,
- teroristické organizace a extremistické skupiny (národní a mezinárodní),
- kvalifikovaná kriminalita namířená především proti finančním, správním a bezpečnostním institucím a jejich KIS,

[11] **Vnitřní hrozby** způsobují ztrátu, zničení dat nebo nedostupnost služby, které jsou způsobené lidskou chybou (*nedostatečné proškolení, úmyslné poškození*), poruchou nebo závadou. Uplatnění hrozeb může způsobit neautorizovaný přístup k informacím, poškození systémových programů a uložených dat nebo zavedení škodlivého programového vybavení.

[12] **Vnější hrozby** způsobují ztrátu, zničení dat nebo nedostupnost služby, které jsou způsobené náhodně nebo záměrně vyvolanou poruchou nebo závadou, nebo člověkem, který nemá přístup ke KIS.

[13] **Fyzické hrozby** způsobují ztrátu, zničení dat nebo nedostupnost služby, způsobené nehodou nebo živelnou pohromou.

- rutinní hackeři, creckeři, studenti a zvídaví lidé s odborným vzděláním v oblasti informatiky, kteří často bez motivace pronikají do KIS a rozrušují jejich integritu,
- informační válka jako specifický faktor, který vstupuje do budování vojenských KIS.

K zabezpečení obecných požadavků na ochranu informací je nutné implementovat *vnitřní bezpečnostní ochranné mechanismy* do technického, programového a mikroprogramového vybavení používaných přenosových prostředků. K dosažení komplexní ochrany je nutné implementovat *vnější bezpečnostní ochranné mechanismy* formou fyzických, personálních, procedurálních a administrativních bezpečnostních opatření.

Armáda by měla pro optimalizaci využívání informací stejně jako jiná firma hledat způsoby, jak si upřesnit vlastní postavení ve společnosti a zjistit co nejpřesněji znalost vlastních silných a slabých stránek. K tomu potřebuje:

- stanovit, co je pro strategii obrany prioritní a podstatné,
- definovat, které informace potřebuje a které jevy v okolním světě musí monitorovat,
- působit na nepřátelské informace a procesy na nich založené, včetně působení proti nepřátelské technice,
- zajistit dostatečně výkonné a kapacitní úložiště vlastních dat a nástroje pro jejich zpracování,
- zajistit ochranu vlastních informací a procesů na nich založených, včetně ochrany informační techniky,
- zajistit KIS kryptografickou ochranou (šifrováním) ve všech kanálech, fyzickou odolnost uzlových a jiných důležitých bodů,
- řídit bezpečnost propojování KIS se sítěmi veřejných operátorů (*veřejnými telefonními a datovými sítěmi*), celosvětovou sítí internet a definovat okruhy a porty, na které se předpokládá nasadit kryptografická ochrana,
- zamezit odposlechu a vyhodnocení vyzařování elektromagnetického pole komunikační a výpočetní techniky,

- zaměstnat nadšeného manažera systému pro správu znalostí a zajistit mu nejlepší možné podmínky pro komunikaci s velením,
- zabezpečit procesní model a někoho, kdo se bude trvale snažit najít optimální podobu procesů a informací, které jsou pro jejich optimální průběh a pro zajištění ostatních informačních potřeb nutné (*může být stejný člověk, který zastává funkci manažera znalostního systému, který by řídícím pracovníkům nabízet analýzu informací, předkládat návrhy a projekty*),
- neustále provádět proškolení svých zaměstnanců v oblasti bezpečnosti informací s cílem získat silné bezpečnostní podvědomí uživatelů KIS,
- zajistit zveřejnění zásad a principů pro hodnocení lidí a jejich komunikaci,
- zajistit soulad firemních a osobních zájmů pracovníků a pracovníkům poskytnout co nejvíce informací, aby se mohli chovat racionálně, v souladu se zájmy firmy i v souladu se svými,
- vytvářet efektivní informační infrastrukturu s cílem získat nebo předat informaci jednoduchým způsobem,
- řídit se důležitou zásadou, že sběr informací nesmí pracovníky zbytečně zatěžovat,
- zabezpečit, aby každé funkční místo mělo dostatek informací pro to, aby pracovník pověřený danou prací mohl pracovat samostatně a zodpovědně do té míry, do jaké je dané funkční místo definováno.

Víme, že v nové ekonomice je potřeba spolupracovat nejen uvnitř armády, ale i s externími subjekty. Proto doporučuji přehodnotit i přístup k informacím a jejich utajení. V praxi se setkáváme se skutečností, že zaměstnanci AČR nemají přístup k informacím takového rozsahu, jak jsou zveřejňovány na internetových stránkách. [58]

Výlučné postavení nejen v rámci AČR, ale i odborné komunity ČR získává ve vědecko-výzkumné činnosti Univerzita obrany - katedra ekonomie, která se podílí na rozvoji vědního oboru Ekonomika obrany státu a Ekonomika ozbrojených sil. Pracovníci katedry jsou zapojeni do řešení mezinárodních projektů majících vztah k ekonomickému zabezpečení obrany (*Polsko, Maďarsko, Slovensko, Německo a další*) a dále řešili výzkumné projekty pro Ministerstvo zahraničních věcí ČR (dále jen MZV ČR), Ministerstvo financí ČR (dále jen MF ČR) a Ministerstvo průmyslu

a obchodu ČR (dále jen MPO ČR). Pro své studenty zabezpečuje přístup k informacím cestou vlastní sítě LAN a sítě internetu.

4.1 Moderní telekomunikační technologie zefektivňující činnost veřejné správy

Současný svět se mění obrovskou rychlostí a právě informační a telekomunikační technologie (dále jen ICT), které představují rychle se rozvíjející oblast, dokáží jeho vývoj usnadnit a zachytit. Mluvíme-li o ICT, mluvíme o technologiích a lidech, technologiích a zdraví, o tom, jak jsou ICT využívány v těchto oblastech a jak by v nich měly sloužit.

Jedním ze základních cílů používání ICT veřejnou správou, je poskytování rychlejších, profesionálnějších a méně komplikovaných služeb nejširší veřejnosti. Jedná se o dlouhodobý a náročný proces, který je potřeba statisticky zachytit. ČSÚ sleduje od roku 2003 rozvoj a využívání ICT ve veřejné správě. Jako hlavní zdroj informací slouží „**Šetření o využívání ICT veřejnou správou**[14]“, který obsahuje projekty:

1. „***Průzkum webových stránek veřejné správy***“, který je jednou za rok pravidelně realizován v klíčových oblastech:

- sektor veřejné správy, kde je projekt součástí šetření využívání ICT ve veřejné správě (e-Government),
- školství (e-Education),
- zdravotnictví (e-Health),
- kultura (e-Culture) a audiovizuální sektor.

Periodicita průzkumu umožňuje flexibilně zachytit trendy ve využívání ICT se zaměřením na rozšíření a používání vybraných informačních a komunikačních technologií (počítač, internet, poskytování informací a služeb, nákup přes internet, bezpečnostní opatření atd.). Zpřístupnění informací a on-line služeb na webových

[14] http://www.csu.statnisprava.cz/csu/

stránkách veřejné správy hraje jednu z klíčových rolí ve sbližování veřejné správy s veřejností. [59]

2. „***Šetření o využívání ICT v domácnostech a mezi jednotlivci***“, zdroj informací o využívání internetu ze strany občanů a firem včetně používání technologií ve vztahu k veřejné správě,
3. „***Šetření o využívání ICT v podnikatelském sektoru***“, zdroj informací o způsobu a míře využívání vybraných ICT a systémů mezi ekonomickými subjekty podnikatelského sektoru a jejich zaměstnanci v ČR. Dále dává informace o uskutečněných nákupech a prodejích prostřednictvím sítí založených na internetových protokolech a ostatních počítačově propojených sítích a informace vztahující se k bezpečnosti informačních systémů. Pilotní projekt začal v roce 2002. V roce 2004 poprvé proběhlo dle nařízení Evropského parlamentu a Rady (ES), které sjednocuje definice a metodologii používanou u tohoto výběrového šetření pro celou Evropskou unii.

V souvislosti s vývojem ICT probíhá každoročně Mezinárodní veletrh ICT (dále jen CeBIT[15]), který je největší a nejvýznamnější specializovaný veletrh pro oblast ICT na světě. Jedná se o veletrh pokrývající všechny oblasti průmyslu ICT. Mezi největší evropské vystavovatele v roce 2006 patřila tradičně Velká Británie (189 firem), Holandsko (112 firem) a Itálie (84 firem). Největší vystavovatel ze zámoří byl Taiwan (711 firem), Čína (412 firem), Jižní Korea (229 firem) a Spojené státy (198 firem). V rámci oficiální účasti České republiky se veletrhu zúčastnilo celkem 43 českých firem (včetně expozice MPO a CzechInvestu) na celkové ploše 941 m2.

Z výše uvedeného jednoznačně vyplývá, že zdrojem technologického rozvoje moderních prostředků využitelných pro vojenské účely již není výhradně uzavřený sektor vojenského výzkumu, vývoje a výroby, nýbrž otevřená civilní komerční sféra. Využívání ICT ve vojenství znamená vývoj a budování KIS, propojení simulací a reality, a informatizaci válečného plánování i taktických operací.

[15] http://www.mpo.cz

4.2 Informatizace vojenství

V době globální informatizace světa i armády vytváří svoje informační báze a datové sklady a je velmi snadné nejen potencionálního konkurenta zneschopnit vyřazením výpočetní techniky, ale také vytěžit jeho datové sklady a získat tak zajímavé informace o konkurenci. Pro tento záměr zaměstnávají organizace různé šikovné hackery, crackery a počítačové bezpečnostní experty. Proto obzvláště ve vojenství platí důsledně zásada bezpečnosti a ochrany informací, která v některých případech přerůstá do paranoidní ochrany dat před samotnými zaměstnanci organizace. Informace jsou nakonec přístupné pouze úzké elitě TOP managementu a nejsou pro jejich práci příliš efektivně využitelné. Tak vznikají pouze data pro data.

V AČR je informatizace zaměřena na podporou rozvoje nástrojů pro simulaci reálných systémů s ohledem na bezpečnost jejich provozu v praxi (např. jaderné elektrárny, dopravní systémy, simulace bezpečnostní situace a vojenských akcí). Garantem koncepce informatizace a aplikace státní informační politiky v AČR je Sekce komunikačních a informačních systémů Ministerstva obrany (dále jen SKIS MO), která odpovídá za rozvoj, koordinaci výstavby, provozu a efektivního využívání KIS. Technickým a odborným garantem v oborech komunikačních, informačních a bezpečnostních systémů a technologií zaváděných do rezortu obrany je Agentura rozvoje informatiky (dále jen ARI), která zajišťuje zpracování zadávací dokumentace projektů, podporu projektového řízení výstavby a podporu řešení výzkumných a vývojových projektů v oblasti KIS. [58]

V resortu v současné době existuje cca 11 IS a několik dalších aplikací. U systémů velení byly prioritně zavedeny a certifikovány nejmodernější technologie k jednotkám brigádního úkolového uskupení. Se zahraničními misemi je komunikace realizována několika typy satelitního spojení, mobilními službami a pevným připojením, které umožňuje telefonické spojení vojáků s rodinnými příslušníky.

V roce 2007 je informatizace zaměřena na zvýšení bezpečnosti a spolehlivosti přenosu dat. Bude pokračovat informatizace a modernizace stávajících zařízení u jednotlivých útvarů a zařízení AČR a do zahraničních misí budou zaváděny komunikační informační moduly. Informatizace má za cíl ochranu zdrojů informací a

komunikační infrastruktury před událostmi, které by učinily informace nedostupné v požadovaném čase a celkové zefektivnění vojenských činností.

4.3 Efektivnost vojenských činností

Pojem vojenské činnosti chápeme jako komplex všech činností souvisejících se zajištěním bezpečnosti prostřednictvím vojenských sil, tzn. souhrnný termín, který zahrnuje všechny otázky vojenské teorie a praxe spojené s přípravou a činností ozbrojených sil v době míru a války, a také s přípravou společnosti na možné vojenské i nevojenské ohrožení. Potom můžeme říci, že vojenství je tvořeno komplexem aktivit zahrnujícím všechny oblasti nezbytné pro fungování státu. [58]

Po přijetí ČR do aliance NATO bylo nutno sjednotit chápání a přístupy k realizaci většiny vojenských činností v AČR s jejich pojetím v této organizaci. Dnes je většina rizik pro bezpečnost státu nevojenské povahy, které plynou z ekonomických problémů, etnické nevraživosti či nezajištěných a neúčinných hranic, které umožňují ilegální migraci a pašování. Dále souvisí s organizovaným zločinem a korupcí, jež mají mezinárodní dimenzi a narušují zdravý rozvoj demokracie a tržní ekonomiky. Většina z výše uvedených hrozeb nevyžadují tradiční vojenskou reakci, ale investice do ministerstev vnitra, obrany a institucí krizového řízení. S růstem investic do vnitřní bezpečnosti pak musí růst příspěvek k mezinárodním bezpečnostním operacím a proto je nutné začít měřit náklady na jednotlivé činnosti dle stanovených standardů pro čerpání finančních prostředků. Prostor pro úspory z jednotlivých činností je velmi omezený, protože profesionální armády jsou finančně nákladné. V současné době je celá řada problémů, které mají vliv na efektivitu vojenských činností, mezi které patří zejména ekonomika armády, která není teoreticky rozpracována.

Uvedenými problémy se zabývají dnes všechny země. Je zřejmé, že cesta vpřed vyžaduje zvýšenou transparentnost v obranném plánování a společný přístup. Státy musí přijímat obtížná rozhodnutí a zvažovat otázky, které až dosud byly tabu (dělba vojenských úkolů). Vojenské činnosti musí odpovídat potřebám dnešního světa a musí:

- umožnit překonat instrumentální vztah veřejnosti k vojenství a k vojenské činnosti a převzít odpovědnost za prevenci a eliminaci bezpečnostních hrozeb, rizik a krizových situací,
- znovu zvážit zavedení branné výchovy ve vzdělávacím procesu a nově přistoupit k pojetí civilní ochrany,
- rozvíjet dále v celé řadě vojenských činností využívání digitální geografické informace, které slouží nejen jako lokalizační podklad vojensko odborné nadstavby nebo jako základ pro tvorbu topografických a tematických map, ale samozřejmě i jako podklad pro různé typy analýz terénu, pro studium vzájemných vztahů objektů a jevů modelovaných v databázích, pro plánování a vyhodnocování územně orientovaných činností apod.

Každý dnes ví, že charakter hospodářského prostředí a celé společnosti se mění a přestává platit to, co platilo dosud. Přestávají fungovat univerzální a obecné pravdy a jednoduchá řešení. Každý se musí mnohem pečlivěji než dříve věnovat tomu, kde je jeho místo a jaké má skutečné možnosti či problémy. Nestačí opisovat a bezmyšlenkovitě přebírat dříve úspěšné postupy, ale každý se musí snažit doopravdy, důkladně a přesně poznat vlastní firmu, její skutečné zájmy a vytvářet optimální podmínky pro skutečně efektivní fungování organizace.

5. ZÁVĚR

Cílem mé práce bylo analyzovat současný stav informačních systémů v oblasti vojenství. Na základě shromážděných, dostupných, utříděných a zpracovaných materiálů, vlastních zkušeností, úvah a názorů navrhnout obecná doporučení pro optimalizaci využívání informací ve vojenském výzkumu, vojenském školství a vojenské praxi.

Ve své práci jsem se snažila poukázat na současný stav a perspektivní zlepšení řízení procesu výstavby armády, možnosti, způsoby a postupy při zabezpečování veřejné správy a armády informačními technologiemi. Moji snahou bylo vysvětlit význam informací a znalostí v integrované společnosti a postup e-Governmentu v ČR. Dále jsem poukázala na možná bezpečnostní rizika při poskytování informací v rámci veřejných informačních zdrojů a současně využívání veřejných informačních zdrojů. Práce může být určitým podnětem k zamyšlení odpovědných týmů při dalším postupu profesionalizaci armády ČR, zavádění informačních technologií a při tvorbě nových vnitřních předpisů a norem v celkové organizaci bezpečnosti informací. Zlepšení vidím jak po stránce vybudování účinné organizační struktury, která bude mít dlouhodobější platnost, tak po stránce odborného personálního zabezpečení a zabezpečení finančních prostředků.

Využívání informací formou veřejně přístupných informačních zdrojů není samoúčelný systém, ale prolíná se v každodenní práci velitelů a náčelníků. Při shromažďování podkladů k této práci jsem zjistila, že jen málokterý pracovník resortu obrany dokáže plně a efektivně využívat informace z veřejných informačních zdrojů. V dnešní době je nanejvýš nutné, aby vojenský profesionál na všech stupních velení měl kromě odborných znalostí i odpovídající znalosti v oblasti získávání informací poskytovanými veřejnými informačními zdroji a dovedl je využívat ve své každodenní práci, v práci s podřízenými, nebo při jednáních se státními a soukromými organizacemi. Je potřeba, aby každý pochopil, jakou váhu a cenu má ta či ona informace a rozhodl se, jak tyto informace zabezpečit v souladu s platnými právními normami. Proto navrhuji, aby se do všech škol a zejména vojenských zařazovala výuka získávání informací z veřejně přístupných informačních zdrojů.

K zefektivnění činnosti vojenských profesionálů by bylo vhodné, aby teorie získávání informací byla úzce spjatá s praxí formou účasti při testování informačních a komunikačních systémů a odhalování jejich vnitřních a vnějších hrozeb.

Za přínosy diplomové práce považuji:

- využití jako studijního materiálu pro všechny studia specializace bezpečnosti informací,
- návrhy a doporučení vycházejí z reálných zkušeností,
- logické, systémové a věcné uspořádání jednotlivých kapitol.

Srovnávací analýza některých veřejně přístupných informačních zdrojů dává ucelený přehled informačních zdrojů v oblasti vojenství. Je možno konstatovat, že při výstavbě vlastních i veřejných informačních zdrojů je nutné postupovat v souladu s platnými právními normami a definovat požadavky jak na aplikace, tak i na celý systém z hlediska bezpečnosti.

SEZNAM POUŽITÉ LITERATURY A ZDROJŮ

1. RAUCH, J. *Metody zpracování informací I – informační zdroje a služby*. Praha: Vysoká škola ekonomická, Fakulta informatiky a statistiky. 1994. 55 s. ISBN 80-7079-353-8.

2. PAPIK, R. Báze dat pro oblast vojenství. (původní). *In Infocus*. 1996, roč. 2., č. 10., s. 74-76. ISSN 1211-0892.

3. BALÁŽ, J. Databáze Vojenského ústředního archivu na internetu. *In Historie vojenství*. 2005, roč. 54, č. 4, s. 126-127. ISSN 0018-2583.

4. WANNER, Michal. *Nové standardy v českém archivnictví.* Hradec Králové: Informační systémy státní správy Visegrádská konference V4DIS. 2007.

5. PAPÍK, R. *Vyhledávání informací I.: umění či věda?* Národní knihovna: knihovnická revue 2001, č. 1 s. 18-25. Dostupný z WWW: <http://full.nkp.cz/nkkr/NKKR0101/0101018.html>.

6. KRČ, Miroslav. *Vojenství jako významný fenomén 21. století*. [online]. Dostupný z WWW: <http://www.army.cz/avis/vojenske_rozhledy/2002_1/35.htm>.

7. TRUNDA, Michal. *Datové sklady a jejich přínos v procesech velení a řízení.* UO Brno, katedra speciálních komunikačních systémů. 9. konference spojovacího vojska. 2004. 170 s.

8. Usnesení vlády ČR č. 679 ze dne 7. července 2004. *Koncepce rozvoje knihoven v ČR.* Praha, 2004.

9. HEJL, Pavel. *Systém integrované společnosti.* Hradec Králové: Informační systémy státní správy Visegrádská konference V4DIS. 2007.

10. POKORNÝ, Jan. *Informační společnost a e-Government*. Hradec Králové: Informační systémy státní správy Visegrádská konference V4DIS. 2007.

11. KYSELICA, Andrej. Využívání služeb e-Governmentu jednotlivci. Hradec Králové: Informační systémy státní správy Visegrádská konference V4DIS. 2007.

12. HANÁČEK, P., STAUDEK. *Bezpečnost informačních systémů*. Praha: Úřad pro státní informační systém. 2000. 128 s. ISBN 80-238-5400-3.

13. JONÁK, F. *Informační gramotnost, schopnost orientovat se ve světě informací, jak a kde ji získat.* 2007. [cit. 2007-03-06]. Dostupný z WWW: <http://daidalos.ff.cuni.cz>.

14. Česko. Zákon č. 499 ze dne 30. června 2004 o archivnictví a spisové službě a o změně některých zákonů. *In Sbírka zákonů České republiky*. 2004, částka 173.

15. Česko. MV. Vyhláška č. 645 ze dne 13. 12. 2004 kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů. *In sbírka zákonů České republiky*. 2004, částka 220.

16. Česko. MV. Vyhláška č. 646 ze dne 13. 12. 2004 o podrobnostech výkonu spisové služba. *In sbírka zákonů České republiky*. 2004, částka 220.

17. Česko. Zákon č. 257 ze dne 29. června 2001 o knihovnách a podmínkách provozování veřejných knihovnických a informačních služeb. *In Sbírka zákonů České republiky*. 2001, částka 98.

18. Česko. Zákon č. 365 ze dne 14. září 2000 o informačních systémech veřejné správy a o změně některých dalších zákonů. *In Sbírka zákonů České republiky*. 2000, částka 99.

19. Česko. Zákon č. 119 ze dne 24. dubna 2007 o ochraně utajovaných informací a o bezpečnostní způsobilosti. *In Sbírka zákonů České republiky*. 2007, částka 44.

20. Česko. NBÚ. Vyhláška č. 527 ze dne 14. 12. 2005 o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí. *In sbírka zákonů České republiky*. 2005, částka 179.

21. Česko. NBÚ. Vyhláška č. 526 ze dne 14. 12. 2005 o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele. *In sbírka zákonů České republiky*. 2005, částka 179.

22. Česko. NBÚ. Vyhláška č. 529 ze dne 15. 12. 2005 o administrativní bezpečnosti a o registrech utajovaných informací. *In sbírka zákonů České republiky*. 2005, částka 179.

23. Česko. NBÚ. Vyhláška č. 528 ze dne 14. 12. 2005 o fyzické bezpečnosti a certifikaci technických prostředků. *In sbírka zákonů České republiky*. 2005, částka 179.

24. Česko. NBÚ. Vyhláška č. 523 ze dne 5. 12. 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. *In sbírka zákonů České republiky*. 2005, částka 179.

25. Hanáček, P., Staudek, J. *Bezpečnost informačních systémů* [online]. Úřad pro státní informační systém. 2000. [cit. 2007-07-20]. Dostupný z WWW: <http://www.micr.cz/scripts/detail.php?id=479>.

26. Česko. NBÚ. Vyhláška č. 524 ze dne 14. 12. 2005 o zajištění kryptografické ochrany utajovaných informací. *In sbírka zákonů České republiky*. 2005, částka 179.

27. Česko. NBÚ. Vyhláška č. 525 ze dne 14. 12. 2005 o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací. *In sbírka zákonů České republiky*. 2005, částka 179.

28. Česko. Zákon č. 413 ze dne 21. září 2005 o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti. *In Sbírka zákonů České republiky*. 2005, částka 143.

29. Česko. Zákon č. 101 ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů. *In Sbírka zákonů České republiky*. 2000, částka 32.

30. Česko. Zákon č. 227 ze dne 29. června 2000 o elektronickém podpisu a o změně některých dalších zákonů. *In Sbírka zákonů České republiky*. 2000, částka 68.

31. Česko. Zákon č. 127 ze dne 22. února 2005 o elektronických komunikacích a o změně některých souvisejících zákonů. *In Sbírka zákonů České republiky*. 2005, částka 43.

32. Česko. Zákon č. 140 ze dne 29. listopadu 1961 trestní zákon. *In Sbírka zákonů České republiky*. 1961, částka 65.

33. Česko. Zákon č. 500 ze dne 24. června 2004 správní řád. *In Sbírka zákonů České republiky*. 2004, částka 174.

34. Česko. NBÚ. Vyhláška č. 522 ze dne 7. 12. 2005 kterým se stanoví seznamy utajovaných informací. *In sbírka zákonů České republiky*. 2005, částka 179.

35. Česko. Zákon č. 122 ze dne 7. dubna 2000 o ochraně sbírek muzejní povahy a o změně některých dalších zákonů. *In Sbírka zákonů České republiky*. 2000, částka 36.

36. Letecké muzeum Kbely. *Vojenský historický ústav* [online]. 2006. [cit. 2007-07-20]. Dostupný z WWW: <http://www.vhu.cz/cs/stranka/letecke-muzeum/>.

37. Armádní muzeum Žižkov. *Vojenský historický ústav* [online]. 2006. [cit. 2007-07-20]. Dostupný z WWW: < http://www.vhu.cz/cs/stranka/armadni-muzeum/>.

38. Knihovna. *Vojenský historický ústav* [online]. 2006. [cit. 2007-07-20]. Dostupný z WWW: < http://www.militarymuseum.cz/cz/cz/muzeum.php?id=6>.

39. Muzea. *Vojenský historický ústav* [online]. 2006. [cit. 2007-07-20]. Dostupný z WWW: <http://www.militarymuseum.cz/cz/cz/muzea.php>.

40. Časopis historie a vojenství. *Vojenský historický ústav* [online]. 2006. [cit. 2007-07-20]. Dostupný z WWW: <http://www.militarymuseum.cz/cz/cz/hav.php>.

41. *Produkty a služby* [online]. Albertina icome Praha. 2006. [cit. 2007-07-20]. Dostupný z WWW: < http://www.aip.cz/produkty.php>.

42. *DefenceNews* [online]. 2006. [cit. 2007-05-07]. Dostupný z WWW: <http://www.defensenews.com/>.

43. *Middle East Nesline* [online]. 2007. [cit. 2007-05-07]. Dostupný z WWW: <http://www.defensenews.com/>.

44. *Interfax-agenstvo vojennych novostej*[online]. 2007. [cit. 2007-05-07]. Dostupný z WWW: <http://www.militarynews.ru/>.

45. *Debkafile* [online]. 2007. [cit. 2007-05-07]. Dostupný z WWW: <http://www.debka.com/>.

46. *United Press International* [online]. 2007. [cit. 2007-05-07]. Dostupný z WWW: <http://argus.upi.com/login.php>.

47. *Intelligence Online* [online]. 2007. [cit. 2007-05-07]. Dostupný z WWW: <http://argus.upi.com/login.php>.

48. *Jane´s* [online]. 2007. [cit. 2007-05-07]. Dostupný z WWW: <http://www.janes.com/ >.

49. Česko. Zákon č. 111 ze dne 14. března 2006 o pomoci v hmotné nouzi. *In Sbírka zákonů České republiky*. 2006, částka 37.

50. Česko. Zákon č. 108 ze dne 14. března 2006 o sociálních službách. *In Sbírka zákonů České republiky*. 2006, částka 37.

51. *Český statistický ústav* [online]. 2007. [cit. 2007-07-20]. Dostupný z WWW:<http://www.czso.cz/csu/redakce.nsf/i/domacnosti_a_jednotlivci>.

52. *Český statistický ústav* [online]. 2007. [cit. 2007-07-20]. Dostupný z WWW: <http://www.czso.cz/csu/redakce.nsf/i/verejna_sprava>.

53. *Český statistický ústav* [online]. 2007. [cit. 2007-07-20]. Dostupný z WWW: <http://www.czso.cz/csu/redakce.nsf/i/ict_ve_skolstvi_e_education>.

54. *Univerzita obrany* [online]. 2007. [cit. 2007-07-20]. Dostupný z WWW: <http://www.unob.cz/struktura_uss.aspx?id=468>.

55. Česko. Zákon České národní rady č. 2 ze dne 8. ledna 1969 o zřízení ministerstev a jiných ústředních orgánů státní správy ČSR. *In Sbírka zákonů České republiky*. 1969, částka 1.

56. Česko. Zákon č. 148 ze dne 11. června 1998 o ochraně utajovaných skutečností a o změně některých zákonů. *In Sbírka zákonů České republiky*. 1998, částka 52.

57. Česko. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In *Sbírka zákonů České republiky*. 2005, částka 143.

58. *Ministerstvo obrany české republiky* [online]. 2004. [cit. 2007-07-20]. Dostupný z WWW: <http://www.army.cz>.

59. *Český statistický úřad* [online]. 2007. [cit. 2007-07-20]. Dostupný z WWW: <http://czso.cz>.

60. *Ministerstvo průmyslu a obchodu* [online]. 2005. [cit. 2007-07-20]. Dostupný z WWW: <http://www.mpo.cz/>.

61. Vojenský historický archiv [online]. 2006. [cit. 2007-07-20]. Dostupný z WWW: http://www.vhu.cz.

62. BUCHAROVÁ, Lenka. *Informační zdroje v oblasti bezpečnosti státu*. Praha, 2006, 102 s. Diplomová práce na Filozofické fakultě Univerzity Karlovy na Ústavu informačních studií a knihovnictví . Vedoucí diplomové práce Richard Papík.

63. CEJPEK, Jiří. *Informace, komunikace a myšlení : úvod do informační vědy*. Praha : Nakladatelství Karolinum, 2005. 233 s. ISBN 80-246-1037-X.

EVIDENCE VÝPŮJČEK

Prohlášení:

Dávám svolení k půjčování této diplomové práce. Uživatel potvrzuje svým podpisem, že bude tuto práci řádně citovat v seznamu použité literatury.

V Praze dne 17. 8. 2007.

Václava HAMMEROVÁ

Jméno	Katedra / Pracoviště	Datum	Podpis