

Bezpečnostní a ekologické aspekty ve státní informační politice

Historicky bezprecedentní rozvoj **informačních a komunikačních technologií (ICT)** od počátku 90. let, jak známo, iniciuje a akceleruje zcela nové fenomény v životě a vývoji na všech úrovních lidské společnosti, od občana a rodiny, přes obce, regiony, podnikatelské subjekty a profesní komunity až po státní instituce a systémy, národy, státy a mezinárodní společenství. Stále více se běžnou praxí stává používání pojmů „informatizace“, „informační dálnice“, „informační společnost“, „komunikační a informační infrastruktura“, „informační politika“ a „informační revoluce“, ale, bohužel, také „informační kolaps“, „informační válka“, „informační terorismus a pirátství“.

V geograficky a populačně malých zemích, i při realitě současných integračních (doufám, že nikoliv kolektivizačních) procesů, má kvalitativní posun ve využívání komunikací a informací, a to prostřednictvím jak automatizovaných, tak neautomatizovaných technologií, zvláštní význam. Pokud je zajištěno, aby, zejména v oblasti výstavby informačních systémů, nebyl programově budovaným a udržovaným tunelem na státní nebo obecní prostředky, je tento proces relativně levnou cestou k vytvoření předpokladů pro zvýšení úrovně vzdělání a jeho uplatnění, pro efektivní produkci a využívání zdrojů, racionální fungování státních i samosprávných mechanismů, transparentní legislativu a právní prostředí, i pro redukci potenciálních i reálných bezpečnostních rizik a jiných jevů, neproduktivně mařících zdroje. To umožňuje minimalizovat individuální i společenské ztráty a kompenzovat fyzickou, geografickou, populační a ekonomickou malost vysokou kvalitou řízení, politiky, ekonomiky, kultury, bezpečnosti a obrany. Záleží ovšem na konkrétním využití této možnosti, úrovni, odpovědnosti a vztazích realizujících subjektů.

Přitom nelze, jak se občas stává, roli informací přeceňovat a uplatňovat extrémní názor, že informatizace je jedinou spasitelnou, resp. zcela dominantní silou, která zajistí úspěšný život a vývoj. I v informační společnosti bude podmínkou života a vývoje materiální výroba a fungování infrastruktur, využívání přírody a přírodních zdrojů, i v informační společnosti budou vedle ICT lidé a rodiny, se svými problémy, zájmy a vztahy, konflikty, názory, city a pocity, ekonomické subjekty se svou produkcí, konkurencí, zdroji a zisky, státní systémy se svou politickou strukturou a orientací, legislativou a úředníky. I v informační společnosti budou národy se svým stylem života, historií a stupnicí hodnot. Jde však o to, jaké tyto vztahy, problémy a hodnoty budou a jaký prostor uvedené subjekty vytvoří pro jak pozitivní, tak negativní, deformující a hodnoty devastující jevy a procesy. Lze doufat a snad i předpokládat, že informatická vzdělanost a kultivace, od občanů až po národy, státy a mezinárodní organizace a uskupení, přispěje k tomu, že informatizace společnosti bude koncipována a realizována kulturně a odpovědně, s vnitřní eliminací a redukcí rizik a úskalí, ve prospěch skutečného zkvalitnění a perspektivnosti života.

V České republice je v současnosti uvedeným otázkám věnována značná pozornost. Bylo ustaveno a reálně pracuje **Sdružení pro informační společnost (SPIS)**, probíhají přípravné práce k zřízení *Českého fóra pro informační společnost* jako platformy pro komplexní posuzování systémových, technologických, politických, ekonomických, sociálních, kulturních, bezpečnostních, etických a dalších aspektů výstavby informační společnosti a pro vytváření správné orientace aktivit jak občanských, profesních, akademických, mediálních a podnikatelských komunit, tak státních a samosprávných orgánů a institucí při výstavbě informační společnosti. Jsou reflektovány i vnější aspekty informatizace, a to zejména kontakty s **Fórem pro informační společnost** (Information Society Forum), ustaveným a pracujícím v rámci orgánů EU (připomínám významný dokument Evropské unie, akční plán Evropské komise „Cesta Evropy k informační společnosti“ z roku 1994), a rovněž spoluprací s orgány OECD, WTO a OSN. V **oblasti obrany** má význam uplatnění interoperability a jí odpovídající standardizace informačních procesů, výstavby a funkce systémů C3 (konzultace, řízení a velení), jak na úrovni vojenských, tak politických a odborných struktur NATO a ZEU.

Význam, který vláda ČR přikládá výstavbě informační společnosti, se promítl v ustavení **Rady vlády ČR pro státní informační politiku**, řízené místopředsedou vlády, s účastí rezortů na úrovni náměstků ministrů. Odborné otázky jsou projednávány v odborné pracovní skupině (OPS), v jejímž čele je předseda **Úřadu pro státní informační systém (ÚSIS)**. Členy OPS jsou vedoucí pracovníci odborných složek rezortů a státních institucí (sekcí nebo odborů) a rovněž primátoři měst Plzně a Ostravy a zástupci Svazu měst a obcí. V obou uvedených institucích je zastoupen a aktivně se zúčastňuje prací rezort obrany: v Radě vlády ČR NMO-E, v OPS vedoucí bývalého oddělení rozvoje systémů velení a řízení sekce obranné politiky (SOP MO), bez náhrady a, podle mého názoru, bez racionálního důvodu zrušeného při reorganizaci SOP MO k 31. 3. 1999. Tuto smutnou realitu a nepochopení významu adekvátní organizační složky řízení informatizace na rezortní úrovni, mimo jiné z důvodu odpovídajících vztahů vůči subjektům na státní úrovni, ponechávám bez komentáře.

Významnou aktivitou, iniciovanou vládou ČR, řízenou Radou vlády ČR pro státní informační politiku a realizovanou ÚSIS s participací rezortů a institucí státní správy a samosprávy je zpracování dokumentu „**STÁTNÍ INFORMAČNÍ POLITIKA – CESTA K INFORMAČNÍ SPOLEČNOSTI**“ (dále **SIP**)/1/. Tento závažný dokument byl schválen vládou České republiky, včetně oficiálního uznání jeho strategického charakteru, a jeho realizace bude obsahem připravovaného akčního plánu. Česká republika jako stát tedy proces své informatizace na politické, koncepční bázi realizovat bude.

A co rezort obrany? Považuji za účelné, v kontextu snad ještě ne zcela umrtveného procesu koncipování informatizace rezortu obrany, podat stručnou informaci o obsahu dokumentu SIP, zmínit některé momenty procesu jeho geneze a uvést náměty na realizaci v oblasti bezpečnostní (krizový management, vnitřní bezpečnost, obrana) a ekologické.

Charakteristika dokumentu:

„STÁTNÍ INFORMAČNÍ POLITIKA – CESTA K INFORMAČNÍ SPOLEČNOSTI“

V preambuli úvodní části se zdůrazňuje, že rozvoj informační společnosti není jen úlohou vlády a státních orgánů, a proto vláda předkládá dokument široké veřejnosti,

včetně podnikatelské, profesionální a akademické obce. Dále je charakterizována informační společnost – z hlediska ICT, z hlediska přínosů pro výrobu, podnikání, finančníctví, vzdělání, transfer znalostí a výzkum, veřejnou správu a občany a rovněž z hlediska úskalí a rizik. Část, týkající se negativních aspektů, by si zasloužila větší prostor, protože již současné rané stadium informační společnosti indikuje závažná úskalí a rizika, a to nejen technologická (na př. počítačové viry, problém roku 2000, informační kriminalita), vzdělávací a sociální (nároky na kvalifikaci, zaměstnanost), ale i psychologická a etická.

V další části dokumentu jsou uvedeny aspekty integrace do evropských a světových struktur a související šance pro Českou republiku. V této části aktuální verze považuji za částečně podceněnou otázku standardizace a efektivnosti instalace a uplatnění ICT, včetně využívání zahraničních investic, a to zejména ve výstavbě a provozování **informačních systémů veřejné správy (ISVS)**. Nemohu popřít, že k této poznámce mne vedou zkušenosti z rezortu obrany (některé z nich jsem prezentoval v /2/). Tento dílčí nedostatek hlavní části dokumentu je však kompenzován v přílohové části.

Dále jsou uvedeny základní cíle a přínosy SIP: jednak z hlediska občana, jednak z hlediska řízení státní správy a samosprávy, z hlediska podpory rozvoje podnikání. Cíl státní informační politiky je prezentován jako „**vybudování a rozvíjení informační společnosti, a tím vytvoření předpokladů zejména pro zlepšení kvality života jednotlivých občanů, zefektivnění státní správy a samosprávy a zkvalitnění podpory rozvoje podnikání**“. Jakkoliv je v cíli SIP i v dalším textu této části prezentován aspekt „zlepšení kvality života“, není ani heslovitou formou na tomto místě zohledněn fakt, že ke kvalitě života patří i bezpečnostní a ekologické aspekty. O této otázce se zmíním podrobněji.

V průběhu geneze dokumentu, zejména v rámci připomínkových řízení, bylo nezahrnutí bezpečnostní a ekologické problematiky opakovaně zřetelně indikováno, avšak, což je pozoruhodné, pouze pracovníky MO ČR, nikoliv pracovníky rezortů, kterých se bezpečnostní a ekologická problematika rovněž, a snad ještě výrazněji, týká. Rezort MO však ve svém názoru zcela osamocen nebyl, jak dokumentuje vystoupení primátora města Ostravy na konferenci, pořádané SPIS v květnu 1999 /3/.

Pracovníci MO ČR, zpracovávající připomínky k předchozím verzím, vycházeli z komplexního pojetí informační společnosti, v níž se informační, komunikační a mediální technologie přiměřeně uplatní ve všech oblastech společnosti, v kvalitě celkového vývoje i každodenního života, na úrovni občana, obce, regionu, podniku a instituce, státní a veřejné správy i na mezinárodní úrovni, a to ve standardních i nestandardních stavech. Ve svých stanoviscích prezentovali názor, že zajištění trvale udržitelného rozvoje, hospodárné využívání a ochrana životního prostředí, racionální a efektivní chování v mimořádných a krizových situacích, zajištění stability, bezpečnosti a obrany mezi výrazné aspekty kvality reálného života a vývoje neodmyslitelně patří. Informatizace společnosti a realizace státní informační politiky by se proto měla uplatnit ve všech těchto aspektech a není žádný rozumný důvod je opomíjet. Navíc bezpečnostní a ekologické aspekty mají vztah i k uplatnění přínosů informační společnosti a realizace státní informační politiky v oblasti ekonomické, komerční, komunikační, administrativní, vědecké, vzdělávací a dalších, které v dokumentu adekvátní místo již měly, a to ve formě samostatných odstavců (oblastí). Prosazení tohoto přístupu nebylo snadné. Teprve ve stadiu vládního projednání byl zpracovatel

požadavek komplexního pojetí a odpovídajícího rozšíření dokumentu akceptován a realizován zapracováním převážné části textu, který dodalo MO ČR, v odstavci „Osm prioritních oblastí státní informační politiky“. Z důvodu stručnosti uvedu pouze strukturu tohoto odstavce:

- I. Informační gramotnost
- II. Informatizovaná demokracie
- III. Rozvoj informačních systémů veřejné správy
- IV. Komunikační infrastruktura
- V. Důvěryhodnost a bezpečnost informačních systémů a ochrany osobních dat
- VI. Elektronický obchod
- VII. Transparentní ekonomické prostředí
 - 1. *Vytvoření transparentního podnikatelského prostředí pro podporu podnikání*
 - 2. *Hospodaření s veřejnými finančními fondy pod kontrolou veřejnosti*
- VIII. Informační společnost: stabilní a bezpečná

Krátce se zmíním o obsahu textu SIP v oblasti VIII., týkající se bezpečnostní a ekologické problematiky. Především se uvádí, že „nutnou podmínkou realizace v předchozích bodech prezentovaných oblastí státní informační politiky je zajištění stabilní existence a vývoje jejich subjektů, objektů i zdrojů, včetně prvků a subsystémů samotné informační a komunikační infrastruktury. Splnění této podmínky není automatické, výstavba informační společnosti však k němu může výrazně přispět“. Zdůrazňuje se, že „koncepte a realizace státní informační politiky se proto musí zaměřit i na oblast krizového managementu a životního prostředí, zajištění bezpečnosti a obrany i na širší kontext výstavby informační společnosti“.

Tím je prezentován požadavek dát krizovým, ekologickým, bezpečnostním a obranným aspektům místo a význam, adekvátní aspektům ekonomickým, administrativním a právním, finančním, vzdělávacím a zábavním.

Stručně řečeno: za určité situace bude pro občana, obec, region, podnik, instituci i státní nebo samosprávný orgán minimálně stejně důležitá kvalitní (věrohodná, včasná, dostupná a využitelná) **informace o krizové situaci** (v nejširším pojetí od dopravního kolapsu, živelní pohromy, průmyslové havárie nebo epidemie, přes násilné projevy terorismu a nezvládnutelnou migraci až po válku), o možnostech prevence, racionální reakce a přípravy na ni, jako, samozřejmě rovněž významné, podnikatelské, komerční nebo vzdělávací informace, získané v internetové kavárně nebo kiosku.

Širším kontextem výstavby stabilní a bezpečné informační společnosti je míněno zejména zaměření na „eliminaci přežívajících anachronismů ve vztahu k bezpečnostním rizikům, přírodním zdrojům a životnímu prostředí z hlediska trvale udržitelného rozvoje, stability a kvalitního harmonického života současné i příštích generací“.

Dále je charakterizována základní rámcová orientace státní informační politiky v oblasti VIII. se zaměřením na:

- informační podporu krizového managementu,
- informační podpora ochrany životního prostředí,
- informace a komunikace k zajištění vnitřní bezpečnosti,
- informace a komunikace k přípravě a zajištění obrany.

V závěru hlavní části jsou uvedeny „principy a základy“ postupu realizace státní informační politiky, opět v dosti redukované podobě, bez zohlednění alespoň středně-

dobého časového horizontu, pozice neautomatizovaných informačních procesů, obecně, nikoliv pouze s automatizovanými ICT spojené, informatické vzdělanosti a základní charakteristiky ekonomických (zdrojových, nákladových) aspektů SIP.

V přílohou části dokumentu, podle mého názoru velmi kvalitní a hodnotné, jsou podrobně rozpracovány obecné, národní i mezinárodní, aspekty, předpoklady a harmonogram realizace úkolů SIP. Kupodivu, některé aspekty, jejichž absenci v hlavní části jsem vzpomenul, v příloze uvedeny jsou, ovšem bez odkazu v hlavní části (standardizace, financování). I bezpečnostním a ekologickým aspektům je v příloze určita pozornost, i když na relativně malém prostoru, věnována.

Možnosti konkrétního zaměření státní informační politiky a výstavby informační společnosti ve vztahu ke krizovému managementu, využívání a ochraně životního prostředí, vnitřní bezpečnosti a obraně

Uplatnění informatizace v bezpečnostní a ekologické oblasti není v naší zemi, stavbou na zelené louce, protože v řadě dílčích aktivit se moderní informační a mediální technologie již uplatňují. V dalším vývoji jde o to, na bázi státní informační politiky, dát procesu uplatnění ICT i neautomatizovaných informačních procesů **vnitřní logiku**, systémovost, standardy, řád a efektivnost, jak v informacích a jejich využití, tak v organizaci a vztazích. Klíčovým úkolem je indikace reálných informačních potřeb a jim odpovídajícího obsahu, struktury a způsobu zpracování informací. V tomto odstavci se pokusím o formulaci základních informačních oblastí s vědomím, že musí být doplněny a detailně specifikovány na potřebné úrovni specialistů v jednotlivých oborech.

► **Krizový management**

Ze základních funkcí státu i ze zákona vyplývá právo občanů a povinnost státních, veřejných a samosprávných orgánů a institucí zajistit, získat, resp. předat a umožnit využití informací, týkajících se mimořádných a krizových situací a opatření k jejich zvládnutí, redukci a odstranění následků. Stejně tak vyplývá, na legislativní bázi a se zajištěním potřebné ochrany a bezpečnosti, povinnost občanů a podniků potřebné informace podat, právo státních, veřejných a samosprávných orgánů je vyžádat, zpracovat a využít. Klíčový, a někdy životní, význam má aktuálnost a rychlost získání, předání a zpracování a reálná využitelnost informací. Možná strukturalizace informačního pole je následující:

1. **Systémové informace o krizové legislativě** (včetně kompetencí a odpovědností orgánů veřejné správy a mezinárodních vztahů).
2. **Základní, obecné předběžné informace** pro všeobecnou racionální krizovou přípravu, zaměřené na:
 - prevenci a eliminaci zdrojů a podmínek mimořádných a krizových situací, tj. např. zákony a normativy z oblasti požární, dopravní, bezpečnostní, ekologické, zdravotní, stavební, energetické (včetně jaderné bezpečnosti), průmyslové (výroba, skladování, doprava a likvidace nebezpečných látek atd.), zemědělské a dalších,
 - přípravu a výchovu k racionálnímu chování a jednání občanů, rodin, obcí, podniků a institucí v mimořádných a krizových situacích a k odstraňování jejich následků, tj. zákony, normativy a pravidla v oblasti organizační, komunikační, dopravní, technické, zdravotní, hygienicko-epidemiologické, bezpečnostní atd.,

- přípravu k řídicím činnostem státních, veřejných a samosprávných orgánů v mimořádných a krizových situacích a při odstraňování jejich následků, tj. např. zákony, krizové plány a normativy činnosti řídicích orgánů v oblasti organizační, komunikační, dopravní, technické, zdravotní, sladění činnosti prvků integrovaného záchranného systému (IZS), atd.
- 3. **Databáze informací o potenciálních a reálných zdrojích bezpečnostních rizik a eskalace krizových situací, včetně výstupů monitorovacích sítí.**
- 4. **Konkrétní předběžné informace pro racionální krizovou přípravu v dané lokalitě, resp. objektu, v členění analogickém jako v bodu 1 (tj. požární, komunikační, dopravní, bezpečnostní, ekologické, zdravotní, hygienické, stavební, energetické, výrobní a provozní směrnice a pokyny, konkrétní varovné signály, informace o umístění a stavu technické infrastruktury, informace o technických uzlech, úkrytech, shromaždištích, evakuačních prostředcích, skladech ochranných prostředků, zásobách, atd.).**
- 5. **Evidence disponibilních sil a prostředků na úrovni obce, regionu, státu i mezinárodních organizací k využití při plánování a konkrétním nasazení v krizových situacích.**
- 6. **Konkrétní aktuální informace pro racionální krizové chování, jednání a řízení v konkrétní mimořádné nebo krizové situaci (informace o konkrétních parametrech a prognóze vývoje mimořádné nebo krizové situace, informační podklady pro činnost mezirezortního krizového štábu, krizové štáby ústředních správních úřadů, regionální krizové štáby, informace pro alianční a mezinárodní krizové instituce komunikační zajištění a centralizované zpracování tísňového volání, vyznění osob, varovné, vyznívací a poplachové signály a informace, požární, emisní, radiační a povodňová signalizace, informace o průběhu a následcích přírodních katastrof a průmyslových havárií, informace o hygienické a epidemiologické situaci, evidence osob, zvířat a majetku v zasaženém prostoru, informace a pokyny pro místní, regionální, státní a mezistátní koordinaci krizových opatření, konkrétní preventivní, reakční a následnou činnost při redukci následků, ukrytí, použití ochranných prostředků, informace o reálných možnostech a nasazení složek integrovaného záchranného systému, reálných možnostech a nasazení složek armády a policie, nasazení dalších záchranných složek a prostředků, o evakuaci, nouzovém ubytování, zajištění energie, potravin a pitné vody, lékařské péče, řízení činnosti v zasaženém prostoru, atd.).**

➤ **Ochrana a využívání životního prostředí**

Podstatným znakem moderní informační společnosti bude strategická orientace na trvale udržitelný rozvoj, odpovědné šetrné využívání přírodních zdrojů, a to jak energetických a surovinových, tak ovzduší, terénu, vodních toků a zdrojů, přírodní flóry a fauny. K tomu by měla být směřována komplexní informační báze o životním prostředí, legislativním, organizačním a technologickém zajištění prevence i represe k ochraně životního prostředí a hospodárnému využívání přírodních zdrojů. Součástí aktivit k dosažení těchto atributů bude, vedle výchovy a praktických opatření k obecně ekologickému chování a hygieně, potřebné informační zajištění a schopnost práce s ekologickými informacemi. Jedná se o tyto hlavní informační oblasti:

1. **Systémové informace o legislativě z oblasti ochrany životního prostředí, flóry a fauny a využívání přírodních zdrojů.**
2. **Databáze (registr) se stabilními plošnými informacemi o životním prostředí, sloužící k efektivnímu strategickému i operativnímu územnímu plánování, plánování v oblasti zemědělství, lesnictví, vodního hospodářství, dopravy, energetiky a v dalších oblastech. Tyto informace budou využívány i občany při volbě bydliště, pracoviště nebo rekreačního prostředí.**
3. **Aktuální informace monitoringu životního prostředí (chemické, radiační, biologické, hlukové a elektromagnetické parametry ovzduší, stav terénu, vodních toků a zdrojů, přírodní flóry a fauny) a prognózy jeho vývoje.**

4. Aktuální standardní informace o počasí a jeho předpovědi.
5. Aktuální individuální nebo plošné varovné informace (signály) o nestandardním počasí nebo překročení norem ukazatelů životního prostředí a o doporučených nebo nařízených opatřeních (v případě vazby na krizová opatření).
6. Databáze speciálně sledovaných druhů flóry a fauny a údajů o opuštěných zvířatech.
7. Aktuální informace o hygienicko-epidemiologické situaci.
8. Informace o realizovaných preventivních a represivních opatřeních k ochraně životního prostředí.
9. Modelové informace o možných variantách vývoje životního prostředí k provádění analýz, hodnocení vývojových variant, indikaci synergií a kritických míst a k výchově k ekologickému chování.

► Vnitřní bezpečnost

Informatizace společnosti a realizace státní informační politiky se v oblasti bezpečnosti projeví zejména:

- a) v komplexním zabezpečení bezpečnosti a ochrany informací a informačních procesů,
- b) v posílení všeobecné bezpečnosti občanů, rodin, obcí a regionů, institucí, podniků, jejich majetku a aktivit, obchodu a finanční sféry, znalosti a dodržování zákonů a norem, práv a povinností, plnění vnitřně bezpečnostních funkcí státní správy a samosprávy,
- c) v posílení bezpečnosti ve specifických oblastech (pozemní, vzdušná a vodní doprava, energetická, pracovní a požární bezpečnost),
- d) v posílení bezpečnosti ve vztahu k mezinárodním integračním procesům a zvýšení možností efektivní součinnosti bezpečnostních služeb různých států a mezinárodních bezpečnostních služeb.

Ve všech uvedených oblastech bude významná indikace podmínek, zdrojů, synergií a startovacích mechanismů, prevence, eliminace a redukce negativních jevů a rizik, které s sebou bude výstavba informační společnosti přinášet. Informační zdroje a prostředky v oblasti bezpečnosti budou mít úzký vztah k informačnímu zabezpečení krizového managementu.

Lze předpokládat, že přednosti a nároky informační společnosti se uplatní zejména takto:

a) V oblasti bezpečnosti a ochrany informací a informačních procesů:

Tato oblast bude řešena jako specifická oblast v rámci koncepce a aplikace informačních a komunikačních technologií a výstavby komunikačních a informačních systémů (takto je pojata i v hlavní části SIP).

b) V oblasti posílení všeobecné vnitřní bezpečnosti:

1. Vytvoření a aktualizace veřejně přístupných informací o legislativě z oblasti bezpečnosti k zajištění bezpečnostní výchovy, bezpečnostních znalostí, práv a povinností občanů a institucí, včetně legislativního ošetření zneužívání informační a komunikační techniky a technologií, porušování zákonů o informacích a autorských právech.
2. Výstavba, vedení a využívání databáze (registru) osob a objektů, včetně specifických informací o pobytu a pohybu trestaných, hledaných nebo pohřešovaných osob.

3. Instalace bezpečnostních zařízení k ostraze objektů a majetku a jejich přímého napojení k majitelům a k orgánům policie.
4. Integrace a centralizace tísňového volání a koordinace záchranných, zdravotnických a bezpečnostních služeb v rámci IZS.
5. Informační podpora aktivit policie v boji s kriminalitou (organizovanou i všeobecnou) a při udržování veřejného pořádku.
6. Indikaci nezákonných aktivit a iniciaci bezpečnostních opatření při porušení zákonů v oblasti komunikací, elektronického obchodu a finančnictví.
7. Vytvoření, udržování a využívání informací pro přípravu, realizaci a využití kontrolních a inspekčních opatření (COI, NKÚ).

c) V posílení vnitřní bezpečnosti ve specifických oblastech:

1. Vytvoření a aktualizace veřejně přístupných informací o legislativě z oblasti vnitřní bezpečnosti ve specifických oblastech (doprava, energetika, pracovní bezpečnost, požární bezpečnost) k zajištění bezpečnostní výchovy, bezpečnostních znalostí, práv a povinností občanů a institucí.
2. Výstavba, vedení a využívání databáze (registru) motorových vozidel a řidičů (s evidencí přestupků a pojistných událostí), řešení krádeží motorových vozidel.
3. Informační zabezpečení řízení dopravního provozu, aktuální a pohotovostní nabídka optimálních tras a objížděk, urychlení a zkvalitnění zásahů u dopravních havárií.
4. Automatická indikace požárů a stavu protipožárních opatření, přímé předání informací HZS, koordinace a optimalizace likvidace požárů.
5. Informační podpora ekologických a energeticky úsporných technologií v dopravě a průmyslu.
6. Výstavba, vedení a využívání databáze s evidencí plateb pojistného a o pojistných plněních k poskytování bonusů a podpoře bezškodního provozu motorových vozidel.
7. Informační báze pro bezpečnost a optimalizaci provozu železniční dopravy, koordinace při řešení nehod a neštěstí v železniční dopravě.
8. Informační báze pro zabezpečení a kontrolu vodní dopravy a využívání vodních toků a ploch.
9. Informační zabezpečení řízení letového provozu.
10. Informační báze pro bezpečnost a optimalizaci provozu energetické sítě, řešení provozních výpadků a havárií, informační propojení s Mezinárodní energetickou agenturou OECD.
11. Prevence, řešení a evidence pracovních úrazů.

d) Posílení bezpečnosti v mezinárodní dimenzi:

1. Vytvoření a aktualizace veřejně přístupných informací o legislativě z oblasti bezpečnosti ve vazbě na mezinárodní bezpečnostní standardy, k získání bezpečnostních znalostí a informací o právech a povinnostech občanů, soukromých i státních institucí a institucí ve vztahu k mezinárodnímu prostředí (včetně cest občanů do ciziny a podnikání v cizině).
2. Informační báze k naplnění Shengenských dohod k přípravě vstupu ČR do EU (policejní spolupráce, zbraně a střelivo, nelegální obchod s drogami, azylová, vízová a migrační politika a evidence).
3. Vytvoření, aktualizace a využívání báze policejních informací a komunikačního systému, umožňujících výměnu informací a koordinaci činnosti s policejními složkami jiných států, mezinárodních společenství (EU) a organizací (INTERPOL, EUROPOL) zejména v oblasti prevence a represe organizovaného zločinu, terorismu a praní špinavých peněz.

► Obrana

Současné moderní pojetí obrany se, jak známo, vyznačuje:

- **komplexností** (řeší se široké spektrum bezpečnostních rizik vojenského, nevojenského a smíšeného charakteru, včetně nově se objevujících rizik a jejich synergií),
- **integrálností** (bezpečnostní rizika se neřeší izolovaně a lokálně, ale s uvažováním jejich mezinárodní dimenze, a to jak v plošném a časovém charakteru jejich ničivého působení, tak v opatřeních prevence, redukce a eliminace rizik a jejich následků),

- civilní kontrolou ozbrojených sil (v procesu plánování, přidělování zdrojů, připravenosti a nasazení),
- participací civilních složek (obrana není záležitostí pouze ozbrojených sil),
- akcentem na prevenci vzniku a eskalace krizí,
- preferencí využívání politických a ekonomických nástrojů,
- akcentem na hospodárné využívání obranných zdrojů.

Vstup ČR do NATO plně reflektuje uvedené atributy. K jejich naplnění ve všech typech obranných misí NATO (samostatná obrana vlastního území, kolektivní obrana Aliance, mírové operace mimo území Aliance) vyplývá pro ČR, z hlediska informatizace, zejména nezbytnost dosažení interoperability systémů konzultací, řízení a velení – především uplatněním standardů NATO. Dalším požadavkem je výrazný posun v rozsahu a kvalitě informační a technologické báze obranného plánování, jak na úrovni NATO, tak na úrovni ČR a rezortního plánování.

Stejně požadavky vyplývají z dosažení přidruženého členství České republiky k Západoevropské unii (ZEU), a to rovněž s ohledem na proces přibližování ZEU a Evropské unie (EU).

Moderní, kvalitativně nový přístup k informacím a komunikacím se uplatní ve vztahu ke krizovému managementu, civilnímu nouzovému plánování, ve vztazích AČR a civilních složek rezortu obrany k orgánům státní správy a samosprávy, k médiím a občanům, v řízení činnosti, každodenního života a přípravy vojsk a štábů a v hospodárném využívání zdrojů.

I když značná část informačních procesů v oblasti obrany má rezortní charakter a pracuje s citlivými nebo utajenými informacemi, civilní řízení obranných zdrojů a kontrola armády umožňuje a zároveň vyžaduje úzký vztah k státní informační politice a výstavbě informační společnosti, a tedy i propojení se státním informačním systémem, datovými registry a informačními systémy jiných rezortů. Tato oblast by měla přispět i k pozitivnímu obratu v postoji veřejnosti a chápání výstavby a činnosti armády jako účelné služby k zachování míru a stabilizaci bezpečnostního prostředí

Konkrétně se bude jednat o neutajované informace v těchto oblastech:

1. Vytvoření a aktualizace veřejně přístupné báze informací o legislativě, neutajovaných aliančních, národních a rezortních standardech z oblasti obrany, činnosti a výstavby armády k zajištění branné výchovy, náboru příslušníků AČR, znalosti práv a povinností občanů a institucí při přípravě a realizaci obrany a pravidel akvizice vojenského materiálu a techniky.
2. Návaznost na registry SIS, včetně životního prostředí, k optimalizaci přípravy a činnosti vojsk.
3. Vytvoření a aktualizace veřejně přístupné báze informací o reálném stavu AČR a procesech, které v ní probíhají pro občany, instituce a media.
4. Návaznost na IS a databázi o vzdušné situaci k řízení vzdušného provozu.
5. Informační zabezpečení obranného plánování (v neutajované části).
6. Informační zabezpečení vazby na civilní nouzové plánování.
7. Informační a komunikační zabezpečení vazby na subjekty krizového řízení a IZS.
8. Informační a komunikační zabezpečení přípravy obyvatelstva a řídicích orgánů státní správy a samosprávy na činnost v mobilizaci a ve válce (neutajované informace).
9. Vytvoření, aktualizace a využívání informační báze lidských zdrojů, včetně evidence, zdravotní profesní identifikace vojáků, branců a záloh.
10. Vytvoření, vedení a využívání informační báze o materiálně technických zdrojích, včetně neutajovaných informací o stavu a možnostech dodávek obranného průmyslu, státních

zakázkách a akvizičních procesech a o výzkumu a technologickém pokroku v oblasti vojenské techniky.

11. Vytvoření, vedení a využívání informační báze o finančních zdrojích a jejich vazbě na ekonomický potenciál státu.
12. Vytvoření, vedení a využívání informační báze o informačních zdrojích, včetně informací o stavu a možnostech dodávek informačních a komunikačních technologií pro rezort obrany.
13. Vytvoření, vedení a využívání informační báze o státních hmotných rezervách a přípravě obranné infrastruktury.

Některé neutajované informační báze a procesy, provozované v rezortu obrany, budou využitelné v civilní sféře, např. v oblasti řízení letového provozu, monitorování radiační a chemické situace, meteoslužby, toposlužby (pro specifikované informace o terénu a pro tisk map) aj.

Závěr: Informační společnost – šance a výzva k harmonizaci, stabilitě, bezpečnosti, kulturnosti, efektivnosti a perspektivnosti

V zrcadle možnosti moderních informačních a komunikačních technologií, a zejména intelektuálního vkladu a uplatnění lidského ducha, tvořivosti a práce, vyniká paradoxnost a anachronismus některých fenoménů v současné lidské společnosti: Manipulování společenským vědomím cestou některých masmédií, neschopnost indikace frází, lží a šumu a matení pojmů, povrchní přístup a neúcta ke vzdělání, disharmonie hodnotové orientace a enormní materializace života, neúcta k vytvořeným hodnotám, přírodním zdrojům a životnímu prostředí, neschopnost komunikace a přežívání středověkých praktik ve vykonávání státní moci a ve vztazích mezi státy, národy a lidmi, kontrastující s technologickými, komunikačními a informačními možnostmi.

Neúcta k lidskému životu a neodpovědnost k perspektivě příštích generací, kontrastující s využíváním vysoce sofistikovaných informačních technologií ve zdravotnictví, vědě a výzkumu.

Výstavba informační společnosti je z tohoto hlediska jedinečnou šancí a zároveň výzvou, jak cestou využití moderních informačních a komunikačních technologií a rozvoje informatické vzdělanosti, kultury a efektivnosti provést výrazný krok k postavení přežívajících a účelově podporovaných paradoxů a anachronismů ničení hodnot, násilí, plýtvání zdroji a devastace životního prostředí mimo životní normu. Výstavba informační společnosti je šancí a výzvou k uplatnění humanitární a etické dimenze individuálních, skupinových i společenských procesů a odpovědnosti vůči příštím generacím.

Pro malý stát, jakým je Česká republika, má tato orientace vývoje a praktických kroků k zdravé, stabilní, harmonické, nikoliv idylické a bezkonfliktní, ale přesto hospodárné, mírové, perspektivní společnosti vzdělaných a informovaných občanů, náročných vůči veřejné správě i vůči sobě samým, zásadní význam. Zároveň je příležitostí prezentace jeho kulturnosti a praktického uplatnění intelektuálního potenciálu.

Dokument „Státní informační politika – cesta k informační společnosti“ do tohoto rámce zapadá. Jeho koncipování, zpracování, nebylo jednoduché a moje poznámky nelze chápat jako kritiku, ale jako projev reálného stavu variantnosti názorů a přístupů. Předpokládám, že dokument již nedozná výrazných změn, brzy bude vládou schválen

a vytvoří pro informatizaci v naší zemi příznivou bázi (opět si nemohu nepovzdechnout nad přerušáním prací na koncepci informatizace rezortu obrany). V souvislosti čistě záměrně rovněž nemohu neuvést, že tak jako tvorba, ani realizace SIP nebude snadná, protože konflikty názorů se mohou transformovat do roviny zájmů: informace a jejich inteligentní zpracování a využití dává zelenou pravdivosti, transparentnosti a efektivnosti využití zdrojů, a to jak lidských a materiálních, tak informačních, a vystavuje stop atributům opačným. S tím souvisí i určitý metodologický poznatek, který jsem v procesu připomínkování a úprav dokumentu subjektivně indikoval: preferování technických a technologických a komerčně uživatelských aspektů a určitý strach, ostych nebo averze před komplexním pojetím a netradičními dimenzemi politiky, etiky a odpovědnosti. Není přece pochyb, že tyto dimenze do koncepčního dokumentu na státní úrovni (nikoliv do reklamního materiálu počítačových, obchodních a finančních firem a institucí) organicky patří.

Velice doporučuji prostudování hlavní i přílohové části SIP pracovníkům rezortu obrany – subjektům i objektům státní informační politiky a výstavby informační společnosti. Poučení jsou nesporná, a to jak věcná, tak metodologická. Stejně jako ve společnosti, i v rezortu obrany jde o moderní přístup k informacím, technologii a organizaci jejich tvorby, zpracování a využití, o podporu moderního uplatnění funkcí moderního státu jako efektivně řízeného a fungujícího systému společenských (nikoliv individuálních nebo skupinových) služeb občanům a uznávaného partnera v mezinárodních vztazích. Efektivní aplikace koncepčního materiálu na státní úrovni však nebude možná při absenci systémového přístupu, rezortní koncepce informatizace a organizačního zajištění potřebných aktivit a vztahů.

Literatura:

1. Státní informační politika – cesta k informační společnosti, ÚSIS, 1999.
2. Svoboda, V. : Informatizace a řízení zdrojů rezortu obrany, VR 2/99.
3. Tošenovský, E.: Krizové centrum a zkušenosti z radnice. Přednáška na konferenci SPIS, květen 1999.