

Major Ing. Jiří Baloun

Informační infrastruktura USA pro obranu

Nalézáme se v době radikálních změn. Konfrontace Východ-Západ, která určovala bezpečnostní situaci v uplynulých několika desetiletích, je postupně nahrazována novou bezpečnostní filozofií. Odzbrojovacími rozhovory se daří snižovat rozsah sil a prostředků na počty potřebné pro obranné systémy. Role armády je měněna. Přesto však potřeba bezpečnosti, lokální i globální, zůstává. Eskalace konfliktů v Perském zálivu a v současné době na území bývalé Jugoslávie nám ukazuje, jakým způsobem může regionální konflikt ovlivnit globální bezpečnost.

Ve vojenských a provozních činnostech bude hrát stále důležitější roli pružnost a mobilita. Situace, které mohou vzniknout, budou dynamičtější, plynulejší a komplexnější. Velitelé budou nuceni přijímat rozhodnutí rychleji než kdy předtím. Množství došlých, zpracovávaných a předávaných informací poroste a v souvislosti s tím i význam elektronických zařízení jako prostředků pro práci s nimi. Také software elektronických systémů se plynule zdokonaluje a civilní a vojenské aplikace se postupně sbližují.

* * *

Ve spojitosti s uvedenými skutečnostmi a s reorganizací ozbrojených sil bylo v USA rozhodnuto o vybudování **obránné informační infrastruktury** (DII - *The Defense Information Infrastructure*), zahrnující jak mírový, tak válečný stav. Jedná se tedy o globální informační systém, který by měl umožnit přenos informací ze všech zatím zavedených systémů nezávisle na jejich technickém provedení.

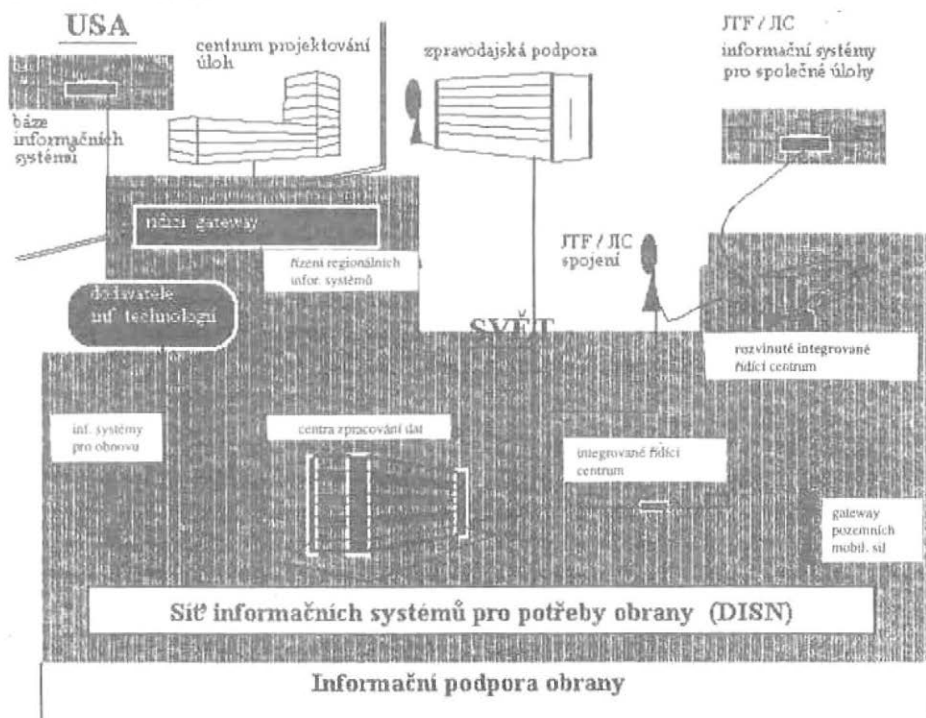
Samozřejmostí je propojení radiotelekomunikačních a počítačových sítí, zajištění automatického výběru nejlepších přenosových cest, pokrytí požadavku na priority a podobně. Tato informační technologie by měla podpořit bojeschopnost ozbrojených sil všude, vždy a při plnění jakéhokoliv úkolu.

DII je definována jako systém spojovacích sítí, prostředků automatizace, databází a aplikací, umožňujících zpracování a přenos informací, jež potřebují uživatelé v míru, všeobecné krizi, konfliktu, humanitární podpoře i při plnění úkolů v době války. To zahrnuje především:

- fyzickou vybavenost prostředky přenosu, uložení, zpracování a zobrazení hlasových zpráv i dat,
- práci s informacemi, které mohou být ve formě videa, databází, zvukových nahrávek, písemných sdělení atd. a jejich přenos po služebních a jiných provozních spojích,
- aplikaci síťových standardů a protokolů, které usnadní vzájemné spojení a spolupráci mezi sítěmi a systémy a zajistí bezpečnost hodnoty v informaci ukryté,

- existenci lidských a dalších zdrojů, které zabezpečí integraci projektů, managementu a provozu DII, budou rozvíjet aplikace, vybavenost a služby a tím zvyšovat možnosti a využitelnost systému.

Na obr. 1 je znázorněna architektura DII. Z obrázku je patrné, že je zde vytvořena síť informačních systémů pro potřeby obrany (DISN - *Defense Information Systems Network*), ve které jsou zahrnuti dodavatelé informačních technologií, regionální řízení informačních systémů, centra zpracování dat (tzv. megacentra), integrované řídicí centrum (stacionární), rozvinuté integrované řídicí centrum (mobilní), pozemní mobilní „gateway“ (mezisíťový počítač) ozbrojených sil.



Obr. 1: Architektura DII

Tato síť je napojena na zabezpečovací základnu, kterou tvoří báze informačních systémů a centrální projektové pracoviště (tyto dva subjekty do DISN vstupují přes vzpomínané regionální řídicí místa) a na pracoviště, podporující systémy z hlediska dodávání zpravodajských informací. Na druhé straně je tato síť využívána ozbrojenými silami při plnění společných úkolů.

Přenos informací zabezpečují stacionární i mobilní spojovací systémy, tvořené spojevacími prostředky různých druhů a typů, které jsou součástí DISN.

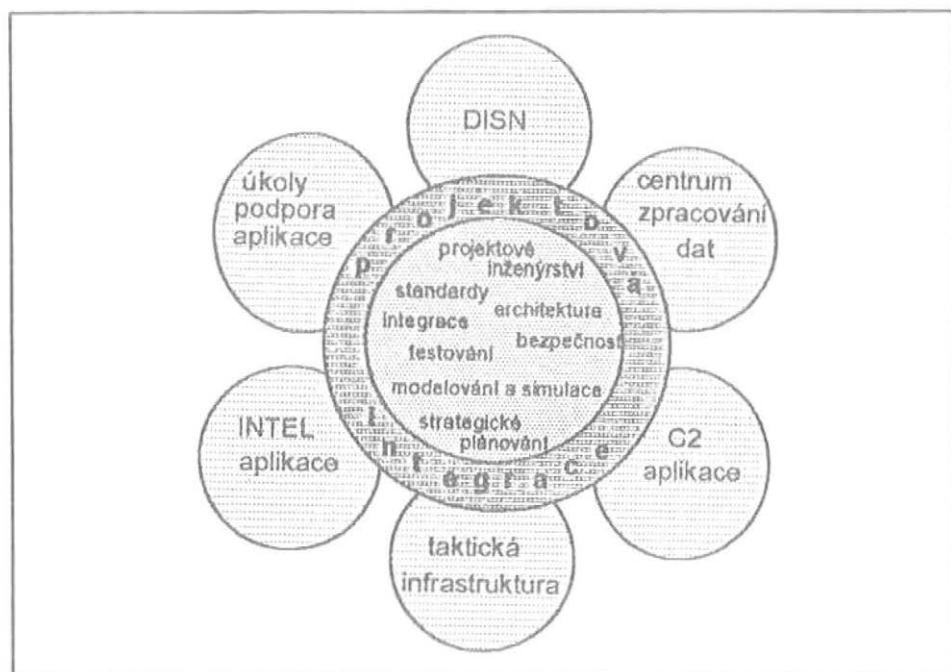
Velmi důležitou složkou DISN jsou samozřejmě lidé (v rámci „západních“ zemí často nazývaní lidské zdroje), na jejichž odbornou způsobilost bude kladen velký důraz.

Proč vytvářet globální informační infrastrukturu pro potřeby obrany?

Důvody bychom mohli shrnout do několika hlavních bodů:

- přístup k informacím je klíčem k bojeschopnosti,
- náklady na fungování současných informačních technologií vážně ovlivňují další modernizaci,
- k modernizaci je důležité přistupovat s vědomím dodržení interoperability, efektivity a spojitosti s bojeschopností, což je v rámci globálního systému lépe řešitelné,
- je nutné podporovat implementace pružných aplikací.

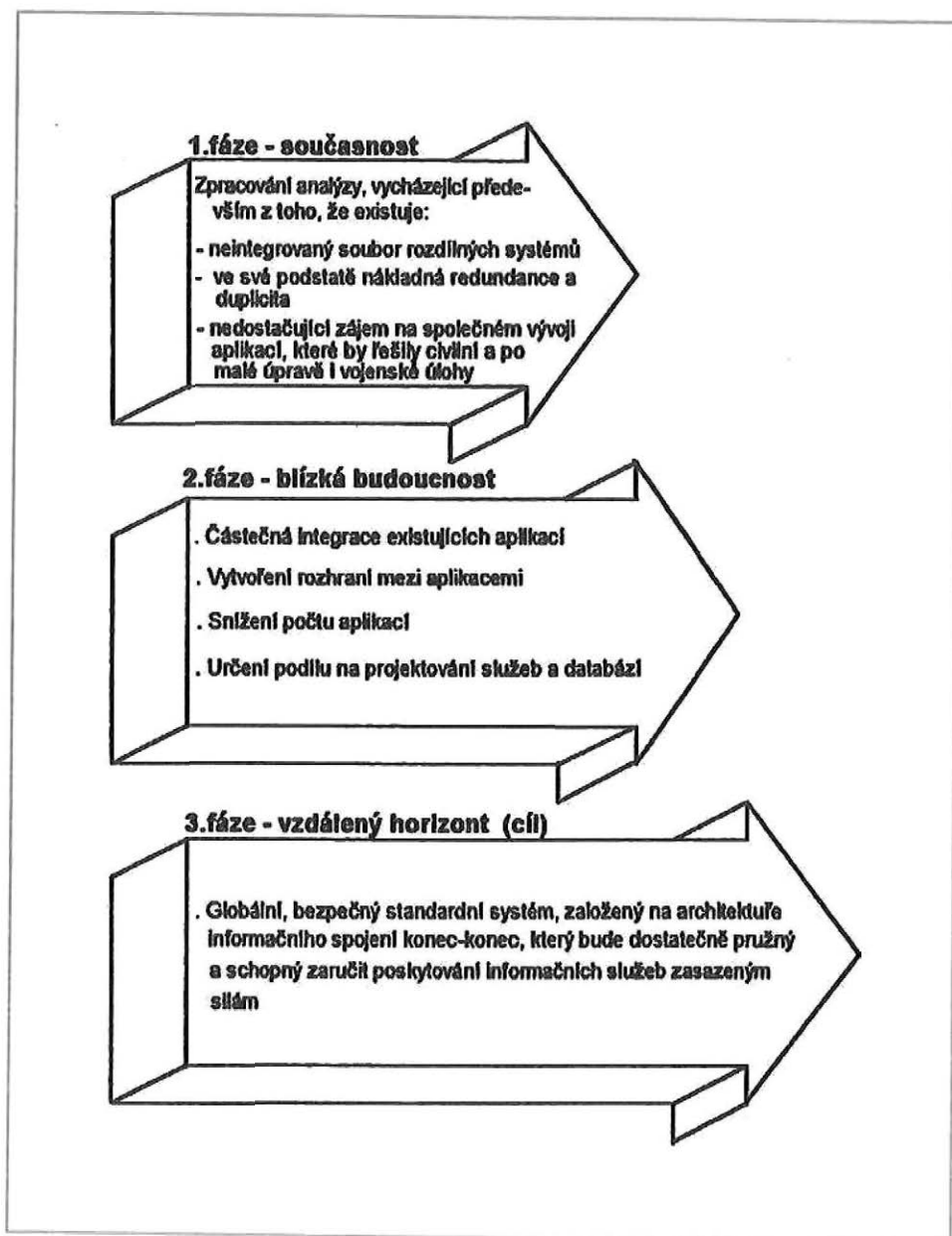
Z těchto důvodů je patrné, že uvést do provozu modernizovanou informační infrastrukturu je jeden z prvořadých úkolů v rámci zajišťování obranyschopnosti státu.



Obr. 2: Strategie zabezpečení DII

Na obr. 2 je celkový pohled na strategii zabezpečení DII, který nám dá představu o tom, co a jakým způsobem se na fungování DII podílí. Komplexním zabezpečením provozu DII se směřuje ke splnění těchto cílů:

- zajistit požadovanou bojeschopnost - umožnit z hlediska přístupu k datům přidělování, spolupůsobení a součinnost vojsk v operacích a zároveň přístup k datům zabezpečit podle stupně oprávnění,
- dát do souladu vývoj a distribuci funkčních aplikací cestou integrace projektů a prototypové operace vést prostřednictvím funkcí a služeb v rámci definice DII,



Obr. 3: Úkoly v rámci realizace DII

- poskytovat vybrané služby jako součást modernizované infrastruktury informačních technologií,
- srovnat úsilí DII s podobnými činnostmi na federální úrovni ve větším ekonomickém měřítku.

Budování informační infrastruktury má probíhat ve třech fázích (obr. 3), které jsou charakterizovány následujícími skutečnostmi a úkoly:

1. fáze - současnost, která se vyznačuje především zpracováním podrobné analýzy.
2. fáze - blízká budoucnost (Near Term), jejímž hlavním obsahem je snížení počtu aplikací a jejich integrace.
3. fáze - vzdálený horizont (Far Term). Konečným cílem, dosaženým na konci této fáze, je globální, bezpečný standardní systém.

Závěr

Armáda České republiky před sebou nemá tak rozsáhlé úkoly jako armáda USA a není zdaleka tak početná. Prostorové působení těchto dvou armád se už vůbec nedá porovnávat. Přesto jsou zde oblasti, které jsou principiálně a systémově srovnatelné a musí být zabezpečeny bez ohledu na výše uvedené kvantitativní poměry.

Mezi tyto oblasti rozhodně patří nutnost mít solidní informační systém (informační systémy), projektovaný a vytvářený s využitím všech dostupných technologií a v duchu světového vývoje. Přitom je důležité si uvědomit dvě základní skutečnosti, že:

1. budování informačního systému (IS) je neustále pokračující proces,
2. moderní IS netvoří jen rychlost, ale především kvalita aplikací a služby, které systém umí poskytovat.

IS by měl být tvořen výkonnými prostředky pro zpracování informací, novými aplikacemi a vysokou rychlostí přenosu ve vyváženém poměru, aby bylo možno efektivně využít vynaložené prostředky. To vše samozřejmě podpořeno komplexním zabezpečením provozu (servis, opravy, školení atd.).

Na konec to nejdůležitější - lidé. Lidé, na jejichž úlohu se často při projektování systémů zapomíná. Jsou to ti, kteří budou zabezpečovat provoz systémů, ale také uživatelé, kterým tento systém výrazně pomůže zkvalitnit práci. Všechny tyto skupiny musí být připraveny, až přijde čas a my o nových, kvalitativně s dosud ničím srovnatelných podmínkách nebudeme jen mluvit, ale budeme je mít. Ty podmínky tu budou brzy.