

K některým otázkám utajeného velení

Plukovník Josef Průša

Naše šifry I. a II. stupně plně zajišťují předání zpráv odpovídajícího charakteru s požadovaným stupněm bezpečnosti utajení.

V podmínkách soudobé operace a soudobého boje vystupuje však vedle dosavadního požadavku bezpečnosti utajení i požadavek nový: požadavek podstatného časového zrychlení hovorů a předávání zpráv. Tento požadavek vyplývá z potřeby co nejrychlejší reakce na časté změny situace, kdy je třeba maximálně zkrátit dobu, potřebnou k doručení příslušných hlášení rozhodnutí, rozkazů a pokynů. Tento požadavek je zároveň i důsledkem dnešní technické možnosti a připravenosti nepřítele, rychle aktivovat účinné rušení provozu našich rádiových spojů.

V soudobých podmínkách operace a boje bude tedy třeba současně řešit jak dosavadní požadavky utajení zprávy a obsahu hovoru, tak i nový požadavek podstatného zkrácení doby předávání zpráv a vedení hovorů.

Při řešení tohoto problému budeme muset uvažovat jednak technickou a jednak taktickou rychlost předávání zpráv. Technickou rychlostí předávání zprávy je rychlost jejího „odehrání“ příslušným pojtkem (rádiovou stanicí, směrovou stanicí apod.). Naproti tomu taktická rychlost předání zprávy je závislá na souhrnném čase, potřebném od okamžiku rozhodnutí předat určitou zprávu, až do okamžiku doručení dešifrované zprávy adresátu. Do výsledné doby, určující taktickou rychlost předávání zpráv bude nutno tedy zahrnout jak sestavení textu zprávy in claris a její zašifrování, tak i technické předávání po pojtkách, dešifrování zprávy a její doručování příjemci.

Dříve než přikročíme k bližšímu rozboru některých faktorů, určujících taktickou rychlost předávání zpráv, bude třeba zatím vyloučit z dalších úvah problematiku šifer I. stupně. Při používání šifer I. stupně zůstane totiž i nadále rozhodujícím požadavkem naprosté utajení odesílané zprávy, neboť šiframi I. stupně budou šifrovány zpravidla jen závažné rozkazy, směrnice a podobně, tedy dokumenty převážně dlouhodobě platnosti a s pochopitelně méně naléhavou potřebou co největší taktické

rychlosti předávání zprávy (ve srovnání např. s doručením povelu k odpálení rakety s jadernou náloží). Požadavek zkrácení textu takové šifrovky bude se v podstatě kryt s požadavkem používat stručnou a jasnou vojenskou mluvu s využitím všech zkratk, předepsaných řády.

Sestavení zprávy má značný vliv na taktickou a technickou rychlost jejího předávání. Z podrobného rozboru zpráv zašifrovaných šiframi II. stupně a předaných po pojtkách v průběhu několika velitelsko-štabních cvičení na stupni štábu armády a divize v minulém roce vysvitá, že naše štáby nevypracovaly si dosud systém dešifrování a jasného vojenského vyjadřování. Převážnou část zkoumaných zpráv bylo možno, při plném dodržení obsahu zprávy, zkrátit o 10 až 30 % slovního rozsahu. Při vedení předem nepřipravených hovorů na pojtkách pak situace je ještě horší: nesprávná terminologie, zbytečná slova, rozvláčné fráze a podobně, nejen prodlužují bezprostřední dobu vedení hovoru, nýbrž i komolí smysl, ztěžují pochopení smyslu a obsahu hovoru. Vynucují si časté dotazy druhého účastníka hovoru a velmi citelně snižují jak taktickou, tak hlavně i technickou rychlost předání příslušného obsahu hovoru. Především bude nutno usměrnit pozornost velitelů a štábů na používání správné, jasné a stručné vojenské mluvy.

Zašifrování zprávy podle dosavadní praxe můžeme rozdělit na „ruční“ šifrování a na šifrování pomocí šifrovacích strojů. Jestliže „ruční“ šifrování bude zpravidla prováděno předem, pak šifrování pomocí šifrovacích strojů může být prováděno buď také předem, nebo automaticky, přímo při vyslání zprávy, napojením příslušných šifrovacích strojů bezprostředně k pojtku. Pokud se týče doby, potřebné pro zašifrování zprávy, jsou u „ručních“ metod rozhodující jednak vhodnost zvolených kódů a šifer, a také připravenost šifrujících k jejich rychlému používání. U šifrování pomocí šifrovacích strojů zdá se na první pohled rychlejší šifrování automatické, kdy odesílatel předává svou zprávu de facto otevřeně a příslušné pojtko, spřažené s automaticky pracujícím šifrovacím strojem, vysílá zprávu šifrovaně. Tento způsob však zpravidla nedovoluje, nebo alespoň podstat-

ně ztěžuje, možnost několikanásobně zrychleného provozu pojítka a tak nepříznivě ovlivňuje technickou rychlost předání zprávy.

Technickou rychlost předávání zprávy musíme posuzovat ze dvou hledisek. Jednak z hlediska jejího vlivu na celkovou taktickou rychlost předání zprávy, a jednak z hlediska bezpečnosti provozu příslušného pojítka, to je z hlediska možnosti nepřátelského zásahu rušením. Jestliže při posuzování celkové taktické rychlosti předávání zprávy mohli bychom na příklad prodlou-

ženou dobu bezprostředního vysílání pojítkem kompenzovat zkrácením některého jiného faktoru taktické rychlosti předávání zprávy, pak z hlediska požadavku časové co nejkratší možnosti nepřátelského rušení, to jest z hlediska technické rychlosti, byla by taková kompenzace nepřipustná.

Vývojově bude tedy nutno hledat a používat takové šifrovací systémy, které by při celkovém zvýšení taktické rychlosti předávání zpráv zároveň i podstatně zkracovaly dobu technického předávání zprávy, zejména při rádiovém spojení.

Příjem a dešifrování zprávy

Při běžném provozu pojítek závisí taktická rychlost předávání zpráv na všestranné spolehlivosti a výkonnosti pojítka a na výcviku a připravenosti jeho obsluhy. Při přímo vedených hovorech samozřejmě i na připravenosti účastníků hovoru.

Zprávy vysílané s použitím systémů mnohonásobných zrychlení vysílání budou při příjmu zpravidla zaznamenávány některým technickým způsobem a poté, popřípadě souběžně, dešifrovány příslušnými šifrovacími stroji.

Při příjmu zprávy, šifrované automaticky, je vyslaná zpráva opět automaticky dešifrována a tak oba účastníci pracují jako při předávání otevřených zpráv, nebo při vedení otevřeného hovoru.

Nepřátelské rušení je velmi závažným faktorem, ovlivňujícím jak taktickou, tak i technickou rychlost předávání zpráv. V soudobých podmínkách vedení boje je nutno předpokládat, že nepřátelský systém rušení nám nedovolí delší časový provoz rádiové stanice na téže frekvenci. Je proto nutno hledat bezpečné systémy přechodu z jedné frekvence na druhou. Dosud běžně užívaný systém přechodu na záložní frekvenci je ztížen tím, že obě stanice, jak vysílající, tak přijímající, musí přejít na záložní frekvenci současně, což ne vždy je možno sladit, a pak dochází zpravidla k dočasnému narušení spojení. Bude proto třeba realizovat takový systém, při němž bude příjem zabezpečen současně na hlavních, tak na všech určených záložních frekvencích. Vysílající bude moci kdykoli přejít na kteroukoli z nich. Tento systém potřebuje ovšem i automatické návěští pro vysílajícího, jakmile bude frekvence, na níž vysílá, rušena. Technicky je proveditelný i automatický přechod při rušení na nerušenou záložní frekvenci.

Organizace odesílání a přijímání zpráv

ve štábech. Poměrně značné zvýšení taktické rychlosti předávání zpráv a plně uplatnění všech technických vymožeností pro zvýšení technické možnosti předávání zpráv umožňuje systém výpraven zpráv. Soustředěním odesílaných zpráv z celého štábu na jednom místě, disponujícím všemi druhy potřebných pojítek, je zabezpečena možnost pružného využití právě toho druhu pojítka, které je v dané době nejvýhodnější. Výhodou je zde rovněž soustředění šifrování a dešifrování zpráv do rukou zvlášť určených orgánů. U šifer I. stupně šifrují pouze příslušníci šifrovacích oddělení. U šifer II. stupně je možno využít i ostatních důstojníků všech složek štábu, např. organizovat služby „dozorčích důstojníků štábu pro šifrování“ přímo u výpravny zpráv.

Systém výpraven pak umožňuje i spolehlivou evidenci všech odeslaných i přijatých zpráv.

Šifrování při mírovém výcviku. Ve skutečném boji je příslušnými řády povoleno předávat celou řadu povelů, hlášení, rozkazů a různých zpráv otevřeně, zejména na nižších velitelských stupních; v podstatě je tomu tak i tehdy, kdy nepřítel má možnost vyslanou nešifrovanou zprávu zachytit, nemá možnost ji však využít. Nedokáže včas na obsah zprávy reagovat. Stejně tak v případech, kdy hrozí nebezpečí z prodlení při šifrování zprávy, může se velitel rozhodnout vyslat otevřeně i zprávu, jež jinak má být šifrována.

V podmínkách mírových cvičení však není možné ani zprávy, povolené v boji, předávat otevřeně, odesílat nešifrované. Nepřítel odposlechem i takovýchto drobných zpráv získává řadu údajů, jež vhodně vyhodnoceny, dávají nepříteli velmi závažné poznatky o způsobu činnosti, o organizaci, o taktických normách a o dalších údajích

nejen taktického, ale často i operačního charakteru.

Je ovšem samozřejmé, že náš dnešní mýrový systém „všechno šifrovat“ ztěžuje velení, zejména na nejnižších velitelských stupních, ve srovnání se skutečnými bojovými podmínkami. Tento fakt je proto nutno brát v úvahu při hodnocení takového cvičení.

Jestliže při předávání zpráv je problematika technického zrychlení vlastního předávání řešitelná především zavedením technicky dokonalých šifrovacích strojů, pak technické zrychlení přímo vedených rozhovorů na pojítkách je v současné době možné jediné výběrem a zavedením vhodných šifer II. stupně a jejich dokonalým zvládnutím hovořícími. Automatické, technické šifrování otevře vedených hovorů není totiž dosud vyřešeno tak, aby zabezpečovalo požadovaný stupeň utajení.

Dosavadní forma a systémy běžných kódovacích materiálů (šifer II. stupně) umožňuje zpracovat ve svých slovnících hlavně jen jednotlivá slova anebo krátké výrazy, složené z několika slov, nebo nejvýše z jedné či dvou krátkých vět. Tyto materiály plně vyhovují svému účelu, tj. utajit obsah předávané zprávy nebo vedeného hovoru. Při tom záleží ovšem na přípravě a úpravě jejich slovníků, což je povinností především uživatelů těchto pomůcek, to jest nikoli příslušníků šifrovacích oddělení, nýbrž operačních oddělení štábů, štábů druhů vojsk a týlu, podle předurčení příslušných šifer. Jsou-li slovníky voleny nevhodně a nadto, jestliže uživatelé prací s těmito materiály neovládají, pak taková šifra je sice pomůckou pro utajení zprávy, ovšem spojení se v takovém případě zdržuje a komplikuje. Při vhodně volených slovnících a při dokonalém ovládnutí těchto šifer uživateli, jsou naše současné šifry II. stupně vhodnou pomůckou pro utajení.

Požadavek podstatného zkrácení zprávy, při zachování dosavadní bezpečnosti utajení obsahu zprávy a hovoru můžeme splnit při vhodné aplikaci dnešních našich kódů.

Podle dosavadní praxe jsou kódy užívány ve formě tzv. kódových tabulek, určených k předávání zpráv různého okruhu otázek a tematiky a pro zašifrování zpráv s vysokou standardností. Tyto kódové tabulky ve svých slovnících zahrnují výrazy, věty, slovní, zkratkové i písmena abecedy, bigramy, trigramy, speciální výrazy,

čísla, číslice atd. Slovník kódových tabulek pak bývá rozdělen podle svého obsahu do speciálních částí, jako např. jména, osady, zbraně apod. Přitom dosavadní kódové tabulky zpravidla nerozdělují se podle druhu boje (určité fáze operace), ani podle stupně velení. Takto připravené kódové tabulky ovšem nemohly by splnit soudobý požadavek podstatného zrychlení technické a taktické rychlosti předávání zpráv. Je to však právě systém kódů, který je možno propracovat, prohloubit a tak novými formami jeho aplikace zabezpečit splnění požadavku všestranného zrychlení předávání zpráv.

Pro zjednodušení dalšího rozboru možností kódového spojení zaměříme se na řešení kódového spojení mezi velitelem armády na PVS a náčelníkem štábu armády na VS v případě, že velitel armády se svou skupinou dočasně vyjel na PVS armády, aby odtud osobně řídil odražení silného nepřátelského protiúderu. Náš kód bude tedy mít následující charakteristiku:

- bude užíván k hovorům, popřípadě k předávání zpráv pouze mezi dvěma místy, a bude tedy vyhovet v minimálním počtu výtisků (2–4 exempláře);
- časově bude v používání jen velmi krátce (do návratu velitele armády z PVS zpět na VS armády).

Tyto charakteristické vlastnosti našeho kódu zabezpečují i při nejjednodušších soustavách šifrování kódů značně vysoký koeficient bezpečnosti utajení hovorů a zpráv.

Nejzávažnější otázkou bude správná volba a příprava slovníku kódu. Zvažme proto, co by měl obsahovat slovník kódu, připravovaného pro uvedený styk PVS a VS armády.

1. Pro vedení přímého hovoru musí náš kód obsahovat základní věty všeobecného charakteru, jako například:

- „Velitel armády se rozhodl“
- „Náčelník štábu, zařídte rozpracování velitelského rozhodnutí a doručení příslušných rozkazů vykonavatelům. Velitel rozhodl takto...“
- „Náčelník štábu, připravte pro velitele návrh rozhodnutí na zítřejší den. Návrh přednese veliteli osobně na PVS v hodin...“
- „Velitel armády hodlá přemístit své PVS. Náčelník štábu, vyžádejte svolení velitele fronty. Spojení z nového PVS bude prostředky dosavadního PVS. Prostor nového PVS — koordináty...“

Příklad možného rozpracování velitelského kódu

Příloha 1

Návrhy NŠ armády z VS – veliteli armády na PVS

Použití jaderných úderů

		v paleb. postavení	na přesunu	ve vyčkávacím postavení
Navrhuji zničit:	baterii Honest John	01	91	71
	CORPORAL	03	93	73
	MATADOR	04	94	74
	atd. ...	06	96	76
	atd. ...	08	98	78
letectvem:		13	brisantním střelivem:	22
raketami:	A	12	jadernou náloží 3 kt	23
	B	11	jadernou náloží 5 kt	25
	V	15	jadernou náloží 10 kt	24
	atd.:	17	atd.	28
atd.		19	atd.	26
z počtu jaderných nábojů, jež jste vyčlenil k přímému řízení přítomným s Vámi na PVS velitelem dělostřelectva				33
z prostředků, jež jste vyčlenil k přímému řízení mnou z VS				35
Na upřesnění cíle odeslal jsem letecký průzkum. Jeho hlášení výsledku průzkumu bude vysíláno v síti Vašeho návodčího				41
Upřesnění cíle doporučuji provést Vaším letcem, na Váš rozkaz				42
atd. ...				45
atd. ...				47
DOBA ZJIŠTĚNÍ CÍLE:	52	+ 23,23	poznámka: k skutečnému číselnému údaji: 920865 přičti 232126 (údaj, kódu)	
KOORDINÁTY ZJIŠTĚNÉHO CÍLE:	51	+ 232126		
DOBA HLÁŠENÍ VÝSLEDKU LETECKÉHO DOPROVĚ- ŘENÍ CÍLE:	53	+ 11,21	a předej 152981	
ATD:				55
Konec zprávy z tohoto listu, přechod na další list:				36

Každý takovýto složený výraz je možno předat kódovým údajem, např. „KOLO 6225“, kde „KOLO“ znamená název použitého kódu a cifra 6225 jsou souřadnice příslušného slovníkového výrazu.

2. Kód musí dále obsahovat podrobně rozpracovaná hlášení, rozkazy, pokyny a podobně, pro očekávaný druh činnosti vojsk armády, v našem případě tedy z té fáze útočné operace armády, kdy velitel armády ze svého PVS řídí odrazení silného protiúderu nepřítelů a zároveň ovšem i narůstání úsilí na hlavním směru armády. I zde bylo by možno uvést celou řadu možných slovníkových výrazů, obsahujících pod jedním kódovým znakem celá hlášení, celé rozkazy a podobně. V podstatě mohou to být větné výrazy, neměnného obsahu, rozpracované předem v mnoha variantách podle očekávaného a pravděpodobného vývoje situace, nebo to mohou být slovníkové výrazy, udávající rovněž jediným kódovým znakem, který obsahuje několik doplňujících údajů (časových koordinát, určení jednotek apod.). V intencích našich předpisů a řádů má každý velitel (NŠ) právo vypracovat pro velení podřízeným „velitelské kódy“.

Ukažme si možný způsob zpracování části slovníku takového velitelského kódu, pomocí kterého bude NŠ z VS armády navrhovat veliteli armády na PVS, aby bylo provedeno raketovými prostředky, jímž velí velitel dělostřelectva, který je spolu s velitelem armády na PVS, zničení zjištěného nepřátelského jaderného odpalovacího zařízení (viz přílohu).

Vezměme si možno situaci k použití tohoto listu kódu:

„V 15.00 byly zjištěny rakety Corporal v palebném postavení v místě, zasažitelném naší raketou B; úkolování této jednotky B raket je vyhrazeno přímo veliteli armády na PVS (resp. přítomnému s ním veliteli dělostřelectva). V 15.10 došla zpráva o zjištění cíle k NŠ na VS armády. V 15.15 startuje letec z rozkazu NŠ na prověření cíle. V 15.20 dostává velitel armády na PVS návrh náčelníka štábu a v 15.30 potvrzuje náčelníku štábu, že návrh akceptuje. V 15.35 hlásí letce leteckému představiteli na PVS, že cíl je na udaném místě. V 15.40 pak je odpálena raketa B s jadernou hlavicí.“

Jak bude podle našeho kódu vypadat zpráva NŠ z VS, zasláná v 15.20 veliteli armády na PVS: „KOLO 36 03 11 25 33 41 52 38 23 51 95 04 71 53 26 56 36“.

Předání této šifrové zprávy přímým hovorem trvá 20–30 vteřin, dešifrování zapsané přijaté zprávy — 60–90 vteřin, to jest celková potřebná doba k předání kódové zprávy a k jejímu dešifrování je 80–120 vteřin.

3. Kód ovšem bude muset obsahovat, kromě obdobně rozpracovaných dalších hlášení, rozkazů a nařízení, i několik zvláštních tabulek s možností kódovat údaje vlastní a nepřátelské organizace, popřípadě různých prostorů, čar a bodů na mapě, údaje o ztrátách, číselné údaje a podobně. Takto upravená slovníková část kódu umožní hovořícím, pokud se slovníkem byli dobře seznámeni, velmi podstatně zkrácení hovoru nebo vyměňovaných zpráv.

Úkolem a cílem článku nebylo a ani nemohlo být řešit nebo dokonce snad vyřešit komplexně problematiku zkrácení celkové doby, potřebné k předání zprávy jakéhokoli druhu velitelem podřízenému a naopak. Zvýšení jak taktické, tak hlavně technické rychlosti vedení hovorů a předávání zpráv není závislé jen na pomůckách utajeného velení; je funkcí celé řady dalších faktorů, mezi nimi např. kvality spojovacích prostředků, stupně výcviku a připravenosti spojovacích obsluh, celkového systému spojení atd.

Příklady, uvedené v článku, bez nároku na bezprostřední praktickou použitelnost, mají čtenáři jen ukázat reálnou způsobilost našich současných kódových systémů, řešit nejen problematiku utajení obsahu zprávy a hovoru, nýbrž i způsobilost příspěvků k podstatnému zkrácení zpráv a hovorů. Tím umožnit značné zvýšení taktické i technické rychlosti předávání zpráv.

Rozhodujícím momentem pro uplatnění soudobého požadavku na zkrácení doby, potřebné k předávání zpráv a vedení hovorů formou odpovídající úpravy a využití našich šifer II. stupně, je, abychom v našich štábech pochopili, že sestavení šifer II. stupně a především sestavení jejich slovníků, není speciálním úkolem šifrovacích orádů, nýbrž jedním ze základních funkčních úkolů velitelů, náčelníků a štábů všech druhů a stupňů.