

OPERAČNÍ A BOJOVÁ PŘÍPRAVA

JAK ZLEPŠIT POUŽÍVÁNÍ POMŮCEK PRO KODOVÁNÍ

Major Václav Háza

Není dnes již jistě ani jednoho příslušníka naší armády, natož příslušníka velitelského sboru, který by nechápal význam ochrany státního a vojenského tajemství před nepřítelem, který by s rozhořčením neodsoudil každý sebemenší pokus nebo nedbalost napomáhající nepříteli k dosažení státního nebo vojenského tajemství. A jistě každý příslušník naší armády si také plně uvědomuje současnou mezinárodní situaci a spolu s ní i to, že mluvení o bdělosti a ostrážitosti, že vyzývání k nejprísnejší ochraně všech skutečností státního a zejména vojenského rázu nesmí být pro nás jen prázdnými hesly, protože nejde jen o nějakou průpravu v bdělosti a ostrážitosti pro čas války, ale že jde v této situaci již dnes o tvrdý boj, který je veden se skutečným a zákeřným nepřítelem. Musíme mít stále na paměti, že američtí imperialisté, kteří věnují stamilionové částky dolarů na financování špiónů, vrahů a záškodníků, vysílaných do Sovětského svazu a do zemí lidové demokracie, plánovitě a intenzivně usilují o získání všech důležitých státních tajemství týkajících se zejména ozbrojených sil zemí socialistického tábora.

Je již dnes celkem správně chápán význam ochrany důležitých a tajných dokumentů, význam bdělosti a opatrnosti na příklad při hovorech s nepovolanými osobami a p. V tomto směru, i když ještě někdy příliš mechanicky a pasivně, projevuje se správná opatrnost a někdy až úzkostlivost v dodržování zásad utajení. Naproti tomu přes všechnu uvědomělost i dobrou vůli je ještě nedokonale chápán význam utajení při velení vojskům pomocí technických pojítek, ať při běžném denním služebním styku nebo při různých cvičeních. Tento nedostatek pramení převážně z nedostatečného chápání významu pomůcek pro kodování. Přes to, že velitelé a štáby jinak plně chápou všeobecný význam utajení při používání pomůcek pro kodování na technických pojítkách, je jejich bdělost podvědomě zeslabována a zatlačována vlivem ostatních objektivních příčin a okolností, jako jsou na př. časové termíny, soustředěný zájem jen o odborné splnění daného úkolu a p. V návalu odborných vojenských i vševojskových úkolů odsunují často štáby věci týkající se utajení na vedlejší kolej. Děje se tak proto, že zejména při cvičeních je pohlíženo na utajení velení jako na každý jiný učební úkol, při čemž je opomíjen faktor skutečného a i při cvičeních existujícího nepřítele. Za takového stavu dochází pochopitelně k porušování zásad utajení velení a k faktickému napomáhání nepříteli. Přitom je často na omluvu používáno argumentů pramenících z nezdravého názoru, že pomůcky pro kodování zatěžují velení, že je zpomalují a činí nepružným. Tento názor je pohříchu hodně rozšířen a je velmi nebezpečný, protože vede k tomu, že se pomůcek pro kodování nepoužívá soustavně a že právě v nejkritičtějších okamžicích je čas a snaha o rychlé zvládnutí úkolu stavěna výše než zájmy utajení velení; pomůcek pro kodování se používá nedokonale anebo se pomíjejí vůbec.

Je samozřejmou snahou dát vojskům do používání vždy pomůcky pro kodování takové, které by velení nijak nezatěžovaly, ovšem je třeba si zároveň uvědomit, že určitý vliv na rychlost velení, kodování zpráv má. Tento vliv nelze však v žádném případě úplně vyloučit a je nutno s ním reálně počítat. Na druhé straně však většina potíží při použití pomůcek pro kodování nepramení jenom ze samé jejich existence, nýbrž především z neznalosti jejich používání samými uživateli, z malé zručnosti a pružnosti, vyplývající z toho, že příprava a výcvik v používání pomůcek pro kodování jsou podceňovány.

Zásadně je třeba si uvědomit podstatný rozdíl v účelu a významu používání pomůcek pro kodování ve válce, v boji a mírovém velitelském styku ať již přímo v posádkách, ve výcvikových prostorech nebo při různých cvičeních.

V době války vtiskuje skutečné střetnutí s nepřítelem použití pomůcek pro kodování naprosto odlišný ráz od použití pomůcek pro kodování v míru. Ve válce a v boji je účelem pomůcek pro kodování zajistit, aby zprávy jimi zakodované byly pro nepřítele alespoň na určitý čas nesrozumitelné, t. j. aby odposlechem zachycené zprávy nemohl odkodovat nebo rozluštit a vyhodnotit v tak krátké době, kdy by ještě mohl na základě jejich obsahu provést účinná protipatření. To znamená, že v boji nám ve většině případů nebude na závalu, jestliže se nepříteli teprve po delší době podaří rozluštit některé kodované zprávy, na příklad za pět nebo více dní, protože za takovou dobu již nebude mít jejich obsah pro nepřítele význam, neboť situace už bude zcela jiná a opatření, která měla být podle obsahu zprávy provedena, budou již zpravidla dávno uskutečněna. Pomůcky pro kodování musí umožňovat především účelnou a rychlou manipulaci, někdy i na úkor jejich kryptologické bezpečnosti.

Naproti tomu dnes v mírovém velitelském styku mezi posádkami, ve výcvikových prostorech i při různých cvičeních vyžaduje situace, aby pomůcky pro kodování utajily zprávy dodávané technickými pojítky tak dokonale, aby nepřítel vůbec nemohl využít zachycených zpráv k vyhodnocení a získání jakýchkoliv informací o stavu naší bojové připravenosti.

Je nezbytně třeba, aby si právě dnes všichni naši velitelé a příslušníci armády jasně uvědomovali skutečnost, že na západních hranicích našeho státu stojí nepřítel, který se odposlouchavacími zařízeními i agenturní činností snaží získávat zprávy. Z toho vyplývá nutnost používat složitějších pomůcek pro kodování v míru než ve válce. V míru musí být používáno pomůcek pro kodování s daleko větší důsledností, a mají-li úplně utajit obsah hovorů, musí být dokonalé a po stránce kryptologické bezpečné. Má-li být tato podmínka splněna, nelze se nikdy vyhnout i složitějším a těžším systémům kodování. Z těchto důvodů není ani možno vždy při našich cvičeních plně využívat ustanovení Polního řádu o používání otevřené řeči, abychom nepříteli nedali možnost získat důležité poznatky o naší armádě. Tyto odchylky od ustanovení Polního řádu jsou vždy řešeny zvláštními nařízeními vydávanými před každým cvičením.

Je proto třeba počítat s tím, že pomůcky pro kodování používané dnes, v míru, budou někdy složitějších systémů a že práce s nimi bude náročnější. Jakmile si však uvědomíme onu naprostou nutnost používat jich za dané situace, nesmí v žádném případě dojít k tomu, aby jejich použití bylo považováno za ztěžování nebo zpomalování velení. Naopak

tato skutečnost musí nás všechny vést k tomu, aby byly radikálně odstraněny všechny příčiny, které stavějí použití pomůcek pro kodování do takového světla.

K zlepšení použití pomůcek pro kodování je třeba vymýtit některé zásadní chyby, které se při kodování nejčastěji vyskytují, a ukázat na jejich příčiny.

Nejvíce se tyto chyby projevují při používání základních pomůcek pro kodování, t. j. zejména hovorových tabulek, po případě tabulek kodů.

Všimněme si nyní některých běžných problémů používání hovorových tabulek, které jsou příčinou jejich špatného a v některých případech i nepřipustného používání a které pak někdy skutečně vedou k falešným názorům na používání těchto i jiných pomůcek pro kodování.

Jedním z nejzávažnějších nedostatků, které pramení právě z onoho podceňování významu utajení velení a všeho, co s ním souvisí, je nesprávný přístup důstojníků k důkladnému osvojení a poznání hovorových tabulek. K dokonalému seznámení s hovorovou tabulkou nestačí jenom pochopit její kodovací systém, po případě grafickou a technickou úpravu, ale je třeba daleko hlubšího prostudování, hlavně její slovní náplně, protože jedině toto studium umožní správné a účelné využití slovního fondu každé hovorové tabulky při sestavování zpráv. To je jednou z hlavních podmínek správného a rychlého využití hovorové tabulky a jedině to může dopomoci k rychlému a vhodnému sestavování a k podávání zpráv pomocí hovorových tabulek. Už jenom splněním tohoto základního požadavku dosáhne uživatel náležité jistoty a důvěry v hovorovou tabulku, které jsou předpokladem k další, rychlé a pružné manipulaci s ní. V opačném případě, při zanedbání tohoto požadavku, dochází k řadě dalších chyb a těžkostí. Uživatel, který dobře nezná obsahovou část tabulky, musí dlouho a pracně výrazy vyhledávat nebo přistupuje k hláskování výrazů, i když jsou tyto výrazy v tabulce obsaženy. To pochopitelně způsobuje velké ztráty času při sestavování, podávání i přijímání zpráv a dává možnost vzniku chyb při zakodování a dodávání takovýchto dlouhých zpráv. Na neposledním místě je dlouhými zakodovanými zprávami ohrožována i bezpečnost hovorové tabulky samé, neboť zbytečně velké množství kódů, z nichž je složena jedna zpráva, usnadňuje nejen luštění zprávy, ale bývá příčinou i prozrazení kodovacího systému.

Je tedy nutno znovu zdůraznit, že znalost obsahové části hovorových tabulek umožňuje přímo snadné a rychlé sestavení (přípravu) zprávy před jejím kodováním. To znamená, známe-li dobře možnosti využití slovního obsahu hovorové tabulky, můžeme kteroukoli zprávu určenou k zakodování upravit tak, aby bylo použito co nejvíce slov nebo i celých řčeních uvedených v hovorové tabulce. Takový způsob použití hovorových tabulek vede ke stručnému, konkrétnímu a jasnému sestavování zpráv. Přizpůsobování (příprava) zprávy podle možností hovorové tabulky nesmí však být prováděno násilně a musí být dbáno toho, aby smysl zprávy byl přesně zachován a nepřipouštěl jiného výkladu. Některé nové hovorové tabulky jsou dokonce upraveny k vhodnému využití slovního obsahu tím, že jsou v nich uvedeny kmeny nejčastěji se vyskytujících slov, které je možno upravit připojením příslušných koncovek podle potřeby.

Další důležitou podmínkou správného používání hovorových tabulek je odesílání a přijímání zakodovaných zpráv ať již formou hovorů nebo telegramů na technických pojítkách. Nejrychlejší a nejvýhodnější způ-

sob odesílání zpráv pomocí hovorové tabulky je umožněn přímým vedením kodovaného hovoru, to znamená, když odesílatel odesílá sám kodovanou zprávu přímo adresátovi. Jedině tento způsob přímého odesílání kodované zprávy může zabránit chybám vzniklým dopravou, zbytečným dotazům a dodatečným vysvětlováním a jediné takto je zaručeno rychlé odeslání kodované zprávy. Zakodovaná zpráva musí být odesílána tak rychle, takovým tempem, aby příjemce stačil zakodovaný text nejen zachycovat, ale současně odkodovávat. Potvrzením převzetí kodované zprávy příjemce musí současně potvrdit, že porozuměl otevřenému znění zprávy. Byl by na omylu ten, kdo by se domníval, že snad tento postup odesílání nebo přijímání zakodovaných zpráv je zdoluhavý, a zejména, že zatěžuje velitele a snadno by se mohl někdo domnívat, že dosáhne úspory času tím, že zprávu zakóduje a odevzdá ji k odeslání jako fonogram nebo telegram další osobě nebo přímo obsluze technického pojítka. Při použití tohoto způsobu odesílání kodovaných zpráv vypadá však namnoze skutečnost tak, že čas, který odesílatel takto pro sebe získal, je draze zaplacen opožděným doručením zprávy, která k tomu ještě bývá často zkomolena dopravními chybami. Nemohou-li velitelé za určitých okolností sami odesílat zakodované zprávy, je nutné, aby pověřili jejich odesláním některého z důstojníků svého štábu. Tento důstojník pak zprávu osobně zakodovává a odesílá a veliteli za správné a včasné odeslání osobně odpovídá. Vlastní odeslání zprávy může se pak uskutečňovat dvojím způsobem. Buďto čtením přímo z hovorové tabulky, kterýžto způsob vyžaduje větší praxe a zběhlost, anebo je-li dost času, tak, že zprávu převedeme do kódů nejprve na papír, znovu přezkoušíme správnost zakodování a pak ji teprve odesíláme. První způsob je ovšem rychlejší a musí být snadno každého důstojníka štábu, aby se k němu soustavným výcvikem a praxí dopracoval. Při přijímání zakodovaných zpráv dopouštějí se někteří příslušníci štábů ještě té chyby, že zakodovanou zprávu nejprve zachytí v kódech a teprve po ukončení hovoru ji převádějí do otevřené řeči. Tento způsob byl již příčinou mnoha nepřijemností, když totiž příjemce teprve dodatečně zjistil chybu v zakodování, zprávy nemohl odkodovat a nové spojení s odesílatelem nemohl pro obsazení pojítek dosáhnout.

Už jenom z uvedených nedostatků je vidět, že jde vesměs o nedostatky poměrně snadno odstranitelné a že jejich likvidováním musí být naprosto vymýcen názor, že jenom pomůcky pro kodování samy o sobě jsou břemenem nebo brzdou při velení. Vidíme, že ve skutečnosti je jen třeba důsledným výcvikem a neustálou praxí prováděnou při každé příležitosti nabývat zručnosti, jistoty a samozřejmosti v ovládání hovorových tabulek i ostatních pomůcek pro kodování a že je při tom třeba si neustále uvědomovat, že soustavné a uvědomělé používání pomůcek pro kodování je přímým a účinným projevem bdělosti a ostražitosti. Je při tom třeba samozřejmě počítat s počátečními těžkostmi při výcviku, které je však nutno překonat. Je samozřejmé, že zakodování a odeslání prvních deseti zpráv pomocí hovorové tabulky bude u každého jednotlivce těžší než zakodování a odeslání dalšího sta zpráv.

Je jisté, že nakonec i forma, kodovací systém a slovní, obsahová část hovorových tabulek hraje důležitou úlohu při jejich používání. Aby hovorové tabulky byly dokonalým, účelným a jednoduchým prostředkem pro odesílání zpráv technickými pojítky zastřenou formou, je nutné, aby velitelé a funkcionáři štábů, uživatelé těchto hovorových tabulek více uplatňovali své požadavky a připomínky při zpracovávání hovorových

tabulek, zejména co se týče slovní náplně a obsahu. Velitelé a příslušníci štábu mají sami nejvíce zkušeností v tom, které výrazy se při velení nejčastěji vyskytují a které najdou v hovorové tabulce největší uplatnění. Při sestavování jednotných hovorových tabulek, které slouží k vedení kodovaných hovorů mezi všemi druhy vojsk a služeb bez rozdílu, je třeba, aby zejména operační oddělení štábů uplatňovala své požadavky na doplnění potřebných výrazů. U tabulek pomocných (speciálních), které slouží k odesílání zpráv uvnitř jednotlivých druhů vojsk a služeb, musí návrhy na jejich slovní náplň ve vlastním zájmu zpracovávat štáb příslušného druhu vojska nebo služby. Jen takovým chápáním součinnosti při sestavování nových hovorových tabulek je možno vytvořit předpoklady k tomu, aby se zvýšila jejich účelnost, aby se upevnila důvěra v jejich spolehlivost a správnost a aby se tím podstatně zlepšilo i jejich používání.

Další příčinou, která má za následek velké časové ztráty při velení vojskům na cvičeních, zejména tehdy, kdy je procvičována dynamika boje, je to, že štáby dosud v malé míře používají možností, které jim skýtají tabulky kodů. Tabulky kodů jsou velmi výhodné pomůcky pro kodování, neboť urychlují odesílání rozkazů, nařízení a zpráv, zejména během vedení boje. Jejich veliká výhoda — značná úspora času při velení — je v tom, že jsou sestavovány na základě plánu boje, a mohou proto obsahovat ucelené rozkazy, nařízení i hlášení, které jsou v průběhu boje předpokládány a mohou být takto odesílány i jedním kódem. Hlavním požadavkem pro vydávání tabulek kodů je tedy co nejvhodnější výběr kodových textů, které bude s největší pravděpodobností možno použít. To vyžaduje těsné součinnosti zejména operačního oddělení se šifrovacími orgány. Je třeba, aby se tyto tabulky kodů co nejvíce vžily, a to je podmíněno opět zvýšeným zájmem velitelů a štábů o utajení velení.

Při používání ostatních pomůcek pro kodování, tedy kodované mapy, krycích jmen terénních předmětů, pseudonymů, volacích znaků a čísel funkcí, se v celku podstatné chyby nevyskytují. Je jen třeba pamatovat, aby vzájemné spojování všech těchto pomůcek pro kodování během hovorů, bylo vždy správně a účelně prováděno, neboť jejich vzájemným spojováním je možno na jedné straně dosáhnout rychlejšího a snazšího zakodování i dodání zpráv, ovšem na druhé straně při nesprávném spojování, může dojít k prozrazení té nebo oné pomůcky. Na př. nevhodným spojováním krycích jmen terénních předmětů s údaji kodované mapy a p.

Aby bylo zajištěno utajení při velení technickými pojítky, musí být kodovací systémy a jednotlivé pomůcky pro kodování v nepravidelných časových intervalech měněny. Kodovací systémy nesmějí být nikdy chápány staticky, jako neměnné věci. Setrvávat na jedněch, stálých a dlouhou dobu používaných kodovacích systémech, by bylo sice pro uživatele pohodlné, ale jistě by nebyl splněn hlavní účel pomůcek pro kodování — nebylo by plně zajištěno utajení odesílaných zpráv.

Jsou-li zaváděny nové kodovací systémy, je třeba, aby se rychle a úplně vžily. Ukázali jsme si, že používání pomůcek pro kodování je vždy jen otázkou výcviku a uvědomělého chápání jejich účelu. Proto je jen na uživateli, aby se snažili pochopit nové kodovací systémy vždy bez jakýchkoli předsudků a aby se jim naučili v nejkratší možné době. Tím, že se velitelé a štáby seznamují s různými kodovacími systémy, dosahujeme toho, že se jejich celková připravenost, pokud jde o pružnost a hbitost v používání pomůcek pro kodování, neustále zvyšuje.

šuje. Je třeba, aby všichni velitelé a funkcionáři štábů vždy pochopili, že změny kodovacích systémů a jednotlivých pomůcek pro kodování ztěžují a znesnadňují nepříteli jeho snahu o získání zpráv o naší armádě tím, že vylučují jakoukoli pravidelnost i vžitě zvyklosti při zastírání zpráv a tím hlavně nedovolují nepříteli, aby průzkumem technickými pojítky získal zpravodajský užitek.

Nakonec je ještě třeba zdůraznit, že pro rychlost kodovaného dorozumívání má velký význam kromě důkladné znalosti používání pomůcek pro kodování i důkladná znalost používání technických pojítek. Proto je třeba neustále provádět výcvik v používání pomůcek pro kodování při současném použití telefonu a radia i za ztížených podmínek (slabá slyšitelnost, rušení a p.). Jedině tímto způsobem získají velitelé a funkcionáři štábu potřebnou praxi ve velení technickými pojítky a splní tak jeden ze základních úkolů, který jim byl uložen rozkazem soudruha ministra pro letošní výcvikový rok. Čím lépe budou velitelé a funkcionáři štábů ovládat používání pomůcek pro kodování již dnes, tím lépe a rychleji budou schopni jich používat za války a tím lépe a důsledněji bude plněna i vojenská přísaha, pokud jde o ochranu a střežení státního a vojenského tajemství.