

TAJNO KOMANDOVANJE TRUPAMA

Iako su tajnost prenošenja poruka (naređenja, izveštaja, obaveštenja itd.), takozvano TKT, i odgovarajuća organizacija i taktika službe veze, jedne od glavnih komponenti obezbeđenja tajnosti komandovanja, nije to i sve ono što može na ovaj ili onaj način, u manjoj ili većoj meri pozitivno ili negativno uticati na tu tajnost. Postavlja se, dakle, pitanje šta je to još što može na odgovarajući način da naruši tajnost komandovanja? Ali, da najpre odgovorimo na pitanje šta je to tajnost komandovanja? Po našem mišljenju, tajnost komandovanja je *skup* mera i postupaka čiji je cilj da se od protivnika sakriju sopstvene namere i to od početnih ideja, razrade tih ideja i odluka, pa preko njihovog sprovođenja do krajnjih rezultata određene akcije (operacije, boja, borbe). Ako se pođe od toga da je to tačno, onda je sem organizacije i primene TKT i adekvatnih mera radi bezbednosti veza neophodan još čitav niz drugih mera i postupaka. Evo samo nekih primera. Nema sumnje da neadekvatno maskiranje i trupe i štabova, slabo i neadekvatno organizovane dezinformacije, neoprezna pisma vojnika i starešina u kojima se iznose podaci koji predstavljaju vojnu tajnu, nedovoljna opreznost u sprovođenju komandantskog izviđanja, na osnovu kojeg druga strana može da izvuče odgovarajuće zaključke, nedovoljno bezbedan rad administracije i sl., mogu da ozbiljno naruše tajnost planova i postupaka u komandovanju. Prema tome, i maskiranje, dezinformacija, cenzura, tajnost priprema štabova i trupa, kao i bezbedan rad administracije, pored TKT i službe veze, predstavljaju skup mera i postupaka kojima se obezbeđuje tajnost u komandovanju.

Očigledno je da se ni jedna od ovih mera i postupaka ne smeju potceniti, a još manje zanemariti i da od preciznosti regulisanja tih mera i postupaka, kao i njihovog sinhronizovanog i planskog usmeravanja ka istom cilju, dobrim delom zavisi i uspeh ili neuspeh u sprovođenju zamisli i odluke komandanta.

Silan razvoj elektronike, u koju se ulažu i ogromna sredstva i naponi, uticao je dominantno na razvoj sredstava veze, naročito posle drugog svetskog rata. Međutim, uporedo sa razvojem sredstava veze, razvijala su se i sredstva za njihovo prisluškivanje. Razvoj i povećane mogućnosti prislušne službe, a posebno radio-prislušne službe, uticali su na razvoj organa dekripterske službe, tj. službe koja se bavi otvaranjem tuđih šifrovanih poruka. Čitav taj razvoj, uz evoluciju savremenog komandovanja, učinio je da je problem očuvanja tajnosti sopstvenih poruka postao komplikovaniji i daleko ozbiljniji nego ranije. U vezi s tim biće korisno da se u najkraćim crtama izlože razvoj radio-izviđanja i dekriptiranja, kao i neki problemi bezbednosti veza i brzine u komandovanju i uticaj svih tih faktora na TKT.

Bez sumnje je da je radio-izviđanje, ili kako se negde taj problem kompleksnije naziva »rat talasa«, postalo jedan od dominantnih faktora koji opredeljuje mesto i ulogu TKT i bitno utiče na njegovu složenost. Od prvog svetskog rata, kada je ovo izviđanje imalo manje ili više karakter samoinicijative pojedinaca, ono se toliko razvilo da je u drugom svetskom ratu preraslo u dobro smišljenu i organizovanu akciju sa mnogobrojnim uspesima¹ koji su ponekad odlučujuće delovali na donošenje odluka, da bi u periodu posle drugog svetskog rata postalo sastavni i nezamenljivi činilac savremene obaveštajne i kontraobaveštajne službe.

Radio-izviđanje ili »rat talasa« je rat koji se nikom ne objavljuje, to je nevidljivi rat, rat bez početka i završetka, on nije vezan za granice, ni za vreme ni za prostor — on traje permanentno.

Njegove bitne komponente su: bežične veze, njihovo izviđanje (prisluškivanje), goniometrisanje i ometanje; radarske mreže, njihovo izviđanje i ometanje; ometanje daljinskog upravljanja raketama; televizijsko i telefaksimilsko izviđanje; radio-obmanjivanje i dezinformacije.

Sve te komponente radio-izviđanja su manje-više uspešno položile ispit u drugom svetskom ratu ili posle njega. To očigledno ukazuje na konstataciju da se danas već mora biti načisto sa činjenicom da nema sredstva veze koje nije moguće prisluškivati.² Time se ne misli reći da samo radio-izviđanje nema teškoća pa, čak i velikih problema, ali je očigledno da ono što je teškoća i nerešiv problem danas, ne mora to biti i sutra. Neshvatanje i nesagledavanje ovih činjenica u takvom svetlu može u određenoj situaciji naneti ogromne štete i nepovoljno uticati na razvoj određenih borbenih radnji.

¹ Da uzmemo samo na dohvat nekoliko primera:

Prema sopstvenim izvorima, američka radio-izviđačka služba otkrila je pripreme Japanaca za napad na Perl Harbur 1941. godine. Napad Japanaca je potpuno uspeo, jer američka komanda nije (ne znaju se stvarni razlozi) preduzela odgovarajuće mere. Taj slučaj je dugo bio, a i danas je, predmet diskusija u Kongresu SAD.

Prisluškivanjem francuskih radio-veza 1939/40. nemačka radio-izviđačka služba uspela je da otkrije raspored francuskih snaga između reka Some i Sene i južno od Some, što su pred napad na Veganovu liniju bili vrlo dragoceni podaci. Nemačka podmornica U-66 koja je kod ostrva Kapverd 1944. godine emitovala poruku svega 15 sekundi, bila je za to vreme snimljena od 25 savezničkih goniometara i nakon toga otkrivena i potopljena.

Alfred Jodl na procesu u Nirnbergu izjavio je: »... Osnovnu količinu obaveštajnih podataka do 90%, crpili smo iz materijala radio-izviđanja i saslušavanja zarobljenika. Radio-izviđanje igralo je osobitu ulogu u samom početku rata (misli na 1941. godinu i napad na SSSR — primedba V. V.), ali nije gubilo svoj značaj ni do poslednjih dana...«

Iz memoara generala Lotara Rendulica vidi se da je nemačka radio-izviđačka služba igrala značajnu ulogu u borbi njihovih snaga protiv NOVJ i da su nemačke komande svoje odluke dobrim delom zasnivale na rezultatima radio-izviđanja.

² Amerikanci su se za vreme hladnog rata u Berlinu, kroz podzemne kanale priključili čak i na telefonske linije u Istočnom Berlinu, na koje su, pored ostalog, bile vezane i jedinice Sovjetske armije i prisluškivale celokupan saobraćaj preko svih telefonskih kanala. (*Der Spiegel* od 26. II 1964. godine).

Nije nikakva tajna da se u mnogim zemljama, prema njihovim mogućnostima, na razvoj radio-izviđačke službe daju velika finansijska sredstva³. Jer, efikasnost prisluškivanja, pre svega, zavisi od sredstava kojima prislušna služba raspolaže i od ljudi koji u toj službi rade. Sredstva kojima radio-izviđačka služba raspolaže moraju biti tehnički najsavremenija ili, u najmanju ruku, na nivou tehnike onog koji se prisluškuje. A ti, obično profesionalni uređaji (prijemnici, panadapteri, radio-goniometri, magnetofoni, analizatori impulsa, itd.) zbog preciznosti, stabilnosti i automatizma vrlo su skupi. Od kadrova koji u toj službi rade ne traži se samo poverljivost — iako je to važan kriterijum, s obzirom da ni samo postojanje ove vrste delatnosti niko javno ne priznaje — već, pre svega, velika stručnost, umešnost i iskustvo. Radio-izviđačke jedinice i ustanove se zbog maskiranja nazivaju raznim imenima, a ponajčešće se maskiraju imenima jedinica veze. One se nalaze u svim komandama od divizija (blisko izviđanje) pa do vrhovnih komandi (strategijsko radio-izviđanje).

Za radio-prisluškivanje, sem stacionarnih prislušnih i goniometrijskih centara, sa raznim sredstvima i na raznim odstojanjima, a zavisno od sredstava veze koja se prisluškuju i njihovih karakteristika, koriste se i razne letelice⁴, plovni objekti, baze na tuđim teritorijama, pa čak i diplomatska i druga predstavništva u stranim zemljama. Posebne vrlo široke mogućnosti u pogledu radio-izviđanja pružaju sateliti koji se danas tako intenzivno izbacuju u orbitu oko zemlje. Prislušni centri su vrlo moderno opremljeni, često sa uređajima za automatski prijem svih vrsta emisija i direktno su vezani sa goniometrijskim stanicama radi utvrđivanja mesta gde se nalazi radio ili drugo sredstvo čiji se signali prisluškuju (izviđaju).

Prisluškivanje žičnih veza obično spada u domen specijalno obučeni i tehnički opremljeni izviđačkih grupa. I tehnika kojom se prisluškuju žične veze je mnogo napredovala, tako da je, na primer, prisluškivati i ovu vrstu veza moguće bez fizičkog priključka na žični kanal koji se prisluškuje. Radi toga i ova vrsta veza postaje sve manje bezbedna.

Takvim svojim razvojem i ulogom prislušna služba, a posebno radio-izviđanje, postali su jedan od bitnih faktora koji utiče na neophodnost da se velika pažnja pokloni prenošenju poruka.

³ Prema izjavama prebeglih američkih pripadnika Agencije nacionalne bezbednosti SAD Mičela i Martina na radio-izviđanje i dekriptiranje troši se godišnje oko pola milijarde dolara (TASS od 6. IX 1960. godine). Slično je i u Austriji: »...Po ugledu na američki i zapadnonemački primer organizovan je u okviru austrijske armije veliki aparat tajne službe — radio-špijunaže, prislušna služba i goniometrijske stanice koje godišnje troše ogromna sredstva...« (List *Volkstimme* u broju od 12. januara 1964. godine).

⁴ Prema već pomenutoj izjavi prebeglih Amerikanaca, a i prema podacima štampe, takav je slučaj sa avionom U-2 i drugima. Septembra 1958. godine američki avion C-130 namerno je povredio sovjetsko-tursku granicu da bi se došlo do podataka o rasporedu sovjetskih radarskih stanica na tom području. Dok su sovjetske radarske stanice pratile i obaveštavale o letu tog aviona, bile su istovremeno intenzivno praćene i snimljene od strane američke radio-izviđačke službe. Ove operacije, prema izjavi prebeglih, Amerikanci nazivaju *ELINT* (elektronsko izviđanje).

Drugi faktor, kojemu je baš radio-izviđanje svojim velikim razvojem omogućilo široko polje rada, jeste služba dekriptiranja. Od rada izuzetno nadarenih pojedinaca, ova služba se, zahvaljujući modernim matematičkim disciplinama i razvoju kibernetike i elektronike, razvila u savremenu nauku.

Pod dekriptiranjem se podrazumeva otkrivanje šifrovane poruke (telegrama, pisma, govora), ali bez posedovanja šifre. Znači, dekriptier raspolaže samo šifrovanim telegramom. Međutim, on je za svoj rad obezbeđen i drugim podacima koje mu stavlja na raspolaganje radio-izviđanje (na primer, mesto stanice koja je predala i koja je primila i dr.), a vrlo verovatno i nekim drugim podacima obaveštajne prirode (koja je komanda u pitanju, imenima starešina, podacima o situaciji i slično).

Govoriti o uspesima dekripterske službe vrlo je teško. Očigledno, oni predstavljaju najveću državnu tajnu i mogu da dođu u javnost isključivo nesmotrenošću ili hvalisavošću pojedinaca. No, poznato je da su Amerikanci, baš zahvaljujući dekriptiranju, saznali za već pomenuti napad Japanaca na Perl Harbur i da su saveznici prilično »redovno« pratili poruke nemačkih pomorskih snaga u drugom svetskom ratu. Poznati su i mnogi primeri uspešnog rada kontraobaveštajnih službi baš zahvaljujući dekriptiranju šifrovanih telegrama. Iz pomenutih izjava Mičela i Martina, prebeglih američkih matematičara — dekriptera, vidi se da Amerikanci dekriptiraju navodno poruke iz 23 zemlje, među kojima je mnogo i njihovih saveznika.

Ono što valja posebno podvući, a što je značajno uzeti u obzir pri oceni kako čuvati sopstvene poruke, to je bez sumnje vrlo visok naučni kvalitet kadrova koji se danas bave dekripterskim poslovima (ponajčešće sa akademskim obrazovanjem), njihov relativno velik broj⁵, pomoć koju im pružaju današnje nauke, naročito visok stepen razvoja modernih matematičkih disciplina, filologija, pre svega kroz statističko posmatranje karakteristika jezika, kao i tehnička opremljenost savremenim elektronskim računarima, čije su praktične mogućnosti upravo fantastične. Savremeni računari sposobni su da obave nekoliko hiljada računskih radnji u sekundi. Najbrža mašina u SAD u stanju je da izračuna u svakoj sekundi 20.000 zbirova desetocifrenih jednaknih brojeva. Prema tome, ti elektronski računari (ili kako ih novinari i nestručnjaci često nazivaju »elektronski mozgovi«) omogućuju da se danas pristupa i onim poslovima kod kojih bi ručni rad trajao nesagledivo dugo.⁶ Ono što je nekad bila utopija i iluzija, postalo je stvarnost.

⁵ Prema izjavama Mičela i Martina, u Agenciji nacionalne bezbednosti SAD radi oko 10.000 lica (TASS od 6. IX 1960. godine).

⁶ Elektronski računari se često upoređuju sa mozgom. Nema sumnje da je takvo mešljenje ipak preterano. Dok mozak može preuzeti funkciju računске mašine, obratno to nije moguće. Mozak radi neukalupljeno, a mašina je sposobna samo za strogo formalne i logične operacije. Osnovna odlika računara je upravo fantastična brzina računanja.

Samo dva primera radi očiglednosti. Za rešenje jednog sistema linearnih jednačina sa 26 nepoznatih, nekoliko vrsnih matematičara radilo bi više meseci, a elektronski računar bi to svršio za svega 30 minuta.

Ili, savremeni elektronski računari sposobni su da izvrše milion sabiranja u sekundi, a jedan knjigovođa sa običnom stolnom računskom mašinom može da izračuna najviše 1000 operacija u jednom danu.

Za razliku od ranijeg shvatanja da je dekriptiranje stvar isključive obdarenosti i hobija pojedinaca, ono je danas toliko razvijeno da predstavlja nov kvalitet, bez kojeg se ne može razmatrati problem tajnosti komandovanja, a posebno bezbednosti poruka.

Pošto sve veća aktivnost na polju dekriptiranja traži ogromna materijalna sredstva i velik broj odgovarajućih stručnjaka, to ovu službu mogu da u širim razmerama razviju uglavnom samo velike i bogate zemlje.

Treći faktor koji bitno opredeljuje mesto i ulogu TKT jesu sredstva veze koja su sva, više ili manje, ranjiva u odnosu na bezbednost otvorenih poruka koje se preko njih upućuju.

Kada je reč o tome da nema sredstva veze koje nije moguće prislušivati, što je po našem mišljenju sasvim tačno, potrebno je ipak imati u vidu bezbednosne karakteristike pojedinih sredstava veze koje, istine radi, nisu sve jednako neotporne u odnosu na prislušnu tehniku i njene mogućnosti. Dakle, pri opredeljenju za ovo ili ono sredstvo veze bitnu ulogu mora da ima saznanje o savremenosti i opremljenosti u prislušnoj tehnici druge strane.

Pri razmatranju koja su sredstva veze bezbednija, obično se, sasvim normalno i pravilno, čini ovakav poredak: kurir, žične telegrafске veze, žične telefonske veze, radio-relejne veze i tek na kraju radio-sredstva, koja se, opet, međusobno čak i umnogome razlikuju.

Međutim, nije i u svakoj situaciji tako. Očito je da određena taktičko-operativna situacija ponekad i značajno i bitno utiče na izneti poredak. Ako, na primer, dejstvuju ubačene neprijateljske izviđačke i diverzantske grupe, mogu kurirati i žična veza sa svojim otvorenim porukama biti čak manje bezbedni od nekog drugog sredstva veze.

U bezbednosnoj proceni nekih sredstava veze ima i proizvoljnih, pa i pogrešnih mišljenja i ocena. Ponekad greše čak i stručnjaci veze. To se, pre svega, odnosi na radio-relejne veze i UKT sredstva koja se smatraju bezbednijim nego što u stvari jesu. Rasturanje snopa u radio-relejnim vezama je veće i jače nego što se to obično pročita u karakteristikama tih uređaja. Slično je i sa signalom UKT koji se ne mora čuti na 5 km, ali se dobro čuje na primer na 200 km.

Za starešine je, pak, naročito važno da znaju tačne podatke o bezbednosnim karakteristikama sredstava veze, kako bi svoje poruke poveravali onim sredstvima koja u određenoj situaciji pružaju najbolju bezbednost. Svaka iluzija o sigurnosti samog sredstva veze može biti vrlo štetna.

Iz iznetih se razmatranja vidi koliko je važno da starešine vode računa o tome kakvim sredstvima i kakvim kanalima veze obavljaju razgovore ili, pak, upućuju poruku i u nekoj borbenoj ili drugoj situaciji. Na izbor sredstava utiče komandni stepen i jednog i drugog korespondenta. Svaki šablon, s jedne, ili zatvaranje očiju pa »neka ide kako ide, samo da stigne na određeno mesto«, s druge strane, mogu da prouzrokuju fatalne greške, koje se najčešće teško popravljaju.

U savremenom ratu postoji još jedan veoma značajan faktor koji se ni u kom slučaju ne može zanemariti u razmatranju naše teme, a to je brzina u komandovanju. Taj faktor je, u stvari, ponajviše kompli-

kovao problem TKT. Sama za sebe tajnost još bi se i mogla obezbediti, ali je mnogo komplikovanije da se neka poruka, zapovest, izveštaj i sl. brzo ili čak vrlo brzo nekome uputi, a da se pri tome obezbedi odgovarajuća tajnost. Potreba tajnosti se povećava što je komanda višeg ranga. Međutim, i to i pitanje koja komanda ima veću potrebu u pogledu brzine naređivanja i obaveštavanja su ipak relativni pojmovi, a kako će biti u praksi zavisi od konkretne situacije i značaja akcije koja se izvodi.

Postavlja se pitanje kako u svetlu navedenih činjenica sačuvati u tajnosti poruke koje se upućuju između raznih komandi? Kakva su rešenja mogućna da se zaštiti tajnost tih poruka?

Ako se ne uzme u obzir lično kontaktiranje starešina, tajnost poruka može se sačuvati, pre svega, primenom šifre, pogotovo kad je reč o određenom možda i većem broju poruka, a posebno kod viših komandi. Mogućnosti u tom pogledu, kao i sama tehnika šifriranja učinili su ogroman korak uz pomoć u prvom redu elektronike. Klasično šifriranje se danas sve ređe primenjuje u svom prvobitnom obliku. Njegovo mesto sve više preuzimaju moderna šifarska sredstva — *šifarske mašine* raznih vrsta i namena. Međutim, ni danas se obično ne menjaju neka bitna kriptografska svojstva i ranije korišćenih šifara. Mehanizacijom šifrovanja postižu se dve bitne i veoma važne stvari: prvo, povećavaju se mogućnost i kapacitet šifrera i šifarskih sredstava u pogledu količine šifrovanih poruka uz daleko manji zamor ljudstva i, drugo, dobija se u brzini, a to znači da se ide ukorak sa potrebama savremenog komandovanja. No, i među savremenim šifarskim mašinama ima velikih razlika u pogledu pomenutih mogućnosti. One se mogu globalno podeliti u dve grupe: *šifarske mašine za rad u lokalni* i *šifarske mašine za direktan rad na liniji*. Kod prvih se određena poruka najpre mašinski šifruje u šifarskom centru, pa tek onda se preko centra veze predaje drugom korespondentu, kod koga se opet u šifarskom centru mašinski dešifruje, pa tek onda predaje adresatu. Kod drugih — a to su uglavnom šifro-teleprinteri ili teleprinteri sa dodatkom za šifriranje teleprinterskih signala (preko tt ili radio-kanala) — poruke se automatski šifruju, odnosno kod primaoca dešifruju. Međutim, ova druga sredstva imaju i svoje slabe strane. Pre svega, neophodni su dobri ili odlični kanali veze, a radi relativne glomaznosti pa, delimično, i skupoće ne mogu se koristiti u nižim jedinicama.

Šta znači ova teškoća u pogledu korišćenja u nižim jedinicama? Ona znači da niže jedinice vrlo često ili ne mogu uopšte ili mogu samo retko da koriste ova danas savremena kriptografska sredstva. Dalje, iako je postignuta relativno velika brzina kod šifarskih mašina, ona još uvek ne zadovoljava u potpunosti potrebe komandovanja u tim nižim komandama, gde se traže neposredna i vrlo brza reaganja.

Zbog svega toga se u nižim komandama još uvek najčešće koriste razna »papirnata« sredstva kao što su: kodne tablice, tablice razgovora i sl. Vojne starešine, iz sasvim shvatljivih razloga, daju otpor i prigovore upotrebi takvih dokumenata, smatraju da se pomoću njih sporo radi, kao i da predstavljaju anahronizam u sistemu savremenog komandovanja. Iako su takva mišljenja sasvim tačna, postoje dve očigledne činjenice o kojima se mora voditi računa. Prvo, da se sve *ne sme*

otvoreno prenositi, i drugo, da *drugih mogućnosti često nema*. Na mogućnosti ćemo se još jednom, kasnije, vratiti. Očigledno je da se ta »papirnata« dokumenta tajnog komandovanja trupama na sadašnjoj etapi razvitka kriptografskih uređaja ipak moraju prihvatiti. Problem je u tri stvari koje se ponajviše zanemaruju, a koje su u TKT veoma vredne pažnje.

Prvo, usvajanje i izgrađivanje određenog *kriterijuma* o tome šta je na određenom komandnom nivou tajna, a šta nije, tj. šta neprijatelj može da iskoristi za protivakciju i šta od njega treba po svaku cenu sakriti, a šta ne, uzimajući pri tom u obzir i vreme i prostor i neprijateljeve mogućnosti. Međutim, nužno je napomenuti da svako unošenje šablona u taj kriterijum može samo da nanese štete. Dveju jednakih situacija neće biti.

Drugo, *prilagođavanje i konkretizovanje* sadržaja tih »papirnatih« dokumenata da što više odgovaraju određenoj situaciji i konkretnoj potrebi, jer je šablon ono što najčešće onemogućava upotrebu takvih dokumenata, ali da se uz to vodi računa o kriptografskoj sigurnosti, o čemu treba obavezno konsultovati nadležnog šifarskog starešinu.

Treće, stvaranje *rutine* kod starešinskog kadra u izrađivanju adekvatnih dokumenata prilagođenih konkretnoj situaciji i njihovoj primeni. Nepostojanje rutine najčešće je uzrok nekorišćenja tih dokumenata. U tome vojne škole i redovna obuka trupe i štabova igraju najvažniju ulogu. Kada je reč o primeni, neophodno je da se vodi računa o njenoj povezanosti sa sistemom komandovanja i komandnim jezikom, jer je očigledno da korišćenje dokumenata TKT ne trpi *suvišnosti* u komandnom jeziku.

Da se ponovo vratimo na mogućnosti rešenja problema TKT u nižim jedinicama, jer starešine su u pravu da ta »papirnata« dokumenta nisu potpuno rešenje. Pravo rešenje je u stvaranju uređaja za šifriranje govora. Njihova upotreba bila bi mnogostruko mogućna. Oni bi se mogli koristiti i za žične i bežične veze, ugraditi u telefone ili telefonske centrale ili, pak, kao poseban dodatak za priključak na razna sredstva veze. Za njihovo korišćenje nije potrebno specijalno ljudstvo, sem za održavanje, a rukovanje je veoma jednostavno. Znači, taj problem mora i jedino može da reši opet tehnika.

Široka naučna istraživanja za rešenje tog problema odvijaju se u mnogim razvojnim laboratorijama širom sveta. Ima, čak, već i nekoliko praktičnih ostvarenja. No, treba konstatovati da do sada poznati sistemi šifriranja govora ne predstavljaju u bezbednosnom pogledu neka naročita ostvarenja.

Koliko je danas u svetu opšte poznato u pogledu tehničkih postupaka koji se primenjuju, postoji nekoliko vrsta šifriranja govora. Najprostiji način je pomoću *invertora*, a sastoji se u tome da se govorni spektar međusobno invertira na taj način što se najviše govorne učestanosti premeštaju na mesta najnižih i obratno. Nešto bolji je sistem *skrembliranja* (permutacija) kod kojeg se govorni opseg podeli u više podopsega koji se između sebe permutuju, a unutar podopsega i invertiraju. Dalje, postoji i opštepoznati metod *maskiranja šumom* u kojem se korisni signal i smetnje (obično je to beli šum sa potpuno haotičnim varijacijama i po vremenu i sa uniformnim spektrom duž frekventne

ose) šalju kroz zajednički kanal i to tako da srednja snaga šuma bude veća od srednje snage korisnog signala kako bi šum mogao potpuno maskirati poruku.

No, svi ti sistemi, kako je već rečeno, ne predstavljaju rešenja koja bi u pogledu kriptobezbednosti zadovoljila TKT. Da bi se na tom planu dobila iole sigurnija ostvarenja, nužna su, pre svega, dugotrajna i svestrana analiza sopstvenog govornog jezika i, naravno, odgovarajući tehnički metod — velik broj vrlo stručnih kadrova i velika finansijska sredstva.

Sudeći po svemu što je rečeno, izgleda da će istovremeno sa praktičnim ostvarenjem upotrebljivog uređaja za šifriranje govora biti najvećim delom rešeno i ono što se danas naziva problemom TKT.

Međutim, sasvim je razumljivo da konstatacija o tome da tehnika treba da konačno i najefikasnije reši problem TKT ne daje pravo starešinama da potcene »papirnata« dokumenta, jer će ona još dugi niz godina biti jedino moguće rešenje. Osim toga, ako se raspoloživa sadašnja sredstva i usvojeni metodi vešto i pravilno koriste, sasvim je sigurno da se na svim stepenima komandovanja može obezbediti najneophodnija tajnost u prenošenju poruka. Ukoliko se starešine više i sistematičnije navikavaju na rad sa dokumentima koji obezbeđuju tajnost i da biraju ono sredstvo za vezu koje najbolje odgovara konkretnoj situaciji, imajući uvek u vidu i zahteve u pogledu tajnosti, utoliko mogu biti sigurnije da će poruke koje šalju ostati nepoznate neprijateljevim organima bar onoliko koliko to traži izvršenje zadatka. A što se tiče brzine u korišćenju dokumentima TKT, ona zavisi, pre svega, od toga koliko su se starešine u svakodnevnom radu navikle da se njima koriste, koliko su u tome okretne i brze, koliko je taj deo njihovog posla u svakodnevnoj praksi trupa, štabova i škola razvijen do automatizma. I ne samo u pogledu primene dokumenata TKT, već i svih drugih mera i postupaka, jer samo kad se sve to zajedno majstorski postavi i primenjuje predstavlja čvrst bedem protiv stalnog i pedantnog delovanja savremene radio-izviđačke i dekripterske aktivnosti. Sačuvati u tajnosti sopstvene namere i stanje, već je upola izvršen zadatak.

Pukovnik

Vlado VALJAN