O KRIPTOGRAFSKOJ ZAŠTITI VEZA U ELEKTRONSKIM DEJSTVIMA

U inostranoj štampi sve češće se razmatraju problemi elektronskih dejstava (ED). Pri tome se stalno ističe korisnost takve aktivnosti, koju, navodno, primenjuju mnoge zemlje, posebno velike i tehnički visoko razvijene sile, kod kojih je ona sveobuhvatna, odnosno data na širokom planu.

Često se tvrdi da su ova dejstva, započeta u toku drugog svetskog rata, nastavila nesmanjenom žestinom svoj razvoj i usavršavanje. Za što potpuniji uspeh ove delatnosti široko se koriste dostignuća nauke i angažuju visoko kvalitetni i stručni kadrovi svih nivoa, pa i naučnici iz mnogih oblasti.

Interesantno je da se otvoreno govori o tome da su za ovakve poduhvate potrebna ne samo velika materijalno-novčana sredstva, odnosno najsavršenija tehnika za otkrivanje, ometanje, prisluškivanje, obmanjivanje, itd., već i veliki broj dobro obučenih ljudi. Obuka ovog kadra je vrlo duga, složena i skupa. Da bi se uhvaćeni materijali mogli brzo i stručno obraditi i koristiti, nužni su i neprekidni pratioci ED: analitičke, prevodilačke i dekripterske službe, koje vrše obradu uhvaćenih materijala.

Pošto ćemo se u ovom članku uglavnom ograničiti samo na jedan deo protivelektronske zaštite prenosa informacija, odnosno na kriptografsku zaštitu veza, to ćemo se prethodno zadržati na nekim delatnostima iz okvira ED, koje izazivaju ili uslovljavaju ovakvu vrstu zaštite. Radi se prvenstveno o RI svih vrsta veze i hvatanju otvorenih, kodiranih i šifrovanih informacija, a zatim o njihovoj obradi — prevođenju, analizi i dekriptiranju.

Za većinu zemalja bitno je u ovom momentu da ne mogu i ne smeju biti nezainteresovane, a još manje nemarne prema saznanju da su ili da eventualno mogu biti izložene takvim dejstvima.

Više se i ne krije da je RI, kao deo ED, delatnost ofanzivne prirode i da spada u opšte pripreme za određene ciljeve i »slučajeve«. Za ovo se iznalaze razna opravdanja, pa čak i zvanična, da je to neophodna mera bezbednosti i predostrožnosti. Njenom primenom je potrebno detaljno izučiti vrstu materijala, sisteme, vrste i kapacitete veza, kao i drugih elektronskih instalacija, kako bi se došlo do što više tajnih podataka iz svih oblasti života i rada zemlje prema kojoj su ovakva dejstva usmerena. Nebudnost u radu i razni neoprezni postupci pri korišćenju sredstava veze sigurno da prisluškivaču nude izvrsne mogućnosti za dobijanje takvih podataka.

Iz gotovo svakodnevnih napisa u štampi se vidi da se prisluškivanje vrši sa kopna — stacionarno ili sa vozila, sa mora — pomoću specijalno opremljenih brodova i čamaca, iz vazduha — pomoću helikoptera, aviona i balona, a u novije vreme i pomoću raznih satelita. Prislušni uređaji su vrlo osetljivi, selektivni, maksimalno pouzdani, rade na svim frekvencijama, automatizovani su i osposobljeni za programiranu obradu uhvaćenih podataka i njihov brz prenos. »Domet« im je gotovo neograničen, jer primaju sve radio-signale koji do njih dopru, što omogućava da određeni prostori budu pod stalnom i neprekidnom kontrolom.

Prema najnovijim podacima, predviđanjima i pretpostavkama, ispituju se mogućnosti da se, pored ostalog, i buduće platforme u kosmosu uključe u sistem radio-izviđanja i prisluškivanja.

Kada se detaljnije razmotri snaga RI službi, njihove mogućnosti i aktivnosti, nameće se zaključak da je vrlo teško ili nemoguće izbeći njihovom radu i da će sve ono što je emitovano preko radija i radio-relejnih sredstava veze biti, najverovatnije, uhvaćeno — uprkos preduzimanju najrazličitijih tehničkih i taktičkih mera za zaštitu veza, odnosno prenosa informacija.

Imajući sve ovo u vidu, može se ozbiljno prihvatiti tvrdnja da se danas u svetu intenzivno izviđaju, ako ne sve, a ono barem sve važnije radio, radio-relejne i žične veze. Iluzorno bi bilo misliti da je bilo koja zemlja od toga pošteđena.

O radu i uspehu dekripterskih službi, kao i koji se sve šifarski sistemi uspevaju (i pod kojim uslovima) dekriptirati, vrlo malo se i nedovoljno konkretno govori, što je sasvim i razumljivo. Međutim, dostupni podaci, mada uopšteni i nepotpuni, potvrđuju pretpostavke da ti uspesi nisu mali. Na takav zaključak navode i najsavremeniji tehnički i elektronski uređaji za analizu i dekriptiranje šifrovanih poruka, kao i angažovanje mnogobrojnog visokostručnog kadra. Najzad, kada ne bi postojao određen uspeh u dekriptiranju, ne bi imalo

nikakve svrhe ni hvatanje šifrovanih telegrama, koje se, kao što je poznato, temeljito sprovodi.

O ED i kriptografskoj zaštiti postoje, između ostalih, i dva rasprostranjena mišljenja koja posebno idu naruku prisluškivačima. Na osnovu prvog mišljenja, radio-izviđačke, analitičke, dekripterske i obaveštajne službe su tako dobro opremljene u kadrovskom i tehničkom pogledu da su, tako reći, svemoćne, da im gotovo ništa ne promiče, da često više njih dejstvuju planski, objedinjeno i da — putem razmene podataka i informacija — izviđaju i otkrivaju. Prema tome, nema svrhe ni potrebe da se bilo šta krije, barem ne preterano pošto će svakako biti otkriveno. U takvoj situaciji »jedina i efikasna« protivmera je brzina i jedinstvo u komandovanju, donošenju i sprovođenju odluka.

Ovakve teorije, pored ostalog, spadaju u kategoriju psihološkog rata radi dezorijentacije, demoralizacije, stvaranja defetizma i umanjivanja napora za organizovanje i uspešnu zaštitu sopstvenih veza, vojnih i drugih tajni uopšte. Takve teorije i shvatanja su vrlo opasne, jer ugroženu zemlju čine bespomoćnom i stvaraju utisak da su svi napori i mere bespredmetni i nepotrebni.

Drugo mišljenje se ogleda u potcenjivanju mogućnosti i zanemarivanju uspeha u prikupljanju i korišćenju podataka putem RI i dekriptiranja, njegovog značajnog uticaja na uspešno odvijanje borbenih dejstava, te da se sve to veštački i nepotrebno uveličava, itd.

Ovakvi stavovi mogu imati za posledicu manju opreznost, posebno pri upotrebi radio-sredstava, korišćenju slabih šifara, a time, objektivno, idu naruku i stvaraju lakše uslove radio-izviđanju i dekriptiranju.

Očito je da su oba ova i njima slična mišljenja neprihvatljiva i direktno štetna za jednu vojnu organizaciju.

II

Iskustva iz NOR-a, naročito u njegovim početnim fazama, najbolje pokazuju šta znači neiskustvo u kriptografskoj zaštiti veza i korišćenje slabe i nesigurne šifre. Razvijenoj i dobro opremljenoj nemačkoj RI i dekripterskoj službi nije bilo teško da uspešno izviđa i vrlo brzo dekriptira, bolje reći pročita, mnoge naše telegrame. Nemci su uspevali da u svojim dnevnim zapovestima citiraju naše šifrovane telegrame. Nije bio redak slučaj da se i otvoreno komandovalo, odnosno vršio prenos tajnih informacija preko radio-stanica.

Sve ovo koristilo je umnogome nemačkom komandovanju, jer su to bili podaci iz prve ruke, verodostojni i prikupljeni na najbrži način.

Razne publikacije govore o posledicama upotrebe slabih šifara u izraelsko-arapskom sukobu 1967. godine. U njima se tvrdi da su Izraelci posedovali šifre pojedinih arapskih zemalja, što nije isključeno, no pre bi se moglo reći da su oni uspevali da im pojedine šifarske sisteme dekriptiraju, što u suštini ne menja stvar. Međutim, bitna je i poučna činjenica da su Izraelci, sistematskim i temeljnim praćenjem arapskog područja nizom godina, došli do gotovo tačnih podataka o namerama, mogućnostima, snagama, itd. svake arapske zemlje. Ne samo da su znali oznaku, formaciju i broj jedinica, naoružanje, brojno stanje, obučenost i kvalitet ljudstva i materijalno-tehničkih sredstava, raspored jedinica u borbenom poretku, pravac dejstva, sisteme veza i sve ostalo što je od značaja za vođenje rata, već i običaje, efikasnost, raspored rada i druge »sitnice« komandi i jedinica, pa i lične osobine mnogih pojedinaca (imena, navike, glas i naglasak, mentalitet, ponašanje na korišćenom sredstvu veze i druge karakteristike potrebne za lažno predstavljanje i imitiranje određenih lica). Naglašava se da su naročito raspolagali preciznim podacima o pilotima, članovima posade tenkova, o posluzi sredstava veze, raketnih jedinica i drugih osetljivih mesta. Očigledno je da se do ovako tačnih podataka može doći samo sveukupnom obaveštajnom delatnošću. Pretpostavlja se da je dobar deo, ako ne i najvažniji, tih podataka i informacija dobiven preko RI i prisluškivanjem svih vrsta. Jasno je i to da se do ovakvih podataka ne dolazi odjednom, već postepeno. Izraelci su takve podatke svakodnevno dobijali, pored ostalog, i praćenjem saobraćaja na sredstvima veze arapskih zemalja.

Zbog toga, znatan deo zasluga za celokupan vojni uspeh Izraelaca ide na konto ED. Nije nevažna i činjenica da mnogi Izraelci odlično vladaju ne samo arapskim jezikom, već i pojedinim njegovim dijalektima, naročito pripadnici nekih specijalizovanih službi. Sve je to doprinelo da su mnoge primljene — uhvaćene podatke od kapitalnog značaja mogli odmah da koriste, bez potrebe da ih prethodno prevode.

Analitičari dokazuju da je ovo, pored nedograđenosti sistema veza i načina njihovog korišćenja, jedan od najvažnijih činilaca postignutog izraelskog iznenađenja.

Mnoga iskustva, od kojih su samo neka ovde pomenuta, navode na razmišljanje kako sačuvati u tajnosti ono što je najbitnije.

Kao što je već izneto, taktičke i tehničke mere koje se preduzimaju, smanjenje snage, lažni saobraćaj i sl. delimično otežavaju RI i dekriptiranje, ali mu se ne mogu uspešno suprotstaviti.

Stoga mnogi smatraju da jedna od prvih mera za umanjivanje uspeha radio-izviđanja i prisluškivanja jeste ujednačavanje kriterija o značaju zaštite tajnih informacija i obezbeđenju discipline u saobraćaju pri korišćenju sredstava veze. Mere opreznosti i budnosti, kako poslužilaca tako i svih korisnika tehničkih sredstava veze, pri prenosu informacija ne bi se danas mogle da shvate kao neka sporedna obaveza, već kao prvenstveni zadatak i sistem rada, od čijeg doslednog izvršenja zavisi uspeh u paralisanju prisluškivača, odnosno bolje čuvanje tajni u miru i ratu.

Druga mera bi se sastojala u dobro organizovanoj kriptografskoj zaštiti veza. Već je rečeno da je kriptografska zaštita samo deo protivelektronskih dejstava i da njen zadatak da, primenom kriptografskih metoda, prisluškivaču učini nerazumljivom informaciju koja se prenosi kanalom veze.

Poznato je da sve informacije koje treba preneti nisu ni podjednako hitne niti tajne; isto tako nije potrebno ni sadržaj svih njih čuvati u tajnosti podjednako dugo.

Vojni autori često ističu da neku informaciju treba čuvati u tajnosti toliko dugo da protivnik, ako uspe i da sazna za nju, nema više neke naročite koristi od toga, niti vremena za efikasno reagovanje.

Broj korisnika sredstava veze je vrlo velik, a najveći njihov deo su neposredni korisnici telefona i radiofonije. Ovim vezama pribegava se kada je potreba za sporazumevanjem hitna, što je najčešći slučaj kod taktičkih jedinica, mada su kod njih i sadržaji informacija manjeg stepena (obima) tajnosti, a rok njihovog izvršenja vrlo kratak.

Kod primene kriptografskih sredstava vodi se borba između službi kripto-zaštite i službi dekriptiranja oko dužine vremena tajnosti, koje prve nastoje da obezbede, a druge što više da skrate. uspeh dekriptirera uvek zavisi od snage i nivoa kripto-službe, odnosno pravilnih procena o upotrebi adekvatnog kripto-materijala. Mnogi uspesi na ovom polju su proizišli, dobrim delom, iz slabosti kripto--službi, čija bi posledica mogla da bude upotreba neadekvatnih kriptografskih metoda, gde bi bitku za vreme zaštite informacija obično dobivali dekriptireri.

Kod većine ozbiljnih obrađivača problematike ED, posebno izviđanja veza, ističe se da RI i dekriptiranje predstavljaju vrlo korisnu i efikasnu, mada ne i svemoćnu delatnost. Zaštita se postiže dobro planiranim i objedinjenim protivelektronskim taktičkim i tehničkim merama, visokim stepenom discipline i obučenosti korisnika i poslužilaca sredstava veze, kao i širokom primenom adekvatnih kriptografskih sredstava.

Namera nam je bila da ovim člankom podsetimo širi krug čitalaca i na ove delatnosti, čija je važnost i aktuelnost sve veća, a bezbednost, obaveze i protivmere sve teže i složenije.

Potpukovnik
Milivoje KOVAČEVIĆ